Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В. А. Трапезникова Российской академии наук

Подразделение АСУ ТП АЭС

Документ стратегического планирования

Концепция нового поколения систем верхнего уровня АСУ ТП АЭС

Список разработчиков:

Руководитель проекта: д.т.н. Полетыкин А.Г.

Зам. руководителя проекта: к.т.н., с.н.с. Жарко Е.Ф.

Главный конструктор: Менгазетдинов Н.Э.

Руководитель группы СПО: к.ф.-м.н. Промыслов В.Г.

Москва

2017 г.

Аннотация

Данный документ был разработан в инициативном порядке группой специалистов Подразделения АСУ ТП АЭС. Документ посвящен системам верхнего уровня АСУ ТП АЭС. Проводится критический анализ достижений в этой области в свете изменений в науке, технике и обществе, произошедших за последние 15 лет. Предлагается описание основных черт систем следующего поколения.

СОДЕРЖАНИЕ

Обозначения и сокращения

АРМ	-	автоматизированное рабочее место
АРС	-	архивный сервер
АСРК	-	Автоматизированная система радиационного контроля
АСУ ТП	-	Автоматизированная система управления технологическими процессами
АТПС	-	Система администрирования программных и технических средств
АЭС	-	Атомная электростанция
БДУ	-	База данных уязвимостей
БПУ	-	Блочный пульт управления
ВВЭР-1000	-	Водо-водяной энергетический реактор
ВСМ	-	Виртуальная суперкомпьютерная модель
ЖЦ	-	Жизненный цикл
ЗИП	-	Запасные части, инструменты, принадлежности
ИБ	-	Информационная безопасность
ИПО	-	Интерфейсное программное обеспечение
ИУН	-	Информационно управляющая подсистема СВБУ для неоперативного контура управления АЭС
КД	-	Конструкторская документация
КМКП	-	Подсистема контроля, менеджмента и коммуникаций персонала СВБУ-2
КУДТП	-	Подсистема контроля, менеджмента и коммуникаций персонала СВБУ-2
КЭ СУЗ	-	Комплекс электрооборудования системы управления защитами
ЛВС	-	Локальная вычислительная сеть
ЛКЦ	-	Локальный кризисный центр
МПУ	-	Местный пульт управления
НСБ	-	Начальник смены блока АЭС
ОС	-	Операционная система
ПЗ	-	Предупредительная защита
ПНР	-	Пуско-наладочные работы

ПО	-	Программное обеспечение
ППР	-	Планово-предупредительный ремонт АЭС
ПТК	-	Программно-технический комплекс
РО	-	Реакторное отделение АЭС
РПО	-	Рабочее программное обеспечение
РПУ	-	Резервный пульт управления
РС	-	Рабочая станция
РЭ	-	Руководство по эксплуатации
СВБУ	-	Система верхнего блочного уровня
СВО	-	Система специальной очистки воды
СВСУ	-	Система верхнего станционного уровня АЭС
СВУ	-	Система верхнего уровня АЭС
СК	-	Суперкомпьютер
СКУ ЭЧ	-	Система контроля и управления электрической частью
СКУД	-	Система контроля, управления и диагностики реакторной установкой
СПД	-	Система подготовки данных
СПО	-	Системное программное обеспечение
СРВПЭ	-	Система регистрации важных параметров эксплуатации АЭС
СРК	-	Система радиационного контроля АЭС
СУБД	-	Система управления базами знаний
СУЗ	-	Система управления защитами
ТАИ	-	(Цех) тепловой автоматики и измерений
ТО	-	Турбинное отделение АЭС
ТС ОДУ	-	Технические средства оперативно-диспетчерского управления
ТУ	-	Технические условия
ТЭП	-	Технико-экономические параметры
УС	-	Устройства серверные
УТК	-	Устройства телекоммуникационные
ЦТАИ	-	Цех тепловой автоматики и измерений
ЦТП	-	Центр технической поддержки
ЧМИ	-	Человеко-машинный интерфейс
ЭВМ	-	Электронно-вычислительная машина (компьютер)

ЭД	-	Эксплуатационная документация
ЭКП	-	Экран коллективного пользования
ЭЧ	-	Электрическая часть

Введение

В середине 90-х годов прошлого века атомная промышленность России начала стремительный выход на мировой рынок. Ряд стран (Иран, Индия, Китай и другие) проявили заинтересованность в приобретении отечественных энергоблоков с реакторами на легкой воде типа ВВЭР-1000. Потенциальных заказчиков устраивали экономические характеристики российских АЭС, их надежность и безопасность. Вместе с тем, ряд подсистем АЭС их не устраивал.

К ним, в первую очередь, относились автоматизированные системы управления технологическими процессами (АСУ ТП), которые строились на основе традиционных средств автоматики с жесткой логикой, а программируемые контроллеры практически не применялись. Кроме этого, средства контроля и управления блочного пульта АЭС создавались на основе архаичных средств - стрелочные приборы, самописцы, световые индикаторы, ключи индивидуального управления оборудованием и т.п. В результате отечественные АСУ ТП АЭС занимали огромные помещения, требовали большого количества эксплуатационного и ремонтного персонала. Не были также реализованы алгоритмы контроля, управления и диагностики, повышающие безопасность АЭС, наличие которых является обязательным в соответствии с требованиями МАГАТЭ. К ним, в частности, относятся: система представления параметров безопасности АЭС, система регистрации важных параметров эксплуатации и другие.

В целом, отечественные АСУ ТП АЭС практически по всем параметрам уступали своим зарубежным аналогам. При этом для АЭС «Бушер», строившейся в Иране, закупки зарубежных технологий были невозможны из-за эмбарго. Было решено создать собственную лицензионно-чистую цифровую АСУ ТП, которую можно поставлять в любые страны без ограничений. Она должна соответствовать требованиям по безопасности в области атомной энергетики, широко применять программируемые контроллеры, цифровые средства передачи информации, включать расчетные и диагностические задачи. Причем в центре АСУ ТП должна находиться интегрирующая часть – вычислительная система верхнего блочного уровня (СВБУ), которая должна концентрировать информационные потоки и предоставить оперативному персоналу АЭС удобные, надежные и быстрые средства управления АЭС, на современном уровне решать как традиционные задачи, так и задачи, повышающие уровень безопасности АЭС.

Задача создания СВБУ была успешно решена усилиями нескольких организаций, включая ОАО «Атомэнергопроект», ЭНИЦ, ФГУП «ФНПЦ НИИИС» и ИПУ РАН.

Основные сведения о работе представлены в открытой печати на русском и английском языках. (Наиболее подробно сведения изложены в монографии, доступной по ссылке http://www.ipu.ru/sites/default/files/page_file/busher.pdf.)

Технические решения по СВБУ АСУ ТП АЭС «Бушер» успешно используются на действующих АЭС за рубежом (АЭС «Куданкулам», блоки 1-2 в Индии) и на новых АЭС в России (Калининская АЭС, блоки 3, 4, Нововоронежская АЭС, блок 6,7).

На каждой АЭС имеются отличия в реализации СВБУ, что позволяет объективно провести их сравнительный анализ. В работе это будет сделано.

За прошедшие 20 лет с момента, когда были сформулированы основные решения по СВБУ, произошли революционные изменения в области вычислительной техники, которые привели к фундаментальным культурным сдвигам, изменили мышление человека. Произошли изменения требований, зафиксированных в нормативной документации. Приобрели остроту старые вызовы и угрозы, такие как проблема подтверждения качества программного обеспечения, кибератаки. Проявились новые, например, укорочение жизненных циклов компонентной базы. Это делает актуальным пересмотр основных технических решений по СВБУ, внесение изменений в жизненный цикл, поиск новых решений, которые были бы достаточны в среднесрочной перспективе: до 2030 года.

1. Виды и свойства систем верхнего уровня АСУ ТП АЭС

К системам верхнего уровня (СВУ) АСУ ТП АЭС относятся:

- Система верхнего блочного уровня (СВБУ);
- Технические средства оперативно-диспетчерского управления (ТС ОДУ);
- Панели управления системами безопасности;
- Система регистрации важных параметров эксплуатации (СРВПЭ);
- Система верхнего станционного уровня (СВСУ).

ТС ОДУ представляют собой панели с традиционными аналоговыми и цифровыми приборами, которые предназначены для решения 3-х основных задач:

(1.) Представление персоналу информацию о состоянии основных параметров и технологического оборудования АЭС,

(2.) Управление основным технологическим оборудованием АЭС,

(3.) Управление (непродолжительное время) и перевод АЭС в безопасное состояние при отказе СВБУ.

СВБУ предназначена для реализации информационных, управляющих и вспомогательных функций во всех режимах работы энергоблока АЭС.

СРВПЭ предназначена для регистрации, хранения и выдачи информации о техническом состоянии энергоблока до, во время и после аварии в объеме, достаточном для последующего анализа аварийной ситуации и выяснения причин ее возникновения, путей развития, а также анализа действий персонала по ее локализации, ликвидации и предупреждению.

СВСУ предназначена для:

- реализации функции сбора и представления информации о состоянии основного технологического оборудования и систем энергоблоков АЭС, общестанционных технологических систем (АСРК, СКУ ЭЧ, МПУ);
- интеграции информации по обще станционным системам АСУ ТП и важной информации по энергоблокам;
- передачи данных во внешние системы.

СРВПЭ – это регистратор, не включенный в контур управления, а СВБУ и СВСУ – системы человеко-машинной коммуникации, вовлеченные в управление непосредственно.

СВБУ автоматизирует работу нескольких основных категорий персонала:

- Операторов-технологов реакторного отделения,

- Операторов-технологов турбинного отделения,
- Операторов систем неоперативного контура (систем спецводоочистки, пожаротушения и вентиляции и др.),
- Начальников смены блока (НСБ),
- Персонала цеха ТАИ АСУ ТП.

АРМы первых трех категорий персонала расположены в помещении блочного пульта или в примыкающих помещениях (АЭС «Бушер-1»). АРМ для персонала цеха ТАИ расположен в удаленных помещениях вблизи помещений для оборудования АСУ ТП.

Для прочего персонала выделены несколько АРМ, через которые можно производить контроль состояния АЭС и анализировать архив.

Определяющей особенностью человеко-машинного интерфейса СВБУ и СВСУ является способ контроля состояния АЭС и управления оборудованием посредством рабочих станций (РС). РС может иметь один или несколько (2-3) пассивных дисплеев, устройства типов трекбол-мышь, обычную и функциональную клавиатуру. Рабочие места (АРМ) СВБУ и СВСУ включают несколько РС, расположенных в ряд. Имеются РС, встроенные в панели ТС ОДУ, но они решают вспомогательные задачи. На приборных (пультовых) стойках РС располагаются отдельные органы управления особо важными агрегатами. В рамках одного АРМ отдельные РС могут иметь специализированное назначение или дублировать друг друга.

ЧМИ СВБУ российских АЭС включают также экраны коллективного пользования (ЭКП), расположенные на блочном пульте управления (БПУ), на которых выводятся данные для всеобщего обзора, дублирующие информацию на РС.

Стиль представления информации и навигации на РС в основном един, но может иметь инородные включения в виде окон, связанных напрямую с низовыми системами АСУ ТП (несколько РС СВБУ АЭС «Куданкулам» имеют возможность отображать окна КЭ СУЗ и СКУД).

Отображение сигнализации на СВБУ и СВСУ включает привлечение внимания звуком, цветовое и символьное кодирование, обобщение и представление информации различными способами. Фрагментарно сигнализация дублируется на ТС ОДУ.

С технической точки зрения СВБУ и СВСУ представляют собой многомашинные вычислительные комплексы, связанные с другими системами АСУ ТП (через шлюзы) и между собой локальной вычислительной сетью (ЛВС). Комплексы строятся из приборных стоек основных трех видов: приборная стойка РС, приборная стойка сервера, приборная

стойка телекоммуникационная. К ним могут присоединяться принтеры, приемники систем спутниковых сигналов (времени), ленточные и иные накопители и т.п.

ЛВС строятся на основе промышленных волоконно-оптических линий связи и сетевого оборудования и общепромышленных протоколов передачи информации (IP-протоколы).

Приборные стойки конструируются на основе модулей различных производителей. Стойки обладают свойством ремонтопригодности: отказавшие модули могут заменяться на ЗИП эксплуатационным персоналом.

Киберзащита включает средства обеспечения защиты от несанкционированного доступа: механическими запорами, ключами, блокировкой сервисов, разграничением доступа, парольной защитой и др.

СВБУ, СВСУ и СРВПЭ разрабатывались по нормам, правилам и традициям СССР. При этом применялись решения, доступные на мировом рынке промышленной электроники, а особенности этого рынка не учитывались. В частности, не было учтено, что показатели надежности компонент не достоверны. Не учитывалось также отсутствие долгосрочных гарантий выпуска продукции в период эксплуатации СВУ и многое другое.

Обслуживание СВБУ, СРВПЭ производится персоналом цеха ТАИ энергоблоков. В этом участвует: сменный персонал (3 смены по 8 часов на пульте АТПС) в составе:

- Оператора АТПС,
- Инженера по эксплуатации программного обеспечения,
- Ремонтный персонал.

Обслуживающий персонал должен иметь среднюю квалификацию по специальности, связанной с эксплуатацией вычислительной техники, и пройти специальное обучение.

Оператор АТПС должен постоянно находиться на пульте и контролировать работу всего АСУ ТП, включая СВБУ, СВСУ и СРВПЭ.

Наличие инженера по эксплуатации ПО и ремонтников (2 человека в 3 смены) связано с необходимостью выполнения требований по обеспечению надежности, обнаружению отказов и ремонту: например, на АЭС «Бушер-1» отказы должны диагностироваться с задержкой не более 10 секунд, а ремонт (замена сменных узлов) не должен превышать 2-х часов.

Обслуживание СВСУ аналогично, но используется отдельный персонал, не связанный с энергоблоками.

2. Критический анализ СВБУ (СВСУ, СРВПЭ) первого поколения

Перечисленные выше общие свойства СВБУ, работающих на энергоблоках АЭС «Бушер» (блок 1), «Куданкулам» (блоки 1, 2), Калининской (блоки 3,4), Ростовской (блоки 3,4), Нововоронежской (блок 6,7), позволяют объединить их в группу с названием «1-е поколение СВБУ».

Несмотря на то, что СВБУ 1-го поколения убедительно доказали, что управление АЭС при помощи РС возможно и не вызывает критических замечаний, можно выделить ряд недостатков.

СВБУ эффективно автоматизируют работу только части эксплуатационного персонала. Дополнительные АРМ не обеспечивают потребностей всего персонала, особенно, при пуско-наладочных работах.

АРМ операторов-технологов, особенно реакторного отделения, включают несколько РС, соединенных в изогнутый ряд и образующих рабочую область большой протяженности. Это приводит к тому, что один оператор в сидячем положении может комфортно работать только с одной 2-х (3-х) дисплейной РС. Исходя из этого ограничения создавался весь дизайн видеокадров. Что указывает на достаточность 2-х (3-х) дисплее на одном АРМ.

НСБ на АЭС «Бушер» и «Куданкулам» выражают претензию, что их АРМ не обеспечивает удобный доступ ко всему набору измеряемых параметров, циркулирующих на всех других РС СВБУ, что было связано с изначальными проектными подходами к распределению информации по АРМам в рамках СВБУ.

Замечено, что персонал цеха ТАИ АСУ ТП активно взаимодействует с операторами-технологами, особенно при неисправностях, которые влияют на управление АЭС, но относятся к сфере компетенции персонала цеха ТАИ АСУ ТП. Поскольку АРМ системы администрирования технических и программных средств (АТПС) АСУ ТП расположен не на блочном пульте, это создает значительные неудобства.

Устройства типа мышь-трекбол и клавиатура, особенно когда они установлены в паре (как на АЭС «Куданкулам») показали свое удобство, но были отмечены их отказы, связанные с износом механических частей (контактов). Эти отказы надежно не диагностируются, что приводит к необходимости разборки конструктивов для поиска причины.

Поскольку на трех энергоблоках АЭС («Бушер-1», «Куданкулам-1, 2») ЭКП не установлены и индийский заказчик («Куданкулам») не требует их установки на блоки 3, 4, то можно считать эти устройства не нужными.

Для звуковой сигнализации, воспроизводимой РС разных АРМ, используются разные мелодии. Но поскольку эти АРМ находятся в одном помещении, то тревожный звук влияет не только на того, кому это предназначено.

Приходится принять как данность, что операторам приходится оперировать большим количеством сигнализации, которую невозможно держать в памяти. Методы фильтрации и агрегации сигналов, применяемые в СВБУ, не эффективны в решении этой проблемы.

Модульная конструкция приборных стоек показала свою эффективность, но имеет и недостатки. Один связан с тем, что стойки внутри представляют собой сложное переплетение кабелей, разъёмов и т.п. При техническом обслуживании (удаление пыли) и ремонтах персонал легко может совершить ошибочные действия, которые иногда могут приводить к серьезным отказам. Второй связан с легкостью внедрения и трудным выявлением инородных (вредоносных) элементов кибератаки.

Опасность кибератак исходит также от подключения к сети принтеров, ИБП, мультиконтрольных блоковкоторые включают в себя полноценные компьютеры с проприетарным программным обеспечением (ПО), а также внешних устройств (флеш-карты, лэптопы и др.).

Из-за снятия с производства компонент промышленной электроники СВБУ, СВСУ, СРВПЭ столкнулись с проблемой отсутствия ЗИП и необходимостью производить замену технических и программных компонент (модернизацию).

Модернизация предусмотрена каждые 10 лет. Она включает замену компонент вычислительной техники, что влечет за собой замену операционных систем и далее внесение существенных изменений в прикладное программное обеспечение. Это дорогое и потенциально опасное мероприятие периодически снижает надежность СВУ.

Для эксплуатации СВБУ, СВСУ, СРВПЭ штатно требуется привлекать 6 человек в день. При исправном оборудовании с запасом ресурса в этом нет необходимости. (Поэтому это требование часто не соблюдается). Но когда оборудование устаревает, не часто, но появляются отказы, устранение которых требует участия нескольких человек. Получается, что нужно содержать персонал, поддерживать его квалификацию, но использовать его крайне редко.

В сложных случаях СВБУ, СВСУ, СРВПЭ требуют привлечения организаций-разработчиков. При этом часто срочно. В реальности это происходит в рамках договоров по технической поддержке и сопровождению. Поскольку в самих СВБУ, СВСУ, СРВПЭ для этого ничего не предусмотрено, то для коммуникаций и работы используются внешние средства (электронная почта, телефон, FTP-серверы и т.п.), к которым не применимы понятия надежности, быстродействия и др. характеристики. Поэтому невозможно оценить надежность и безопасность процесса технической поддержки, гарантировать результат (оказание квалифицированной помощи вовремя) и создает дополнительные риски (кибератаки).

3. Текущее состояние и прогноз развития вычислительной техники для АСУ ТП

За последние 20 лет в вычислительной технике и человеко-машинном интерфейсе произошли качественные и количественные изменения, часть которых можно и необходимо использовать в системах управления.

3.1. Дисплеи широкого формата и высокого разрешения

В 90-х - 2000-х годах профессиональные компьютерные дисплеи имели размеры до 20” (или чуть выше). Разрешение SGA позволяло размещать их на дистанции 70-100см от глаз человека и обеспечивать комфортную работу. Если требовалось расширить площадь, то применялись 2 (реже 3 или более) дисплеев или размещали дисплеи в две ряда (4-6).

Несколько дисплеев на одном рабочем месте имеют один недостаток: невозможно отобразить окна большого размера. А это важное ограничение в АСУ ТП, где информация об объекте управления часто носит связный характер.

В нестоящее время промышленность получила возможность создавать дисплеи практически неограниченного размера с размерами пикселей не больше чем у тех, что были раньше. При этом четкость, контрастность и реактивность значительно улучшились. (А цена наоборот стала меньше.)

ТВ панели с отношением сторон 4:3 снимаются с производства.

Освоены промышленные производства ТВ панелей размерами до 215 см (85") с отношением сторон 16:9 для:

- FHD (2К)- разрешение 1920*1080
- UHD (4К) - разрешение 3840*2180
- перспективное (8К) - разрешение 7680*4320.

Появились панели с отношением сторон 21:9, с разрешением:

- 2560*1080
- 3840*1600
- 5120*2160

с размерами до 2,6 м (105”).

На смену LCD начинает приходить OLED (Organic Light Emitting Diode) (см. рис. 3.1, 3.2). Технология, обеспечивает:

- минимальное время отклика,

- широкий угол обзора и отличную передачу цвета,
- низкое энергопотребление,
- возможность создавать гибкие экраны,
- диапазон рабочих температур (от −40 до +70 °C)

На сегодня недостатком OLED-телевизоров является непродолжительное время работы, относительно ЖК-панелей - 30 тысяч часов против ста тысяч.

Рис. 3.1.

Рис. 3.2

Поэтому на рабочих местах пультов управления вместо много дисплейных конструкции можно применять одно дисплейные и снять ограничение на размер окон, доведя его до охвата всей зоны видимости одного человека.

3.2. Интернет, беспроводные технологии и мобильные устройства

Беспроводные технологии разнообразны. Они включают инфракрасные устройства, устройства на основе радиоволн, на основе света и т.д.

Развитие Интернет и беспроводных технологий носило взрывной характер и в настоящее время почти все пространство земли оказалось ими охвачено.

Вместе с мобильными устройствами они превратили большинство мест в околоземном пространстве в точки доступа к информации.

В профессиональной области эти технологии позволили интенсифицировать труд людей в том месте, где они находятся и тогда, когда это нужно.

На промышленных предприятиях это позволило качественно повысить информационную оснащенность работников, связать их напрямую с автоматизированными системами управления.

Беспроводные технологии позволили включать в контуры управления для решения сложных задач уникальных (и труднодоступных) людей-экспертов, находящихся вне предприятий.

Технологии оказали качественное влияние на поведенческую культуру людей: с точки зрения современного человека доступ к информации (всей/любой) есть/должен быть всегда и находится рядом с ним. (А отсутствие этой возможности вызывает у современного человека чувство оторванности, беззащитности.) Разработчики автоматизированных систем управления должны рассматривать это как одно из главных (если не основных) эргономических требований.

В части беспроводных сетей:

- Повышение несущей частоты WiFi:
    - Широко освоенный стандарт 802.11ac- несущая частота -5Ггц.
    - Стандарт 802.11ad (Технология WiGig) - несущая частота- 60Ггц. Специфированный предельный скоростной уровень для WiGig – 8 Гбит/с, в 3-5 раз быстрее, чем у современных устройств, поддерживающих стандарт 802.11ac (Wave I), при этом радиус покрытия технологии ограничивается 10 метрами. Считается, что WiGig с легкостью вытеснит с рынка технологию Bluetooth.

- Начинает развиваться технология Li-Fi (Light Fidelity) (Стандарт IEEE 802.15.7), которая позволяет передавать с помощью светодиодной лампы информацию на очень высоких скоростях, и по факту является оптической, высоко помехоустойчивой версией Wi-Fi.

  Стандарт IEEE 802.15.7 определяет для Li-Fi физический уровень сетевой модели OSI PHY (Physical layer), а также уровень управления доступом к среде MAC-адрес (Media Access Control). Рабочая версия IEEE 802.15.7 выделяет три PHY, различных по пропускным способностям, которые представлены в таблице 3.1.

Таблица 3.1. Характеристика физических уровней стандарта IEEE 802.15.7

	PHY I	**PHY II**	**PHY III**
Область применения	Наружное применение. Приложения с небольшим объемом данных	Внутри помещения	Множественные источники и приемники RGB
Скорость работы, Мбит/с	≈ 0,012 – 0,268	1,25 - 96	12 - 96
Алгоритм коррекции ошибок	Convolutional. Reed Solomen	Reed Solomen	Reed Solomen
Тип модуляции	OOK (On-off keying). VPPM (Variable pulse position modulation)	OOK (On-off keying). VPPM (Variable pulse position modulation)	CSK (Colour shift keying)

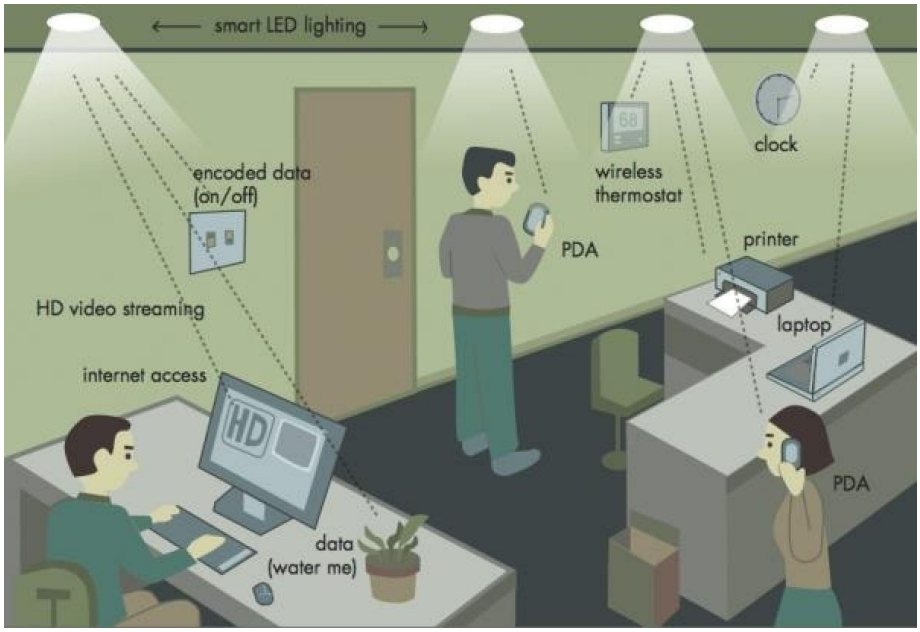

Рис. 3.3

Преимущество Li-Fi в сравнении с Wi-Fi:

1 Использует электромагнитный спектр светового диапазона и соответственно может имеет более широкую полосу пропускания (проверенные скорости передачи до 224 Гб/с).

2 Может иметь детерминированную (заранее определенную) зону (площадь) покрытия в пределах прямой видимости, что позволит обеспечить более высокий уровень информационной безопасности.

3 Возможность использования системы освещения для организации, локальной вычислительной сети с регламентированными зонами доступа (см. рис. 3.3).

- Технология Near field communication «NFC» — коммуникации ближнего поля
  - высокий КПД при работе на дистанциях до 0.5…1 м;
  - низкий уровень питающих токов в режиме приема и передачи;
  - низкий коэффициент поглощения поля тканями человеческого тела;
  - высокая степень защиты данных;
  - низкий уровень шумов за счет создания короткодействующего поля.

Применение технологий поможет повысить комфортность для людей при выполнении служебных обязанностей за счет снятия ограничений, связанных с обязанностью находиться на рабочих местах в сидячем или стоячем положениях и т.п.

3.3. Контактные устройства

Данный вид устройств (браслеты, датчики, часы, наушники, очки и др.) улучшают жизнь и бурно завоёвывают популярность у людей.

Часть из них пассивна и управляются командами от человека. Это наушники, очки для просмотра фильмов и др.

А некоторые устройства активно взаимодействуют с людьми. Пока в ограниченном объеме: для браслетов и часов это контроль пульса, давления, управление двигательной активностью и т.п.; для устройств дополненной реальности - навигация в пространстве.

Общим для этих устройств является наличие органов ввода информации от человека и устройства для прямого воздействия на органы его чувств: тактильные, звуковые, световые.

Если разместить эти устройства на теле и/или одежде человека можно контролировать параметры его здоровья, эмоциональное состояние, перемещения,

разговоры и т.д. А если использовать устройства воздействия на человека, то можно им управлять. Это открывает широкие возможности для совершенствования управления производством, в котором используются люди.

Для потенциально опасных объектов контроль и управление персоналом является одной из важнейших задач. Применение контактных устройств поможет ее решать гораздо эффективнее. Люди, оснащенные контактными устройствами, могут включаться в качестве объектов в автоматизированные системы управления.

3.4. LINUX и виртуализация в системном программном обеспечении

Linux и стандарты POSIX, ANSI C, X11 и др. заняли доминирующее положение и породили семейства операционных систем, завоевавшие основные рынки системного программного обеспечения (СПО), включая СВУ АЭС. Альтернатив этой тенденции пока не наблюдается, хотя попытки имеют место.

Тенденция имеет два направления. Первое состоит в создании полноценных полифункциональных систем, которые конкурируют с MS Windows. Это «системы для бедных» или для тех, кто не может использовать качественные проприетарные продукты (спецслужбы, военные и т.п.). Они не очень надежны, еще менее стабильны и редко используются в промышленных офисах.

Примеры: Fedora, Альт Линукс и др.

Вторая тенденция: создание узкоспециализированных (с ограниченными функциями) СПО с ориентацией на специфическое оборудование. Эти СПО, наоборот, очень надежны и стабильны.

Примеры: МАС ОС, LICS и др.

Это имеет простое объяснение. Дело в том, что компоненты проприетарных СПО сделаны более качественно, чем у Linux. Естественно, полномасштабные СПО собранные на их основе будут лучше. Но узкоспециализированные СПО имеют необходимый минимум компонент и их можно лучше проверить. В результате у разработчиков со средними возможностями получаются высококачественные продукты.

Основываясь на опыте по созданию СПО для СВУ АЭС, предлагается продолжать линию LICS с периодом обновления в 10 лет.

До недавнего времени этапы жизненного цикла программ от модернизации до модернизации зависели от времени поддержки версий операционных систем

производителями. При смене версии производителям прикладных программ, приходилось их адаптировать, внося существенные изменения, и (увы, неизбежно) на какое-то время снижая их надежность.

Для АСУ модернизация прикладных программ особенно вредна, опасна и затратна. Поэтому очень часто для их работы используются устаревшие технические средства (дорогие и не надежные) и устаревшие операционные системы иногда уже вне пределов поддержки производителями.

Чтобы продлить стабильные участки жизненного цикла прикладных программ начали широко применяться программные среды виртуализации. В их основе лежит принцип относительной стабильности сервисов, которые операционные системы предоставляют для разработчиков прикладных программ. Оказывается, что стабильные участки в жизненном цикле этих сервисов намного превосходят время жизни версий и самих операционных систем.

Было предложено выделить стабильные части из операционных систем и создать на их основе, так называемые среды виртуализации, которые играют роль стабильных промежуточных слоев между операционными системами и прикладными программами. (Подробнее см. Приложение 5).

Примеры: Oracle VM, Docker и др.

В результате стало возможным продлевать жизненный цикл прикладных программ на интервалы времени, определяемые сменой семейств процессоров (определяется системой команд), которые занимают многие десятки лет и сопоставимы со временем жизни АСУ промышленных объектов.

Предлагается разработать среду виртуализации для атомной энергетики с периодом обновления в 30 лет.

3.5. Тенденции развития вычислительных средств

3.5.1 Частота процессора

Рост частоты процессора остановился. Закрытии Intel проектов, продолжателей архитектуры NetBurst (Pentium 4) в направлении увеличения тактовой частоты, по сути ознаменовало переход в эпоху многоядерных процессоров (см. рис. 3.4).

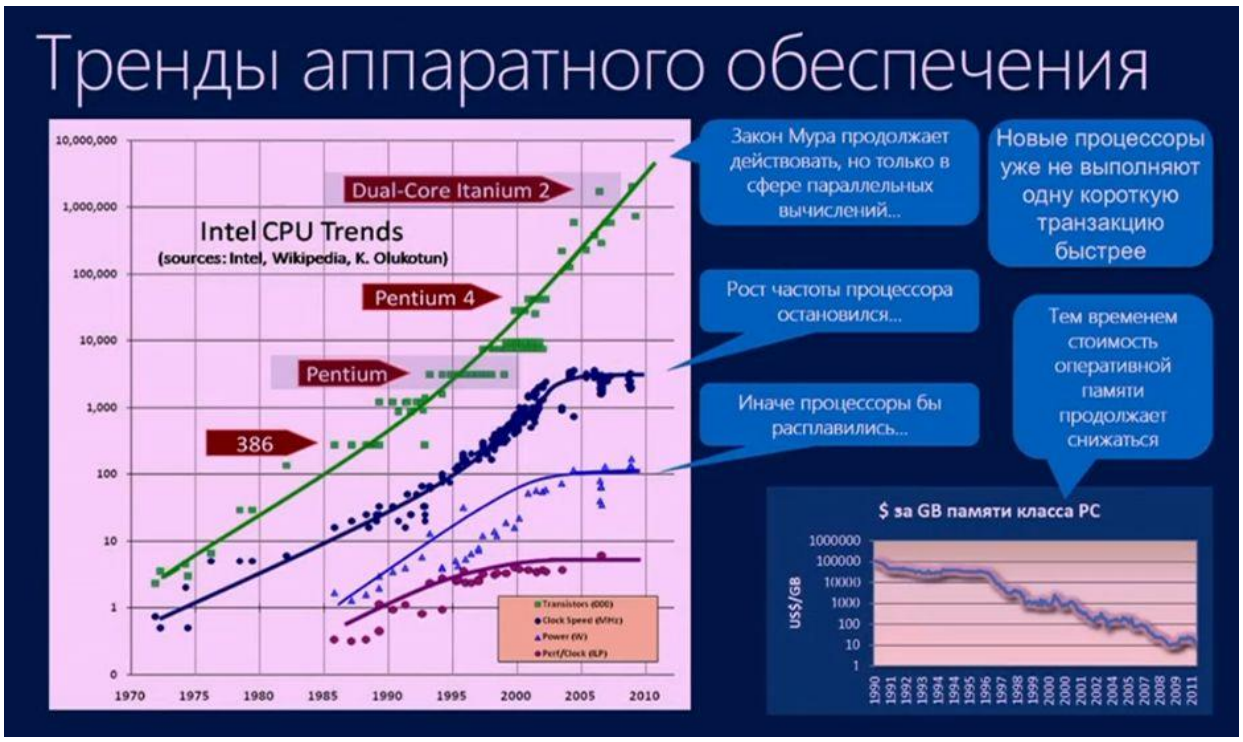

Рис. 3.4

3.5.2 Тренд вытеснения архитектурной платформы x86 архитектурой ARM.

Наметился тренд вытеснения архитектурной платформы x86 архитектурой ARM. Монополии Intel и AMD с архитектурой платформой x86 начинает противостоять большая группа независимых изготовителей и разработчиков процессоров с архитектурной платформой ARM. При этом и Intel, и AMD начинают собственное производство ARM процессоров (см. рис. 3.5, 3.6).

ARM Holdings ожидает, что крупномасштабные развертывания серверов, основанных на ARMv8-A-совместимых процессорах, начнутся в 2016 или 2017 году и, что каждый четвёртый сервер в 2020 году будет использовать процессор с архитектурой ARM.

Специализирующаяся в области стандартов организация Linaro в настоящее время готовит к выпуску референсную Open Source-платформу для серверов, оснащенных процессорами с 64-разрядной архитектурой ARMv8-A. Эта платформа предоставит производителям чипов, проектировщикам и разработчикам свободное ПО

и микропрограммные средства, необходимые для интеграции создаваемых ими продуктов и технологий в ARM-серверы.

Прогнозируется, что бурное развитие и применение ARM архитектуры будет обусловлено взрывными темпами роста технологии IoT (интернет вещей).

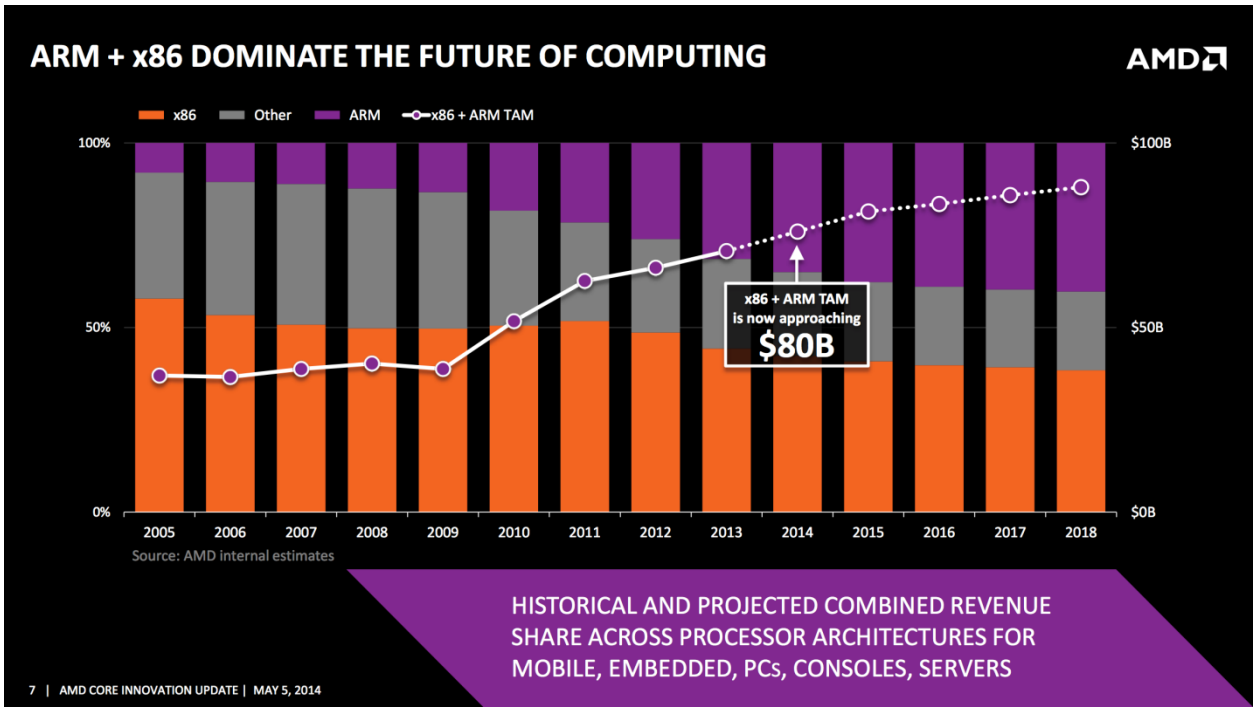

Рис. 3.5

Рис. 3.6

3.5.3 Эволюционные изменения в конструкциях вычислительных средств.

Значительное уменьшение массогабаритных характеристик, количества механических контактных соединений, тепловыделения, повышение надежности и помехоустойчивости основаны на технологиях SiP (System-in-Package, «система-в-упаковке») и SoC (System-on-Chip, «система-в-чипе»)

Примеры эволюции системных блоков рабочих станций представлены на рис. 3.7, 3.8 и 3.9, которые соответствуют 2005г., 2016 г. и 2017-2020гг.

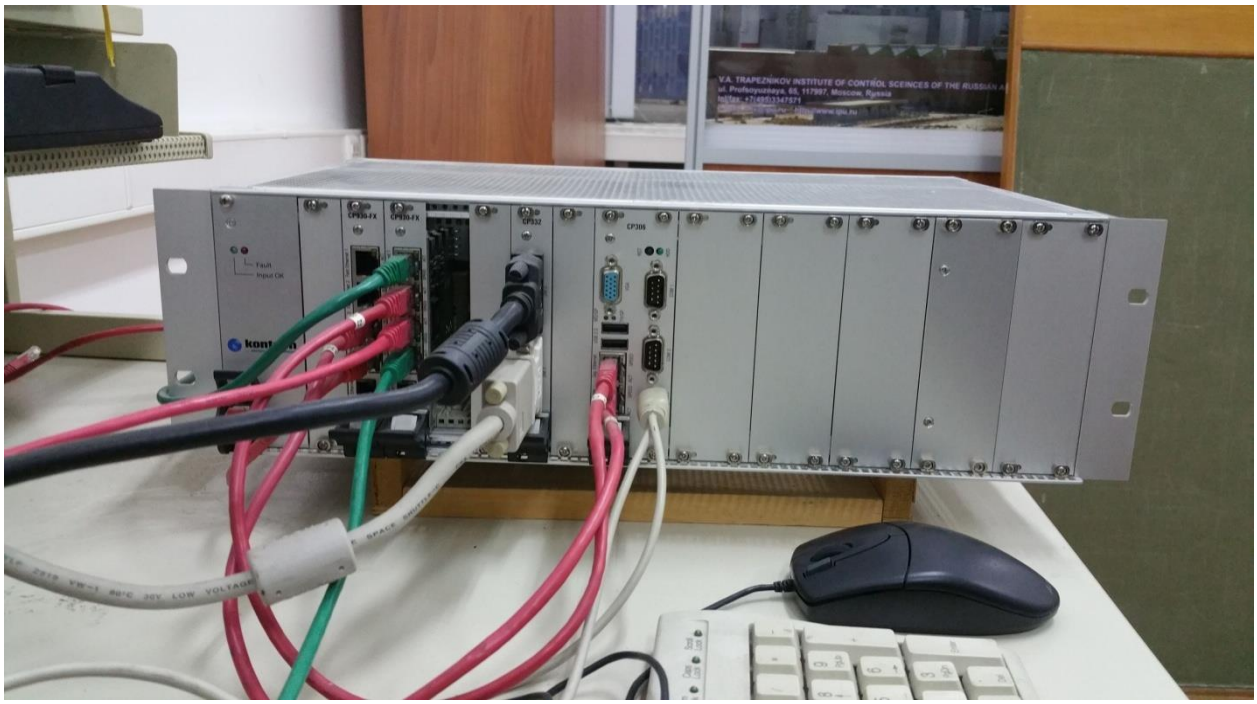

Рис. 3.7

Рис. 3.8

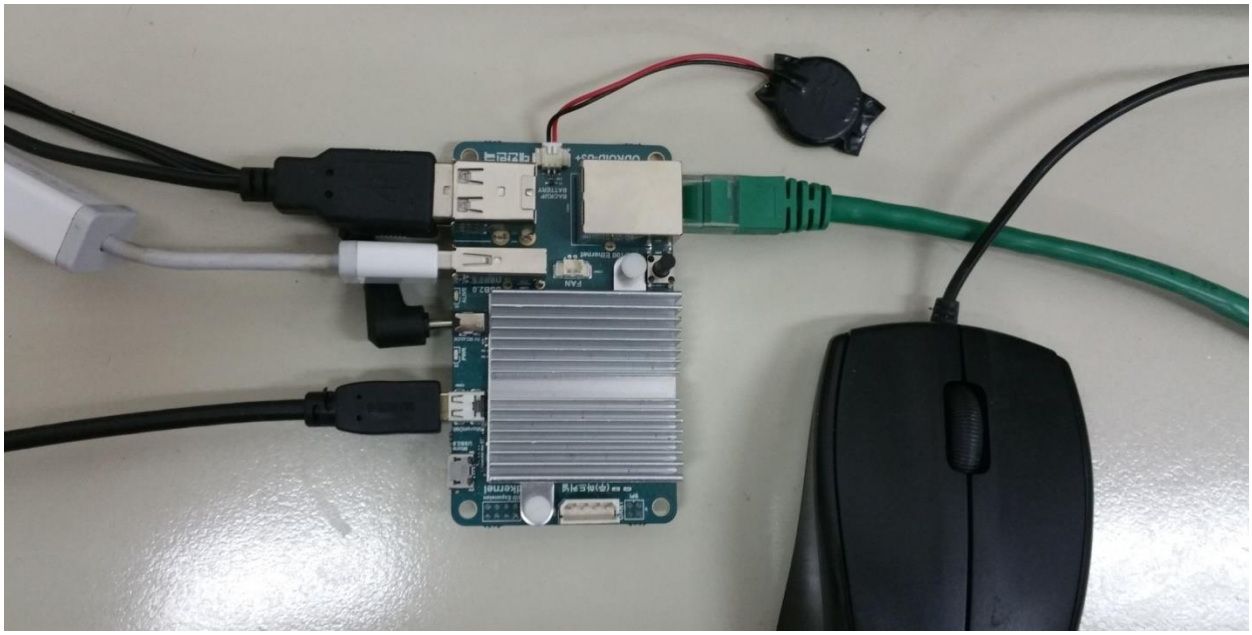

Рис. 3.9

В настоящее время широкое применение SoC технологий в телевизионных приемниках, превращает их в интеллектуальное информационное средство, подключенное к интернет среде.

3.5.4 Эволюция конструкции серверов

Эволюция конструкции серверов основана на модульном принципе, называемые Blade-серверами, или серверами-лезвиями (blade — лезвие).

Первыми компаниями, интегрировавшие данные системы в свои IT-инфраструктуры, стали NASA и военные структуры. Впоследствии эту технологию производства серверного оборудования выкупила компания HP, а затем и другие компании – гиганты IT-индустрии: Intel, IBM, DELL, Cisco и др.

Помимо форм-фактора, основные отличия блейд-серверов от традиционных систем в том, что все необходимые элементы управления кластером серверов, мониторинга, питания, охлаждения и пр. физически расположены «в одной коробке». Объединяющим элементом является пассивная системная плата BackPlane.

Преимущества Blade-серверов:

- уменьшение стоимости и повышение надежности;
- сокращение количества коммутационных проводов;
- повышение удобства управления системой;
- уменьшение занимаемого объема;
- уменьшение энергопотребления и выделяемого тепла;
- высокая масштабируемость;
- гибкость.

Пример реализации отечественного блейд-серверов представлен на рис. 3.10.

Рис. 3.10

- Компании «Рикор» и «Альт Линукс» представили отечественный аппаратно-программный комплекс. Решение включает блейд-сервер от «Рикор» и операционную систему ALT Linux.
- Как говорится в заявлении «Альт Линукс», блейд-сервер от «Рикор» построен на базе ARM-процессоров Armada-XP. На «лезвиях» этого блейд-сервера работает специальная сборка ALT Linux и различные решения под ее управлением.
- Среди таких решений: стандартный сервер типа LAMP (Linux+Apache+MySQL+php); модульная система удаленного управления Alterator (ALT Linux); система управления бизнес-процессами Runa WFE; а также удаленное офисное рабочее место, доступное в режиме терминального доступа (VDI).
- Подробнее:http://www.cnews.ru/news/line/rikor_i_alt_linuks_predstavili

3.6. Информационная поддержка

Среди разнообразных средств получения информации наибольшую популярность получили несколько технологий искусственного интеллекта.

Первая обеспечивает людей информацией. Это поисковые системы, которые понимают письменную или устную речь и находят ответы на самые разнообразные вопросы.

Вторая технология связана с логистикой и планированием. Это разнообразные навигационные ресурсы: планирование путешествий, поездок по странам и городам и т.п.

На основе указанных технологий строятся системы управления разного назначения. В частности поисковые системы используются для манипулирования потребительской, политической и др. активностями масс людей. В промышленных системах поисковые системы используются для доступа к документам, инструкциям, записям и т.п.

Технологии логистики легли в основу систем управления перевозками такси. Это пример из области транспорта. Но сфера применения технологии планирования гораздо шире.

Третья технология – социальные сети. В ней искусственный интеллект выступает в роли организатора интеллектуальной деятельности множества людей. Такого рода деятельность характерна для работы в промышленности при решении сложных проблем управления и ее интенсификация является, безусловно, актуальной.

Четвертая технология, виртуальная реальность, находится на подъёме и уже занимает прочные позиции в сфере развлечений. Примером применения в технических системах являются тренажеры. Они используются в авиации, управлении судами, машинами и т.п. Для управления АЭС технологии виртуальной реальности могут также использоваться для тренировки персонала. Например, для создания условий, которые невозможно воспроизвести на функциональных и полномасштабных тренажерах: для тренировки работы на резервном пульте управления, управлении АЭС в условиях сейсмических колебаний, при пожарах и т.п. При этом виртуальные модели могут подключаться как к компьютерным моделям, так и к реальным данным от АСУ ТП.

Технологии виртуальной реальности также могут успешно применяться при проектировании/модернизации блочных пультов, их верификации и валидации. При этом могут применяться и технологии дополненной реальности, когда часть оборудования моделируется натурно, а часть при помощи компьютеров.

Технологии дополненной реальности одни из самых новых и перспективных. В АСУ ТП их можно применять для замены традиционных показывающих приборов и компьютерных пультов управления. В первом случае показания можно привязать к месту (метке, коду) на оборудовании или окружающих поверхностях, при сканировании

которого цифровой камерой на экране появляются данные измерений. Местные компьютерные пульты управления можно имитировать при помощи переносных устройств, которые будучи помещены в определенное место, автоматически перепрограммируются и выполняют все функции замещаемого компьютера.

Дополненная реальность позволяет совмещать в пространстве видео изображения реальных устройств и информацию о них из АСУ ТП, что позволяет усилить информационную поддержку персоналу при работе с оборудованием АЭС и АСУ ТП на местах их расположения.

Распространение перечисленных технологий сделало их незаменимыми, превратило в часть культуры, цивилизации. Поэтому в системах управления, в тех местах, где используются люди, нужно ориентироваться именно на эти технологии при организации информационной поддержки.

4. Вызовы

Вызовы, влияющие на АСУ ТП АЭС, связаны с эволюционными и революционными изменениями в области вычислительной техники (см. п. 3), автоматизированных систем управления, преступной деятельности, человеческого быта и мышления.

4.1. Автоматизированные системы управления

В отличие от старых автоматизированных систем, которые включали машины как объект управления, оборудование АСУ для автоматического и дистанционного управления и людей на самом верхнем уровне, самые современные автоматизированные системы имеют иную структуру. В качестве объектов управления выступают не только машины, но и люди. Для связи с ними используются промышленные и публичные средства коммуникации. Для управления применяется симбиоз человек-машина, где решение задач равноправно распределено между людьми и автоматикой под общим руководством алгоритмов искусственного интеллекта.

Примером такого рода систем могут служить системы перевозок Uber, Yandex и др.

Появление и доказанная эффективность нового вида автоматизированных систем позволяет по-новому организовать управление АЭС.

Во-первых, можно непосредственно включить обслуживающий персонал АЭС в качестве объектов управления наряду с механизмами. Это позволит увеличить производительность труда и минимизировать влияние человеческого фактора на безопасность.

Во-вторых, используя возможности современных средств связи и методы искусственного интеллекта, можно в рамках АСУ ТП АЭС автоматизировать контуры управления, существовавшие в неформализованном виде. Имеется в виду административное управление, техническую поддержку со стороны заводов-изготовителей, экспертов, надзорных органов и т.д. Это может иметь значительный экономический эффект за счет сокращение затрат на документооборот, совещания, командировки и т.п.

4.2. Киберпреступления

Являясь компьютерными системами, АСУ ТП (и АЭС) стали объектами кибератак давно, но в 2008 году, после атак на иранские центрифуги, наступила эпоха кибервойн, которая характеризуется следующими особенностями:

- Целью является нанесение вреда объекту управления,
- Комплексно используются уязвимости в технологическом процессе, системе охраны и информационной безопасности,
- Явно уличить виновных невозможно,
- Орудия применяются однократно, после чего утрачивают разрушительную силу.

Ответ должен быть симметричным. Это означает, что:

- Защищать нужно объект, используя методы оценки риска по аналогии с теми, что применяются для технологической и специальной безопасности,
- Защита должна комплексно использовать все средства из арсенала информационной, технологической и специальной безопасности,
- Защита должна совершенствоваться по мере развития методов нападения.

Защита от киберугроз предлагается рассматривать как непрерывный процесс, охватывающий все этапы жизненного цикла, включая эксплуатацию.

Для реализации этого процесса в СВБУ должна решаться специальная задача. Для нее в проекте необходимо предусмотреть: помещение, персонал и специальные аналитические инструменты, позволяющие оперативно контролировать уровень безопасности, выявлять новые угрозы, оценивать риски и выбирать меры по их минимизации.

4.3. Изменение ментальности

Web, поисковые системы и офисные программы сделали информацию доступной, а бумажную форму не нужной. Беспроводные сети, ноутбуки, планшеты и смартфоны обеспечили доступ к информации из любой точки в пространстве, а перемещение к ее источникам не нужным. Социальные сети создали виртуальную среду общения, сделав очные встречи не нужными. «Интернет вещей» обеспечил удаленный интерфейс людей и машин, что сделало не нужным физический доступ к ним.

Все эти достижения революционно повлияли на способы жизни, работы и мышления людей. В частности, это изменило общий способ решения проблем, которым пользуются люди.

Если возникает бытовая проблема, то современный человек делает следующее:

1. Производит запрос к поисковой системе (Google, Yandex или др.),
2. Если ответ не позволяет решить проблему, то он обращается к социальным сетям, размещая текстовые описания наряду с аудио и видеоинформацией.
3. Если и это не помогает, то человек пытается разобраться сам, привлекая информацию из таких источников, как Википедия, электронные инструкции и мануалы, размещенные в сети и т.п.
4. Если самостоятельно решить проблему не получается, то прибегают к традиционным способам (звонки в сервисные центры, вызов специалистов, эвакуация и т.п.), используя при этом все возможности Интернет.

Пункты 1, 2, 3 могут меняться местами для разных людей.

Нетрудно заметить, что это не совпадает с тем, как решаются проблемы на производстве. И это порождает диссонанс, заставляя людей постоянно перестраивать способ мышления с бытового на профессиональный.

Между тем описанный новый способ решения проблем в быту выработан в результате развития человеческой цивилизации и внедрения самых современных технологий: искусственного интеллекта (I), автоматизированного интерсубъектного взаимодействия (II), Интернет (III). Он намного более современный и эффективный, чем старый, основанный на библиотеках документов, телефонных переговорах, совещаниях, командировках и т.п. Его адаптация к производственной деятельности сулит большую экономию человеческого рабочего времени, одновременно повышая качество продукции.

Адаптация в части СВБУ состоит в создании развитых производственных сетей обмена информацией и в применении информационных инструментов, включая:

- Производственные поисковые системы с управлением при помощи текстов на естественном языке, голосом,
- Системы интерсубъектного аудита, поддерживающие работу целевых виртуальных экспертных групп,
- Экспертные систем для решения различных задач,
- Банки данных и знаний по тематике производства и др.

4.4. Фундаментальные ограничения вычислительной техники

К настоящему времени иллюзии о том, что возможно путем верификации и валидации создавать ПО без ошибок, можно считать окончательно утратившими силу. Осознано, что компьютеры современной архитектуры, всегда будут иметь ошибки. Это такое же фундаментальное ограничение как скорость света.

В силу невозможности определить вероятность ошибочной работы ПО для АСУ, ошибки в которых могут приводить к большим потерям, риск применения ПО считается недопустимым.

Это касается АЭС: применить ПО можно только в тех случаях, когда возможный ущерб и риск не критичен, например, для решения задач контроля, диагностики, информационной поддержки и др. при нормальной эксплуатации, а для управления системами безопасности нельзя.

Часть ошибок ПО можно использовать для организации киберпреступлений. Это так называемые уязвимости ПО. Их наличие – точнее невозможность убедится в их отсутствии – также следует рассматривать как ограничение. Оно ограничивает возможность применения вычислительной техники, если возможный ущерб от киберпреступлений велик, а эффективных мер борьбы с потенциальными киберпреступниками нет или они не применяются.

В отличие от ошибок в ПО, для противодействия киберпреступникам разработаны многочисленные способы борьбы (См. ФСТЭК N 31). Анализ угроз, оценка рисков с последующими выбором и реализацией мер киберзащиты могут снять данное ограничение для конкретных АСУ или их частей.

По-видимому, такое положение дел будет сохраняться, пока не будут разработаны принципиально новые виды вычислительной техники, но это дело будущего.

5. Новые функции

Был проведен анализ российских стандартов, касающихся СВБУ. В результате были выявлены те их требования, которые не реализованы в СВБУ-1 в полном объеме. В таблице 5.1 представлены результаты с предложениями по учету в СВБУ-2.

Таблица 5.1

ГОСТ	Пункт	СВБУ 1.0	СВБУ 2.0	Примечание
ГОСТ Р ИСО 11064-6-2013 – Эргономическое проектирование центров управления. Требования к окружающей среде	5.4.8. Следует использовать различные частоты и уровни громкости для дифференцирования звуковых предупредительных сигналов по степени важности и источникам тревоги.	+-	+	Для СВБУ-1 дифференсация есть только, но частичная. Нет диффенсации по группам важности, технологическим подсистемам. В СВБУ-2 предлагается звуковую сигнализацию дополнить голосовым сообщением, дифференцированным с нужной степенью детализации.
ГОСТ Р МЭК 60073-2000 - Интерфейс человеко-машинный. Маркировка и обозначения органов управления и контрольных устройств. Правила кодирования информации	4.2.3.2 Частоты мигания визуальных сигналов. Приняты две частоты мигания: f1 и f2. Информация самого высокого приоритета должна передаваться с наибольшей частотой мигания. Допустимые диапазоны частот мигания следующие: -f1 — медленное мигание: 0,4 — 0,8 Гц (от 24 до 48 миг./мин); -f2 — нормальное мигание: 1,4 — 2,8 Гц (от 84 до 168 миг./мин). Если применяют только одну частоту мигания, то это должна быть частота f2. Отношение f1:f2, должно быть постоянным для данного применения и составлять от 1:2,5 до 1:5. Рекомендуется отношение 1:4 (например, частоты 0,5 и 2 Гц).		+	В СВБУ-1 не 2 частоты, а 3 – 0,5Гц, 2Гц, 8Гц. В СВБУ-2 предлагается удалить частоту 8Гц, которая используется только для обозначения хода задвижек. Использовать для этого нормальное мигание.
ГОСТ Р МЭК	5.2.5 Если рабочая	-	-	В СВБУ-2 не

ГОСТ	Пункт	СВБУ 1.0	СВБУ 2.0	Примечание
61227–2012	станция включает в себя несколько дисплеев, то система должна показывать, на каком из них курсор является активным. 5.3 Специальные требования для сенсорных панелей			предусмотрены много дисплейные рабочие станции.
ГОСТ Р МЭК 61772–2011	4.2 Опыт применения дисплеев на АС показывает, что оперативному и ремонтному персоналу необходим доступ через дисплеи рабочей станции ко всей станционной информации – как непосредственно измеряемой, так и получаемой в результате обработки данных, а также специальные средства, позволяющие отображать следующую информацию: − логические алгоритмы управления; − уставки срабатывания защиты; − уставки срабатывания сигнализации; − масштабирующие коэффициенты сигналов; − назначения входов и другие характеристики, используемые для определения качества функционирования дисплейной системы. Такие средства имеют особую значимость во время ввода станции в эксплуатацию и в процессе пуска после модернизации. 6 Разработка и внедрение экранов коллективного пользования	-+	+	В СВБУ-2 предлагается реализовать эти функции в полном объеме.
ГОСТ Р МЭК 62241–2012	8.3.1 Должны быть предусмотрены средства подавления сигнализации вручную, позволяющие	-+	+	В СВБУ-2 предлагается реализовать эту функцию в полном объеме. (Разумеется с

ГОСТ	Пункт	СВБУ 1.0	СВБУ 2.0	Примечание
	выбрать сигнал и определить требуемую функцию подавления. Должны быть предусмотрены средства, позволяющие проводить проверку, регистрацию, возврат в работу и подтверждение подавляемой сигнализации. Это эффективно реализуется в случае представления информации на экране дисплея. 8.3.2 Шумящая сигнализация Должны быть предусмотрены средства, позволяющие оператору управлять подавлением сигнализации, которая повторяется и является шумящей. С момента подавления и до момента возврата в работу соответствующие сигналы не будут вызывать никаких изменений состояния средств отображения информации, однако информация об их состоянии должна быть доступна оператору по запросу.			учетом возможностей современных проектных организаций.)
IEC 60964	П. 7.7.2.5 Для повышения безопасности, работоспособности и эффективности АС Должны быть предусмотрены функции поддержки оператора, такие как отображение параметров безопасности и контроль за функциями безопасности(см.МЭК60960); функции диагностирования АС; функции выдачи советов оператору в режимах нормальной эксплуатации послеаварийных	+-	+	В СВБУ-2 данные функции предлагается реализовать в полном объеме. (Разумеется с учетом возможностей современных проектных организаций.)

ГОСТ	Пункт	СВБУ 1.0	СВБУ 2.0	Примечание
	ситуациях, например основанные на симптомно-ориентированных и событийно-ориентированных процедурах; функции автоматического контроля энергетических режимов 7.9.1 Для повышения эффективности и безопасности АС между БПУ и другими информационными центрами желательно предусмотреть системы неречевойкоммуникации, такиекакфаксимильнаясвязьиканалыпередачиданных(между компьютерами)			

6. Жизненный цикл

До эксплуатации этапы жизненного цикла СВБУ/СВСУ/СРВПЭ первого и второго поколения совпадают.

Необходимость изменений для СВБУ/СВСУ/СРВПЭ связана с несоответствием длительностей жизненных циклов эксплуатации АЭС и электронных комплектующих СВБУ: если первая составляет 30-60 и более лет, то время жизни компонент в настоящее время составляет не более 10 лет с тенденцией к сокращению.

Выходом является перманентная модернизация, цикл которой начинается сразу после ввода в эксплуатацию и включает следующие подэтапы:

A. Исследования тенденций в развитии комплектующих,
B. Выбор технических средств на замену,
C. Подготовку модернизации,
D. Модернизацию.

Начало следующего подэтапа A должно начинаться сразу после завершения D и включать научно-исследовательскую (аналитическую) работу, которая должна позволить сделать выбор направления модернизации и определить дату ее завершения.

При вычислении даты завершения (окончания цикла модернизации) необходимо принимать во внимание недостоверность вероятностных аналитических методов определения остаточного ресурса современных электронных устройств. Взамен предлагается следующее правило: модернизация должна проводиться не позднее момента времени, когда комплектующие перестанут быть доступными.

Пояснение. Предложенное правило вполне выполнимо при условии, что взаимоотношения АЭС, поставщика СВБУ/СВСУ/СРВПЭ и производителя комплектующих носят не разовый характер, а продолжаются все время, пока эксплуатируются комплектующие. При этом ответственность за выбор поставщиков комплектующих и мониторинг их состояния должен производить поставщик СВБУ, связь которого с АЭС в форме договора о поддержке должна носить постоянный характер.

Предложенное правило позволяет производить частичную модернизацию, когда заменяются только компоненты определенных типов, например, сетевое оборудование, серверы и т.д.

Выбор технических средств на замены (подэтап B) должен производиться так, чтобы сроки последующих модернизаций были максимально сдвинуты в будущее с учетом следующих ограничений:

- поставщики комплектующих должны быть надежными и диверсифицированными,
- надежность компонент должна быть доказана практикой,
- стоимость модернизации должна находиться в разумных пределах (не более 50 процентов от стоимости СВБУ) и др.

Модернизация СВБУ/СВСУ/СРВПЭ (подэтап D) должна укладываться в ППР и занимать не более 2-х недель, включая полных комплекс автономных испытаний и испытаний совместно с АСУ ТП.

Для этого подготовка (подэтап С) должна проводиться с применением специальных стендов и устройств, включая в качестве обязательного компьютерный имитатор АСУ ТП. (Подробнее см. Приложение 4.)

7. Структура СВБУ второго поколения

7.1. Технические средства

Как и СВБУ 1-го поколения СВБУ 2-го поколения (СВБУ-2) предлагается строить на основе трех основных конструктивов:

- Рабочие станции (РС),
- Устройства серверные (УС),
- Устройства телекоммуникационные (УТК).

Но их конструкция и свойства различаются.

7.1.1 РС

РС предлагается создавать в виде неразборных самопрограммирующихся конструкций (моноблоков), в которых единственный дисплей и компоненты электроники смонтированы в виде единого прибора, который монтируется на АРМ и имеет подключение к электропитанию, сети/WiFi и ИК-порт.

Пояснение: Ремонт РС становится очень простой и безопасной операцией, в ходе которой невозможно совершить опасную ошибку или нанести умышленный вред. Это относится и к ремонтному персоналу, и ко всем остальным людям, которые имеют или могут получить доступ к РС в штатном или разобранном состоянии. Самопрограммирование означает, что моноблок самостоятельно идентифицирует свою роль в СВБУ и устанавливает нужное ПО. Для этого в него встроен сканер кодов, которые должны наноситься на корпус РС.

Для дисплеев предлагается использовать матрицы, совместимые с разрешением UHD. Размер матриц 60Х120см.

Пояснение: Матрицы данного разрешения и размера являются самыми перспективными, и в будущем будут доминировать на рынке. Разрешение и размер позволяют отображать 4 видеокадра СВБУ 1-го поколения, а именно столько находится в поле зрения операторов-технологов на действующих АЭС. На практике доказано, что этого вполне достаточно для работы операторов-технологов. Поэтому одного моноблока будет достаточно для работы любого оператора АЭС. С учетом возможности отказа одного моноблока, на АРМ необходимо и достаточно устанавливать два моноблока и не более.

Для процессорной части предлагается использовать компьютеры на одной плате (single board computer).

Пояснение. Этот вид устройств является доминирующем на рынке и вытесняет все прочие.

В качестве устройств ввода/вывода предлагается использовать беспроводные устройства типа мышь, алфавитно-цифровая и функциональная клавиатуры с ИК-интерфейсом.

Пояснение. Устройства данного типа являются наиболее надежными, дешевыми и долговечными, а ИК-связь наиболее защищенной от помех. Беспроводная связь позволяет обслуживать (чистить, дезинфицировать, тестировать) и заменять устройства чаще без помех для операторов.

7.1.2 УС

В качестве УС предлагается использовать блейд-серверы, которые могут содержать одинаковые вычислительные модули, объединенные сетевыми интерфейсами. Число модулей может насчитывать десятки с сотнями процессорных ядер.

Пояснение: Блейд-серверы позволяют оперативно наращивать мощность простым добавлением модулей без заметного влияния на уже установленные.

Модули должны быть автопрограммируемыми и их замена должна производиться без выключения УС: ПО должно загружаться в соответствии с маркировкой посадочного места без участия человека.

Пояснение: Ремонт и замена модулей представляет собой не сложную операцию, в ходе которой невозможно совершить опасную ошибку или нанести умышленный вред. Это относится и к ремонтному персоналу, и ко всем остальным людям, которые имеют или могут получить доступ к УС в штатном или разобранном состоянии.

Для процессорной части модулей предлагается использовать компьютеры на одной плате (single board computer).

См. пояснение для РС.

В качестве долговременной памяти для архивов предлагается использовать флеш-память с объемом, достаточным для надежного хранения информации в течение 10 лет.

Пояснение. Разделение на кратковременный и долговременный архивы в настоящее время не имеет смысла. Также нет необходимости копировать информацию на сменные носители. Архив будет накапливаться весь срок работы УС. Технологии RAID-массивов позволяют выявлять дефектные флеш-карты и производить их автоматическую замену с

последующей репликацией, что обеспечивает не ограниченное время хранения информации. При замене УС на ЗИП или при коренной модернизации информация может копироваться на новые устройства в полном объеме или за разумный срок (например, за 1 год).

Приборная стойка УС должна иметь ограниченное число внешних подключений: одно (два) подключения к сети электропитания и два подключения по оптоволоконной сети.

УС должен иметь:

- блок бесперебойного питания,
- датчики и контроллер несанкционированного доступа,
- внутренние коммутаторы: для основной и резервной ЛВС,
- диод данных с выходом на модем беспроводной связи,
- модуль глобального времени.

7.1.3 УТК

УТК должно включать несколько одинаковых модулей коммутаторов, каждый из которых должен иметь однотипные оптоволоконные подключения.

Модули должны быть автопрограммируемыми: ПО (настройки) должно загружаться в соответствии с маркировкой посадочного места без участия человека.

УТК должно иметь:

- одно (два) подключения к сети электропитания,
- блок бесперебойного питания,
- датчики и контроллер несанкционированного доступа.

7.1.4 Мобильные устройства

Наряду с основными в состав технических средств СВБУ 2-го поколения предлагается включать мобильные устройства типа:

- Нетбук,
- Ноутбук,
- Лэптоп,
- Планшет,
- Смартфон.

Они должны представлять собой серийные изделия в промышленном исполнении и выдерживать установленные в помещениях климатические, электромагнитные и иные неблагоприятные воздействия.

Мощность процессоров, размер и разрешение дисплеев должны выбираться исходя из особенностей применения.

В устройствах должны быть применены надежные меры защиты информации, включая электронную подпись на весь исходящий поток данных.

Устройства должны иметь ограниченный (правилами) доступ со стороны персонала и находиться в определенных местах.

Устройства должны использоваться только при выполнении служебных обязанностей.

Способ подключения – через беспроводные сети или подключения по проводным сетям.

На БПУ, РПУ устройства должны размещаться на рабочих местах, панелях управления и в других местах, где для них предусмотрены специальные способы сейсмо/виброустойчивого закрепления. А сами устройства должны быть стойкими к неблагоприятным воздействиям в случаях аварий АЭС.

7.1.5 Персональные устройства

В состав СВБУ предлагается включать устройства типа смартфон, переданные в постоянное пользование конкретным людям.

Устройства должны находиться вблизи от хозяина и в рабочее и во внеслужебное время.

7.1.6 Контактные устройства

Предлагается использовать компьютерные устройства, непрерывно прилегающие к телу человека.

К ним относятся:

- Электронные часы,
- Электронные браслеты,
- Электронные наушники,
- «Умные очки» и др.

Устройства должны иметь датчики контроля наличия контакта с человеком: измерение пульса и др.

Устройства должны иметь средства воздействия на человека с целью привлечения внимания: вибрация, звук и др.

Устройства должны иметь средства ввода команд от человека.

Пояснения: Контактные устройства являются одной из бурно развивающихся ветвей вычислительной техники. Они позволяют решать задачу контроля и диагностики состояния людей, а также дистанционно управлять людьми. Они позволяют выполнять часть работы, не совершая физических перемещений. Они позволяют значительно расширить границы рабочих мест персонала.

7.1.7 Виртуальные устройства

В СВБУ-2 предлагается использовать ПО, устанавливаемое в вычислительные среды, не относящиеся к СВБУ.

Примеры. Это могут быть программы для отображения информации для руководства АЭС, использующие офисные компьютеры АСУ управления производством. Это могут быть программы, расположенные в других организациях и получающие информацию через InterNET.

Пояснение. Включение их в СВБУ означает, что ответственность за их работу несет служба СВБУ с учетом ограничений накладываемых внешней средой. Ответственность, в частности, включает гарантии по доступности информации (при наличии связи) и ее достоверности (безусловно).

7.2. Назначение и функции

Объектом автоматизации для СВБУ-1 является АЭС в части технологического оборудования и АСУ ТП. Для СВБУ-2 в состав объектов автоматизации предлагается дополнительно включить персонал АЭС, непосредственно вовлеченный в процесс эксплуатации технологического оборудования, включая:

- оперативный персонал, имеющий доступ к технологическому оборудованию и АСУ ТП,
- ремонтный персонал,
- вспомогательный персонал (уборщики и т.п.), имеющий доступ в помещения АЭС, где расположено технологическое оборудование или АСУ ТП.

В состав пользователей СВБУ-2 предлагается добавить всех людей прямо или косвенно вовлеченных в эксплуатацию АЭС, включая:

- Оперативный персонал АЭС,
- Персонал служб АЭС,
- Руководство АЭС,
- Сотрудники служб надзорных органов,
- Сотрудники организаций, осуществляющих техническую поддержку.

Местами доступа к СВБУ-2 должны являться:

- Все помещения, где расположены РС СВБУ-1,
- Помещения АЭС, где расположено оборудование и АСУ ТП,
- Помещения служб АЭС,
- Кабинеты руководителей,
- Места коллективной работы на АЭС: залы заседаний и т.п.,
- Помещения вне АЭС,
- Места нахождения персонала.

СВБУ-2 должна выполнять все функции СВБУ-1 за исключением функции «Записи операторов», которая не востребована.

Дополнительно СВБУ-2 должна включать следующие функции:

Информационные

(1.) Контроль состава, физического состояния и местоположения оперативного персонала АЭС,

(2.) Функции системы подготовки данных (внесение изменений в ПО),

(3.) Обеспечение информацией служб АЭС,

(4.) Пассивное информирование персонала АЭС: вибрация, звук, голос

(5.) Активное (с квитирование) информирование персонала по месту нахождения,

(6.) Выдача данных по запросам со стороны внешних организаций,

(7.) Отображение информации и ведение диалога в части интеллектуальной поддержки.

Управляющие

(1.) Голосовое управление видеокадрами,

(2.) Выдача распоряжений персоналу АЭС,

(3.) Выполнение команд по блокированию и восстановлению оборудования СВБУ при наличии подозрений о кибератаках,

(4.) Автоматическое блокирование оборудования СВБУ при наличии признаков кибератак.

Диагностические

Диагностика состояния персонала по медицинским показателям: пульс, давление, физическая активность.

Вспомогательные

(1.) Временное понижение важности сигнализации.

(2.) Обеспечение многосторонней мультимедийной связи (тексты, фото, речь, видео, видеокадры, архив) между персоналом АЭС и сторонних организаций.

Информационная (интеллектуальная) поддержка персонала

(1.) Качественное моделирование для поиска причин неисправностей (объяснение сигнализации),

(2.) Советы в части оптимизации ТЭП,

(3.) Помощь в составлении планов оперативных работ,

(4.) Навигатор и составитель маршрутов для перемещений по станционным помещениям и поиску оборудования и материалов,

(5.) Оценка и советы по управлению рисками в части:

- ТЭП,
- Технологической безопасности (функций безопасности),
- Кибербезопасности.

Замечание. Авторы осознают, что приведенный материал может рассматриваться только как перечень возможных направлений работы, сформулированный учеными. Основная работа должна проводится с участием специалистов проектных и эксплуатирующих организаций.

7.3. Размещение и функции оборудования

7.3.1 БПУ

На БПУ предлагается разместить 5 РС.

Две РС для НСБ. На этих должна отображаться информация по всем технологическим системам и оборудованию, включая АСУ ТП. Должна отображаться информация о составе, состоянии и местонахождении подконтрольного персонала.

Система сигнализации РС НСБ должна позволять замечать и реагировать на аномалии в работе АЭС и операторов-технологов, и персонала ЦТАИ (сигналы высших приоритетов, несвоевременное квитирование и др.).

НА РС НСБ должны быть реализованы функции (включая управление) в объеме АТПС.

Пояснение. АРМ НСБ СВБУ-1 не требует постоянного присутствия, а используется, когда НСБ это считает нужным. СВБУ-2 расширяет список функций АРМ НСБ, но смены режима работы не предусматривает. Серьезные аномалии с АСУ ТП требуют коллективной работы с участием операторов-технологов, НСБ и персонала цеха ТАИ. Этим объясняется предоставление возможностей для работы с АСУ ТП на БПУ.

Для операторов реакторного и турбинного отделения выделяется по одной РС, через которые выполняются все функции СВБУ в части контроля и управления технологическими процессами.

И еще одна РС размещается в зоне видимости обоих операторов. Она может играть роль экрана коллективного пользования (ЭКП) или при отказе использоваться одним из операторов-технологов. (см. рис. 7.1).

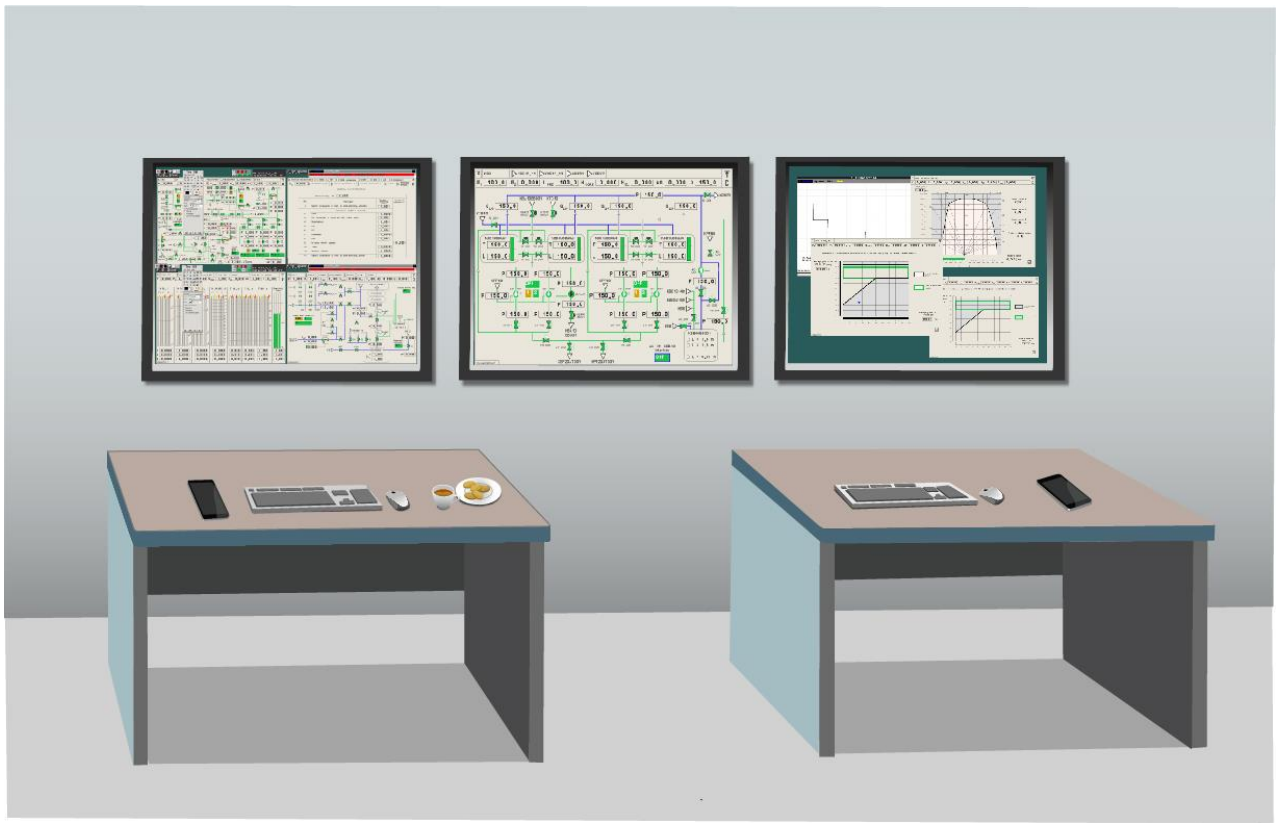

Рис.7.1 Рабочие места операторов технологов РО и ТО и ЭКП.

Пояснение. Увеличение на одной РС информационного поля более чем в 4 раза по сравнению с РС СВБУ-1 делает использование нескольких РС на одном АРМ ненужным. При этом компактность позволяет помещать общую РС в зону видимости обоих операторов. Наличие двух РС для НСБ объясняется, во-первых, тем, что его АРМ не должен терять функциональность при отказе одного устройства. Во-вторых, по распоряжениям НСБ АРМ может использоваться персоналом ЦТАИ для контроля и управления АСУ ТП. АРМ неоперативного контура (вентиляции, спецводоочистки, систем переработки РАО и других систем) в СВБУ-2 не применяются: все их функции возложены на АРМ операторов-технологов.

На БПУ должны постоянно находиться несколько мобильных устройств, которые полностью дублируют информационные функции РС АРМ операторов-технологов и подключаются в основной ЛВС по проводным линиям связи. Они должны выдаваться по распоряжению НСБ и при работе закрепляться (для стойкости к землетрясениям) на конструкциях БПУ, включая панели СБ.

Пояснение. Мобильные устройства могут использоваться для различных целей. В частности, для работы с панелями СБ. В СВБУ-1 для этого применяются отдельные РС, но очень редко и для выполнения специфических технологических процедур.

Все РС и дублирующие мобильные устройства БПУ должны быть объединены в сеть цифровой связи, через которую НСБ должен отдавать регистрируемые распоряжения операторам-технологам.

Операторы-технологи и НСБ должны работать с надетыми контактными устройствами, соединенными с РС по радио или оптическим каналам точка-точка в зоне прямой видимости. Через них автоматически должно проверяться самочувствие, контролироваться и регистрироваться местоположение (с точностью до помещения). Контактные устройства служат также для уведомления о событиях, требующих внимания и квитирования: звуком, вибрацией, речью. Контактные устройства должны принимать сигналы от человека: нажатием кнопок, вращением визиров, голосовыми командами, жестами (например, встряхиванием).

Пояснение. Широковещательная звуковая сигнализация в СВБУ-2 может быть упразднена. Контактные устройства являются более удобным средством привлечения внимания операторов. Кроме того, они позволяют эффективно (быстро, точно) реагировать на события и вводить не сложные команды по навигации при работе с АРМ. Все это позволяет операторам свободно перемещаться по БПУ, отворачиваться от дисплеев АРМ, работать стоя, выполнять физические упражнения и т.д.

Для выполнения дополнительных задач, непосредственно не связанных в управление АЭС, на рабочих местах операторов-технологов и НСБ устанавливаются служебные мобильные устройства типа планшет с большой площадью (до 20”). Через беспроводную ЛВС на БПУ с их помощью операторы технологи могут общаться (мультимедиа) с персоналом АЭС и других организаций, выходить в InterNet .

Пояснение. Мобильные устройства на рабочих местах являются заменой традиционной телефонной связи на современные средства коммуникации, обычные в быту.

Полноценная цифровая связь РС и служебных мобильных устройств предусмотрена только в одну сторону: от РС. В обратную строну (к РС) связь ограничена, позволяя передавать только текстовую информацию на ограниченном естественном языке.

Пояснение. Из-за ограничений вычислительной техники (см. 4) необходимо учитывать вероятность опасной ошибки ПО или взлома РС СВБУ через цифровые каналы. Тем не менее, иногда информация извне на РС может понадобиться. Для этого предложен простой безопасный метод, разработанный в ИПУ РАН.

7.3.2 РПУ

Состав технических средств полностью аналогичен тому, что используется на БПУ. Разница только в режиме работы: все РС находятся в выключенном состоянии и включаются автоматически только при появлении персонала с определенными полномочиями, которые определяются по многофакторной модели идентификации: по изображению, голосу и надетому контактному устройству.

*Пояснение***.** Полный аналог БПУ можно себе позволить из-за невысокой стоимости и низкого энергопотребления РС. Время запуска РС в работу не превышает 1 минуты. Поэтому нет необходимости постоянно эксплуатировать оборудование. Поскольку РС РПУ крайне редко используются операторами, но через них могут вводиться команды управления, то их защита от несанкционированного доступа должна быть и надежной и необременительной для операторов-технологов в аварийных ситуациях.

7.3.3 Помещения АСУ ТП

В помещениях СВБУ размещаются на постоянной основе УС, УТК и устройства беспроводной связи: резервированные комплекты в двух взаимно изолированных

помещениях. Доступ к ним (открывание двери, разъединение контактов) предусмотрен только для проведения регламентных работ или ремонта.

Работы с СВБУ выполняются с использованием мобильных устройств, выдаваемых сменному персоналу. В устройствах производится полное архивирования действий, которые должны проверяться при сдаче устройства на хранение.

Сменному персоналу, обслуживающему СВБУ, также должны выдаваться контактные устройства, на которые выводится сигнализация в объеме АТПС. При этом для квитирования персонал должен посетить помещение БПУ и выполнить необходимые действия на АРМ НСБ или сделать это из помещения цеха ТАИ при помощи мобильного устройства.

Пояснение. Практика показала, что персоналу очень трудно находиться на АРМ АТПС, поскольку события, требующие реакции, крайне редки. В результате персонал узнает о событиях от персонала на БПУ, перемещается к пульту АТПС и начинает работу с большим опозданием. Специфика АСУ ТП состоит в том, что реакция не обязательно должна быть мгновенной – задержка 5-10 минут допустима. После получения сигнала по контактному устройству этого вполне достаточно, чтобы дойти до помещения и начать работу.

Персонал, обслуживающий другое оборудование АСУ ТП должен иметь возможность доступа к СВБУ через мобильные устройства. Для этого помещения должны оснащаться устройствами беспроводной связи, связанные с СВБУ. Эти устройства используются для контроля измеряемых параметров, просмотра архивов и электронных документов, а также для связи с персоналом по контактным устройствам.

7.3.4 Центр технической поддержки

Для организации коллективной работы центр должен включать РС, аналогичную РС АРМ НСБ, но без функции управления АСУ ТП.

Кроме этого, в центре должен быть набор (5-10) мобильных устройств для индивидуальной работы экспертов. Устройства прикреплены к рабочим столам, подключаются к СВБУ по беспроводной связи и предоставляют доступ ко всем информационным функциям СВБУ через ЧМИ, аналогичный тому, что используется на АРМ БПУ.

Пояснение. Замечено. Что при пуско-наладочных работах, при ремонтах и т.п. наблюдается дефицит ресурсов доступа к СВБУ. Поскольку обслуживание мобильных

устройств (очистка, ремонт, замена) удобнее стационарных, то можно предоставить значительно больше устройств доступа к СВБУ.

7.3.4 Технологические помещения АЭС

В обслуживаемых помещениях АЭС предлагается разместить устройства беспроводной связи с СВБУ.

Эксплуатационный персонал должен работать с надетыми контактными устройствами, имея при себе персональные устройства.

Контактные устройства предназначены для автоматического контроля состояния и местоположения персонала в помещениях АЭС, а также для привлечения его внимания по команде НСБ.

Персональные устройства используются для обмена информацией в текстовой, видео, аудио или иной форме. Они также могут применяться для доступа (ограниченного) к информационным функциям СВБУ.

Для полного доступа к СВБУ персонал может получать во временное пользование мобильные устройства.

7.3.5 Административно-хозяйственные помещения

Для отображения оперативной информации, доступа к архивам СВБУ и коммуникации с персоналом (в текстовой, видео, аудио или иной форме) на рабочих местах руководителей и персонала служб АЭС предлагается разместить виртуальные программы-агенты СВБУ.

Программы-агенты должны загружаться из СВБУ через специальный шлюз с офисной сетью АЭС, полностью контролироваться СВБУ и обеспечивать достоверность информации.

7.3.6 Помещения вне АЭС

Для запросов оперативной информации, доступа к архивам СВБУ и коммуникации с персоналом (в текстовой, видео, аудио или иной форме) на рабочих местах специалистов организаций, которые вовлечены в эксплуатацию АЭС, предлагается разместить виртуальные программы-агенты СВБУ.

Программы-агенты должны загружаться из СВБУ через специальный шлюз с InterNET, полностью контролироваться СВБУ и обеспечивать конфиденциальность и достоверность информации.

7.3.7 На мобильных устройствах вне АЭС

В случае необходимости для коммуникации с персоналом (в текстовой, видео, аудио, вибро или иной форме) вне АЭС, на их смартфонах предлагается разместить виртуальные программы-агенты СВБУ.

Программы-агенты должны полностью контролироваться СВБУ и обеспечивать конфиденциальность и достоверность информации.

7.4. Вычислительная сеть

ЛВС СВБУ-2 имеет несколько уровней:

- Основная (технологическая) ЛВС, аналогичная по структуре СВБУ-1: дублированная оптоволоконная сеть с высокими показателями производительности, надежности и защищенности, и низкими задержками прохождения информации (доли секунды),
- Служебная ЛВС для подсоединения мобильных, персональных и контактных устройств в помещениях АЭС: множество сегментов беспроводной сети, подключенных к СВБУ.

Виртуальные логические каналы:

- внутри ЛВС АЭС для работы со службами АЭС,
- в InterNET для работы с внешними организациями,
- в телефонной сети со смартфонами персонала АЭС.

Абонентами основной сети являются:

- шлюзы с низовыми ПТК,
- СРВПЭ (2 шт.),
- РС на БПУ (5 шт.), РПУ (3 шт.), ЦТП (1 шт.),
- УС в помещениях АСУ ТП (2 шт.),
- мобильные устройства на БПУ, РПУ с разъемами для подключения к сети и ПО РС (до 10 шт.),
- СПД.

Служебная ЛВС представляет собой кластер WiFi модемов на основе оптоволоконной линии, расположенных в помещениях АЭС, включая БПУ, РПУ, ЦТП, помещения АСУ ТП и др. помещения АЭС.

Абонентами служебной ЛВС являются:

- Мобильные устройства: на БПУ (3 шт.), РПУ (2 шт.), ЦТП (до 20 шт.), и переносные (до 20 шт.),
- Персональные устройства (до 500 шт.),
- Контактные устройства (до 1000 шт.),
- УС, подсоединенное по проводной связи к оптоволоконной линии через первый внутренний коммутатор (1 шт.).

Для организации виртуальных логических каналов служебная ЛВС соединена с ЛВС АЭС и InterNet путем подключений к внутреннему второму коммутатору УС. При этом УС перенастраивается так, чтобы работа со вторым коммутатором всех процессорных модулей кроме одного была блокирована, а на одном процессорном модуле было установлено специальное шлюзовое ПО для безопасного подключения внешних абонентов к служебной ЛВС.

Виртуальные логические каналы образуются между мобильным ПО, которое должно загружаться во внешние вычислительные устройства из УС и компонентами ПО, работающими на УС или др. устройствах, подключенных к служебной ЛВС.

7.5. Подсистемы СВБУ

СВБУ имеет две подсистемы:

Подсистему контроля, управления и диагностики технологического процесса (КУДТП),

Подсистему контроля, менеджмента и коммуникаций персонала (КМКП).

КУДТП включает основную ЛВС и всех ее абонентов. В Таблице 7.1 представлены ее элементы и выполняемые ими функции.

Таблица 7.1.

Элемент КУДТП	**Функции СВБУ-1**	**Новые функции СВБУ-2**
РС оператора-технолога РО на БПУ	Все функции контроля и управления СВБУ-1 в части РО, СВО, ПЗ.	
РС оператора-технолога ТО на БПУ	Все функции контроля и управления СВБУ-1 в части ТО, ЭЧ	
РС ЭКП на БПУ	Все функции контроля и управления (при	

Элемент КУДТП	Функции СВБУ-1	Новые функции СВБУ-2
	необходимости) СВБУ-1 в части РО, СВО, ПЗ, ТО, ЭЧ	
РС НСБ (2шт) на БПУ	Все функции контроля и управления (при необходимости) СВБУ-1 в части РО, СВО, ПЗ, ТО, ЭЧ, СВБУ, АСУ ТП	Временное понижение важности сигнализации. Выполнение команд по блокированию и восстановлению оборудования СВБУ при наличии подозрений о кибератаках.
РС оператора-технолога РО на РПУ	Все функции контроля и управления СВБУ-1 в части РО, СВО, ПЗ.	
РС оператора-технолога ТО на РПУ	Все функции контроля и управления СВБУ-1 в части ТО, ЭЧ	
Мобильные устройства с разъемами для подключения к основной сети	Настройка на дублирование функций РС РО, РС ТО и РС НСБ (одно из)	
Контактные устройства операторов технологов, связанные с РС: браслеты, наушники, микрофон		Пассивное информирование о событиях от СВБУ голосом Активное (с квитированием) информирование о сигнализации: вибрация, звук, голос. Голосовое управление видеокадрами. Диагностика состояния персонала по медицинским показателям: пульс, давление, физическая активность.
УС	Все функции серверов СВБУ-1	Передача информации в КМКП.

КМКП включает служебную ЛВС, всех ее абонентов и программные агенты во внешних LAN/InterNet, порожденные и связанные с СВБУ виртуальными логическими каналами. В таблице 7.2 представлены ее элементы и выполняемые ими функции.

Таблица 7.2.

Элемент КМКП	Функции СВБУ-1	Новые функции СВБУ-2
УС	Все функции СВБУ-1.	Новые диагностические функции. Новые функции информационной (интеллектуальной) поддержки персонала.
Мобильное устройство оператора-технолога РО	Все функции контроля и СВБУ-1 в части РО, СВО, ПЗ.	Обеспечение многосторонней мультимедийной связи (тексты, фото, речь, видео, видеокадры, архив) между персоналом АЭС и сторонних организаций. Качественное моделирование для поиска причин неисправностей (объяснение сигнализации), Советы в части оптимизации ТЭП
Мобильное устройство	Все функции контроля СВБУ-1 в части ТО,	

Элемент КМКП	**Функции СВБУ-1**	**Новые функции СВБУ-2**
оператора-технолога ТО	ЭЧ	Оценка и советы по управлению рисками в части ТЭП и технологической безопасности (функций безопасности)
Мобильное устройство НСБ	Все функции контроля СВБУ-1	Все функции мобильных устройств операторов РО и ТО. Контроль состава, физического состояния и местоположения оперативного персонала АЭС, Пассивное информирование персонала АЭС, Активное (с обратной связью) информирование персонала по месту нахождения. Выдача данных по запросам со стороны внешних организаций. Выдача распоряжений персоналу АЭС. Отображение информации и ведение диалога в части интеллектуальной поддержки.
Устройство СПД (суперлэптоп с большим дисплеем и разрешением UHD)		Функции СПД.
Мобильные и персональные устройства		Обеспечение многосторонней мультимедийной связи (тексты, фото, речь, видео, видеокадры, архив) между персоналом АЭС и сторонних организаций. Пассивное информирование персонала АЭС. Активное (с обратной связью) информирование персонала по месту нахождения. Отображение информации и ведение диалога в части интеллектуальной поддержки: Навигатор и составитель маршрутов для перемещений по станционным помещениям и поиску оборудования и материалов.
Контактные устройства		Пассивное информирование о событиях от СВБУ голосом Активное (с квитированием) информирование о сигнализации: вибрация, звук, голос Диагностика состояния персонала по медицинским показателям: пульс, давление, физическая активность
Виртуальные устройства	Подмножества функций контроля СВБУ-1, скомпонованные для разных пользователей.	Обеспечение многосторонней мультимедийной связи (тексты, фото, речь, видео, видеокадры, архив) между персоналом АЭС и сторонних организаций. Подмножества новых функций, скомпонованные для разных пользователей.

На рис. 7.2 приводится понятийная схема СВБУ-2, в которой некоторые устройства (коммутаторы, диоды данных, межсетевые устройства) обозначены отдельно, хотя они входят в состав УС.

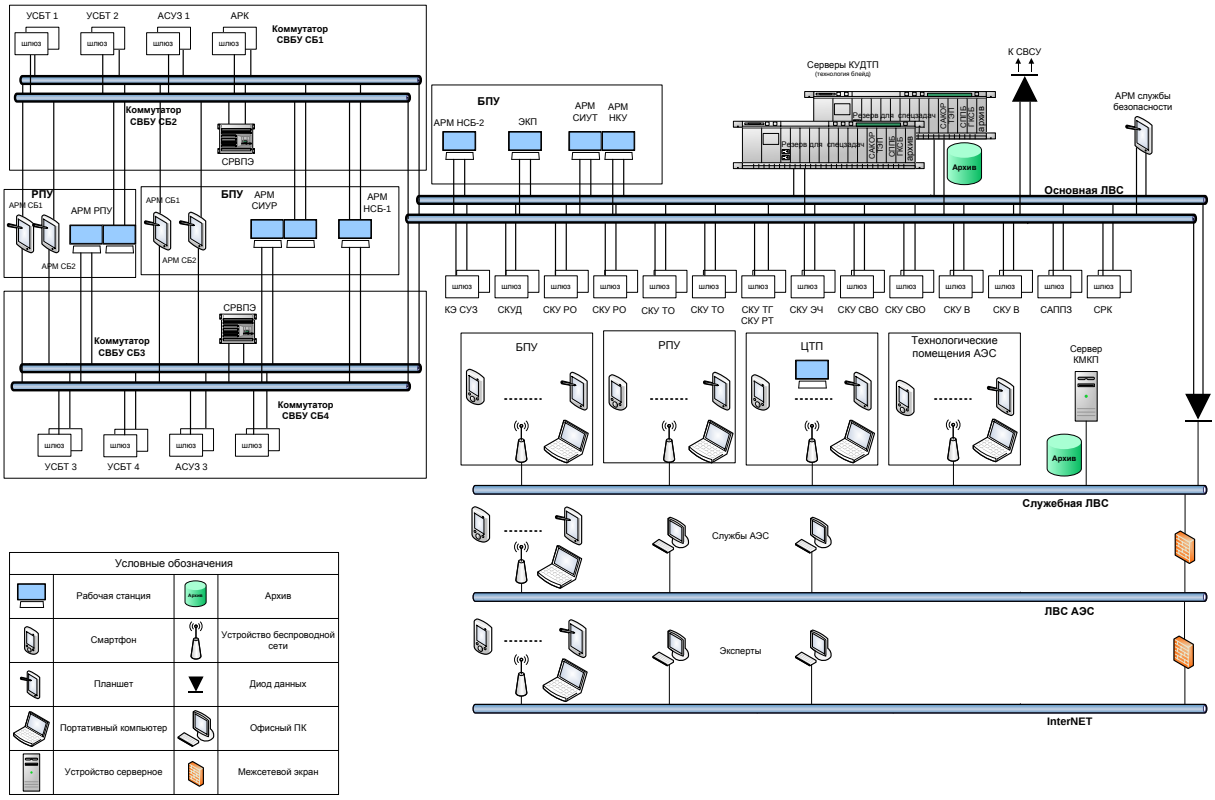

Рис. 7.2. Понятийная схема СВБУ-2

8. Человеко-машинный интерфейс

ЧМИ СВБУ-2 в части языка представления информации на экранах дисплеев и способов ввода управляющих воздействий при помощи устройств типа мышь и функциональных клавиатур аналогичен ЧМИ СВБУ-1 (Устройства типа трекбол предлагается не применять).

Предлагается использовать новые элементы и методы представления информации на экранах дисплеев:

- Форматы мнемосхем различных размеров и цветов,
- Растяжение/сжатие/перемещение мнемосхем,
- Использование мнемосхем с размерами больше экрана,
- Отображение нескольких мнемосхем (5-10) одновременно,
- Дополнение мнемосхем пометками, комментариями или пиктограммами механизмов/параметров в процессе работы,
- Создание и помещение на постоянно видимую часть рабочего стола уменьшенных копий мнемосхем (пиктограмм) для быстрого вызова,
- Сохранение и восстановление конфигураций окон,
- Всплывающие краткие информационные окна.

Для ввода текстовой и цифровой информации предлагается использовать экранные клавиатуры, настроенные на тип вводимой информации (цифры, строки из больших букв и цифр для кодов и др.) и с подсказкой при вводе (как в поисковых системах).

Звуковую сигнализацию предлагается совместить с тактильной при помощи контактных устройств для операторов: устройства будут активироваться адресно только для нужного оператора, а воздействие будет сниматься после квитирования сигнализации.

Работа с сигнализацией будет дополнена функцией понижения важности, которая позволяет временно помечать сигналы как не актуальные и исключать из протоколов сигнализации. Эта операция может быть выполнена с АРМ НСБ путем ввода команд с указанием даты отмены понижения важности и нескольких электронных подписей (НСБ и уполномоченным от руководства АЭС). По достижении даты понижение важности необходимо подтверждать в ходе специального диалога – в противном случае сигналам будет возвращена проектная группа важности.

Замечание. Данная функция является только предложением, требующим всестороннего рассмотрения и одобрения.

В ЧМИ будут добавлены средства коммуникации с персоналом, находящимися в помещении АЭС и вне его, а также с сотрудниками внешних организаций. Для различного персонала эта функция будет реализована по разному: операторы-технологи получат возможность обращаться с запросами к эксплуатационному персоналу, который будет обязан отвечать, а к ним может обращаться только НСБ; НСБ получит возможность запрашивать информацию у абонентов, подключенных к служебной сети СВБУ (включая сотрудников внешних организаций), и отдавать распоряжения всему эксплуатационному персоналу; руководство АЭС получит возможность запрашивать информацию и руководить НСБ и т.д.

ЧМИ средств коммуникации предлагается реализовывать на основе Web-технологий.

Печатные копии экранов и протоколов предлагается заменить на электронные, которые можно обрабатывать (и редактировать) на мобильных и персональных устройствах и, при необходимости, пересылать через средства коммуникации и далее по электронной почте.

Для углубленного анализа архивов предлагается использовать СУБД с языком SQL. Функция будет доступна на оборудовании ЦТП.

9. Безопасность и кибербезопасность

Кибератаки подразделяются на две большие группы: случайные и целенаправленные. Первые производятся вредоносными программами и устройствами без точного целеполагания со стороны человека. Это вирусы широкого профиля, опасные устройства и т.п. Их атаки могут нарушить выполнение штатных функций АСУ, но вряд ли смогут активизировать скрытые функции[1].

Целенаправленные атаки готовятся по правилам проведения диверсионных операций. Ставится цель нанесения вреда объекту (завод, транспорт, АЭС и т.д.) определенной величины и в определенное время. Формируется мульти дисциплинарная команда, куда входят специалисты по технологическому процессу, АСУ, профессиональные взломщики, хакеры и др. Специалисты по технологическому процессу и АСУ определяют какие штатные функции нарушить или какие скрытые активизировать, чтобы достичь вреда нужной величины. Взломщики находят уязвимости в системе физической и специальной защит, чтобы достичь точек входа в АСУ, доставить инструменты кибервзлома и т.д. Хакеры готовят ПО для взлома. Эта работа может быть очень трудоемкой и длительной. После этого проводится собственно кибердиверсия. Она может начаться мгновенно, с задержкой или ждать сигнала извне.

Проведенные оценки рисков по методике, разработанной и выполненной в ИПУ РАН, показали, что нарушения штатных функций[2] СВБУ могут привести к останову АЭС на несколько суток, но нанести оборудованию АЭС серьезный ущерб не могут.

Оценки рисков для случаев активизации скрытых функций показывают, что кибератаки на СВБУ могут привести к последовательностям ложных команд.

Для оценки последствий в ИПУ РАН не хватает специалистов и мешает еще одно обстоятельство.

Точка зрения ИПУ РАН. Исследования возможных кибератак на АЭС должны проводиться обязательно, но вестись с соблюдением строжайших мер защиты информации и только по заказу и под контролем органов государственной власти. Бес соблюдения этих условий такая деятельность представляет опасность для государства и общества.

---

[1] Скрытая функция - скрытыми функциями будем называть те, что не входят в перечень штатных функций, но могут выполняться в силу физических особенностей объекта и наличия возможности внесения изменений в программное обеспечение.

[2] Штатная функция - функция объекта является штатной, если она санкционирована в соответствии с регламентом эксплуатации, принятым для данной операции и исполняется в предусмотренном разработчиком окружении.

Кибербезопасность является частью общей задачи обеспечения безопасности АЭС и тесно переплетается с другими ее направлениями. Меры физической безопасности (заборы, пропуска, шлюзы, контроль проноса предметов и т.п.) служат незаменимыми барьерами против кибератак. Меры специальной безопасности (контроль при приеме на работу, тесты на алкоголь, контроль состояния финансов работников и т.п.) служат преградой для инсайдеров, которые могут использоваться при кибератаках. Технологические защиты оборудования - особенно построенные с использованием «жесткой логики» и принципов разнообразия - могут служить надежными барьерами против попыток разрушить оборудование или повлиять технологический процесс. И так далее.

В отличие от явлений природного характера кибератаки являются результатом деятельности людей. Пока человечество не найдет средства покончить с этой деятельностью приходится смириться с ситуацией постоянного совершенствования кибероружия и методов его применения.

С учетом этих обстоятельств, предлагается решать задачу обеспечения кибербезопасности СВБУ 2-го поколения на всем жизненном цикле следующим образом.

На этапе формирования технических требований должна быть предусмотрена специальная служба (служба киберзащиты АЭС), отслеживающая состояние киберугроз и настраивающая меры для борьбы с ними. Методом должна быть инженерная методика оценки рисков. При работе службы должны быть объединены компетенции физиков, технологов, специалистов по АСУ, защите информации, физической и специальной безопасности.

При проектировании АЭС сверху вниз службой киберзащиты должна быть проведена оценка угроз/рисков и распределена ответственность между различными участниками сооружения и службами АЭС, за противодействие каким из них каждая отвечает.

Пример. Может быть принято решение, что борьбой с инсайдерами должна заниматься служба специальной безопасности. Поэтому, персонал должен считаться доверенным и киберугрозы с его стороны не должны приниматься во внимание разработчиками оборудования АСУ. Это дает им право не использовать сложные пароли, контроль доступа к приборным стойкам и т.д. В противном случае, если персонал изначально считается не доверенным, то разработчики оборудования должны обеспечить максимальную защиту от возможных злоумышленников на АЭС.

Выбор должен производиться с учетом специфики размещения АЭС: страны, региона. Учитывая негативные тенденции в развитии общества – появление террористических идеологий, войны т.п. – для АЭС в РФ предлагается учитывать наличие среди эксплуатационного персонала инсайдеров с враждебными намерениями. Поэтому, защита СВБУ от кибератак должна строиться так, чтобы минимизировать влияние «человеческого фактора» на работу штатных функций и сделать невозможным активизацию скрытых. В терминах ИПУ РАН СВБУ это означает, что на этапе конструирования для СВБУ должен быть применен принцип киберустойчивости, описанный в Приложении 1.

Изготовление оборудования, его транспортировка, монтаж и наладка могут использоваться для внедрения закладок при подготовке кибератак в будущем. На этих этапах роль людей остается исключительно высокой. Поэтому, для их выполнения (для СВБУ-2 для АЭС в РФ) должны использоваться правила и технологии, характерные для создания военной техники.

Эксплуатация СВБУ-2 будет, по-видимому, охватывать столетие. Трудно прогнозировать на такой срок, какими будут средства кибератак, кто и как их будут применять. Поэтому, на АЭС должна быть предусмотрена служба киберзащиты, функционирующая на всем протяжении эксплуатации. Ее целью должно быть поддержание рисков на приемлемом уровне. Как и служба, работающая при проектировании, служба при эксплуатации должна привлекать разнородных специалистов, находящихся как внутри, так и за пределами АЭС.

В Приложении 2 приводится концепция вычисления киберрисков и пример ее применения для СВБУ.

10. Сопровождение и перманентная модернизация

Поскольку СВБУ-2 будет представлять собой сложный программно-технический комплекс, максимально закрытый для эксплуатации (в том числе по соображениям кибербезопасности), он будет нуждаться в постоянном техническом сопровождении со стороны разработчиков, организаций и лиц, вовлеченных в его разработку. Сопровождение должно обеспечивать поддержку разработчиков при решении плановых задач и оперативных проблем, с которыми эксплуатационный и штатный ремонтный персонал не могут справиться самостоятельно.

Сопровождение должно обеспечивать поддержку при:

- замене оборудования,
- модификации функций,
- добавлении новых элементов, связей, функций,
- модернизациях низовых систем АСУ ТП.

Сопровождение должно включать периодический аудит во время ППР и непрерывный мониторинг технического состояния с прогнозированием времени модернизации.

Периодический аудит должен проводиться в ППР и завершаться подготовкой отчета, куда должны входить:

- Перечень проверяемого оборудования,
- Информация и статистика отказов,
- Обеспеченность ЗИП,
- Выявленные проблемы.

Мониторинг технического состояния должен проводиться непрерывно путем ведения базы данных, где должны содержаться сведения об отказах за все время эксплуатации.

Сопровождение должно включать прогнозирование развития науки и техники и предоставлять варианты выбора вариантов модернизаций.

Поскольку длительность жизни электронных компонент СВБУ-2 (около 10 лет) много меньше, чем у АЭС в целом, то необходимо перманентно проводить модернизацию.

Прогнозирование времени модернизации должно производиться на основе данных аудита технического состояния и непрерывного мониторинга: на основе статистики

отказов по типам компонент должен формироваться прогноз отказов и вычисляться время исчерпания ЗИП.

Дата ближайшего планового ППР, предшествующего времени исчерпания ЗИП, должна быть указана как критический срок проведения модернизации.

Прогнозирование и развития науки и техники и формирование варианты выбора модернизации должны производиться на основе научного анализа материалов из открытых печатных изданий.

Работы должны производиться ежегодно с предоставлением отчетов Заказчику для передачи на АЭС.

Для выполнения работ по сопровождению и модернизации на этапе выдвижения технических требований к СВБУ-2 должна быть предусмотрена и далее спроектирована и разработана специальная распределенная информационная инфраструктура с элементами роботизации и интерсубъектного аудита (предложения по ее функциям и структуре см. в Приложении 3). Необходимость такой системы вытекает из фундаментальных изменений в методах решения проблем (см. Раздел. 4). Ее применение приведет к оптимизации расходов на сопровождение в общей корзине затрат на владение АЭС и повысит конкурентоспособность российских АЭС.

Поскольку перманентная модернизация на действующей АЭС влечет дополнительные расходы и риски, в том числе и для безопасности и кибербезопасности, для ее выполнения на этапе выдвижения технических требований для СВБУ необходимо предусматривать специальное инструментальное оборудование для ее модернизации (предложения по ее функциям и структуре см. в Приложении 4).

11. Влияние на ТС ОДУ

Пока СВБУ-2 работает в штатном режиме, ТС ОДУ не нужен. Но, с учетом обстоятельств, указанных в п. 4, вероятность отказов СВБУ-2 исключать нельзя и тогда нужно использовать ТС ОДУ. Таким образом, АРМ СВБУ-2 операторов-технологов РО и ТО и ТС ОДУ взаимно резервируют друг друга, а операторы-технологи остаются одними и теми же и работают либо с одним, либо с другим - и нет ситуаций, когда им нужно работать с ними одновременно.

Из этого следует, что компоновка БПУ/РПУ может быть построена так, что ТС ОДУ и АРМ СВБУ-2 будут расположены в разных местах с тем, чтобы операторы технологи перемещались бы при необходимости между ними. При этом панели ТС ОДУ могут быть гораздо компактнее (уже, ниже) и удобнее («все под рукой») для работы, чем на современных БПУ.

Приложение 1. Киберустойчивые программно-технические средства

Киберпреступления вообще и по отношению к АСУ в частности являются проявлением злой воли людей, которая постоянно совершенствуются. В этом состоит отличие от вредных явлений природного характера (вибрации, влажности, старения и. т.п.), от которых необходимо защищать программно-технические комплексы АСУ.

Изучением природных явлений и защитой от них занимаются естественные науки (фундаментальные и прикладные), а киберпреступления и защита от них традиционно относятся к сфере наук гуманитарных.

Поскольку способы мышления в технических и гуманитарных науках различаются радикально людям с инженерным образованием (мышлением) очень трудно применять методы защиты информации, разработанные специалистами по безопасности (военными, правоохранителями, экономистами и менеджерами и др.), по причинам неясности формулировок целей, субъективизма оценок, неточности критериев и т.п.

Фундамент киберзащиты закладывается на этапе выработки технических требований. С учетом того, что эти требования должны быть реализованы инженерами, предлагается применять положения теории киберустойчивости, целью создания которой была формулировка понятий кибербезопасности в форме, понятной для инженеров.

Формулировка использует понятия штатных и скрытых функций объекта управления (в нашем случае АЭС):

- Штатная функция - функция объекта является штатной, если она санкционирована в соответствии с регламентом эксплуатации, принятым для данной операции и исполняется в предусмотренном разработчиком окружении.
- Скрытая функция - скрытыми функциями будем называть те, что не входят в перечень штатных функций, но могут выполняться в силу физических особенностей объекта и наличия возможности внесения изменений в программное обеспечение.

Понятие «киберустойчивость» основано на восприятии киберпространства (понимаемое в самом широком смысле) как агрессивной среды, которая может модифицировать ПО АСУ. Критерии киберустойчивости формулируются так:

Первый критерий киберустойчивости требует, чтобы не существовало конфигураций ПО, при которых не выполняются штатные функции.

Второй критерий киберустойчивости требует, чтобы не существовало конфигураций ПО, при которых активизируются скрытые функции.

Если один или оба из критериев нарушаются, это влечет за собой угрозы материального ущерба: ущерб при нарушениях критерия I связан с неправильной работой штатных функций, а при нарушении II с активизацией не безобидных скрытых функций. При этом, в вопросе о «источниках угрозы» (хакер, инсайдер и т.п.) принимается «наихудший вариант», что это будет кто-то, обладающий всеми возможными знаниями и умениями относительно объекта управления и АСУ.

Критерий I нарушается, если имеются способы нарушения нормального выполнения штатных функций, а критерий II нарушается, если имеются способы активизации скрытых функций путем модификации ПО. Эти способы будем называть уязвимостями.

Используя так определенное понятие уязвимости, определим риск как ожидание ущерба, выраженное как возможность того, что какой-нибудь источник угрозы из киберпространства воспользуется уязвимостями системы.

Введенные определения требуют, чтобы конфигурация АСУ была неизменна, а ПО рассматривается как переменная величина. Поэтому понятия ориентировано на разработчиков ПО, оставляя задачу обеспечения целостности технических средств в компетенции служб охраны. Однако при решении задачи построения киберустойчивых АСУ выбор конфигураций оборудования играет столь же важную роль, что и выбор мер защиты информации. При этом разработчикам предоставляется максимальная свобода творчества при наличии четко проверяемых критериев достижения результата.

Методы доказательства удовлетворения критериям киберустойчивости могут быть разнообразными, но они категорически исключают применение проприетарного ПО в АСУ («черных ящиков»). ПО должно подвергаться специальным процедурам верификации на наличие не документированных включений и функций в соответствии с российскими и международными стандартами: ГОСТ Р МЭК 60880-2010, ГОСТ Р МЭК 62138-2010, ГОСТ Р 51188-98, ГОСТ Р ИСО/МЭК 27004-2011, ГОСТ Р ИСО/МЭК 25040-2014, ГОСТ Р ИСО/МЭК 12207-2010, ГОСТ Р ИСО/МЭК 15026-2002, IEEE Std. 1012-2012.

Требование киберустойчивости предлагается использовать при конструировании оборудования АСУ, дополняя их требованиями по физической защите от не санкционированного доступа. Это не решает задачу киберзащиты АСУ полностью, но создает фундамент для ее решения (методы решения на основе управление рисками приводятся в Приложении 2).

Приложение 2. Концепция вычисления киберрисков

При разработке нормативных документов по защите информации (ИБ) для систем управления объектами промышленности возникает проблема их встраивания в общую систему мер обеспечения безопасности. Один из подходов состоит в том, что ИБ АСУ должна быть обособлена. Из этого вытекают, в частности, такие следствия как требования по созданию специализированных подсистем, организационных структур, которые занимаются исключительно ИБ АСУ. «Зеркальный» подход состоит в том, что отдельные меры по обеспечению ИБ АСУ включаются в уже имеющиеся бизнес-процессы: обеспечение качества, надежности, функциональной безопасности, физической защиты, экономической эффективности и др. Следствием этого является дополнительные работы на этапах создания и дополнительная нагрузка на эксплуатационный персонал при эксплуатации.

На практике применяются смешанные решения с подавляющим преобладанием второго подхода. Это происходит главным образом (но не только) потому, что указанные выше бизнес-процессы носят более общий характер по сравнению с обособленными ИБ АСУ и поэтому распространяются и на нее как на составную часть АСУ.

ИБ АСУ можно с достаточной степенью общности понимать, как систему дополнительных барьеров, которые действуют совместно с другими (физической защитой, технологической защитой, защитой труда и т.п.) для того, чтобы исключить аварии. При этом барьеры ИБ АСУ ориентированы на специфические сценарии умышленного или злонамеренного нанесения вреда: через изменение системы управления воздействовать на технологическое оборудование с тем, чтобы активизировать опасную особенность технологического процесса и вызвать аварию.

Практики справедливо указывают, что барьеры, установленные для других целей (например, для физической, технологической защиты и др.) служат также барьерами ИБ АСУ.

Если АСУ изолирована, то для атаки на нее необходим человек, готовый стать нарушителем. Тем самым нужно воспользоваться уязвимостью в системе работы с персоналом. Нарушителем может быть посторонний или работник: пользователь АСУ, штатный обслуживающий персонал, временно командированный или другой, не связанный с АСУ. Постороннему необходимо воспользоваться уязвимостями в системах охраны внешнего периметра объекта, пропускной системы, досмотра личных вещей и/или приемке грузов, охраны помещений внутри объекта, надзора за выполняемыми работами.

Для работника, в зависимости от полномочий, возможно, понадобится только часть их этих уязвимостей.

П2.1. Барьеры ИБ АСУ

Если АСУ не изолирована, то атаку может производить человек или робот через внешние связи, используя уязвимости в межсистемных соединениях.

На рис. П2.1 представлены основные барьеры, препятствующие кибератакам, виды нарушителей и стрелками сценарии основные типы кибератак на АСУ ТП АЭС. Типизация сценариев (Н1-Н6) проведена по числу и последовательности преодолеваемых барьеров.

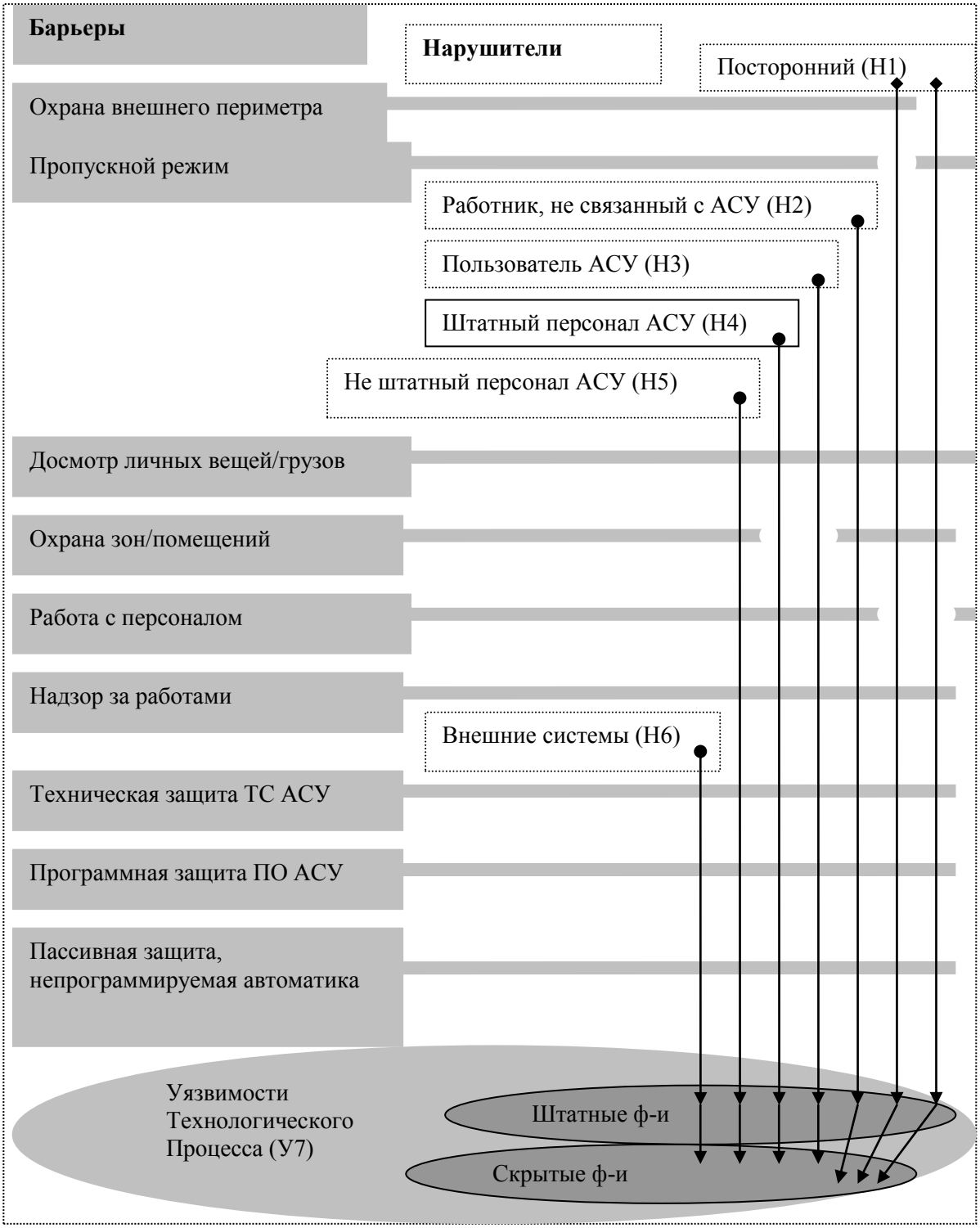

Рис. П2.1.

П2.2. Шкала возможных ущербов

Процедуры оценки рисков [ISO/IEC 27005, информационные технологии, методы обеспечения безопасности, управление рисками информационной безопасности требуют определения шкалы ущербов, связанных с работой объекта, которые обладают

спецификой. В частности, для атомных электростанций (АЭС) существуют два вида ущербов. Первый связан с нарушением ядерной безопасности, которая имеет абсолютный приоритет и не сводится только к экономическим категориям. Второй вид – это экономический ущерб, который для АЭС, как объекта электрогенерации с фиксированной мощностью, удобнее оценивать в часах (днях) простоя.

Для ущербов первого вида воспользуемся Международной шкалой ядерных событий (INES, сокр. International Nuclear Event Scale), которая включает следующие уровни инцидентов на АЭС (см. табл. П2.1).

Таблица П2.1

Уровень по шкале INES	**Критерии оценки безопасности**			**Примеры событий[1]**
	Население и окружающая среда	**Радиологические барьеры и контроль**	**Глубокоэшелонированная защита**	
Уровень 7. Крупная авария	Сильный выброс (радиологический эквивалент более нескольких десятков тысяч ТБк I-131): тяжёлые последствия для здоровья населения и для окружающей среды			Авария на Чернобыльской АЭС, СССР, 1986 год Авария на АЭС Фукусима-1, Япония, 2011 год
Уровень 6. Серьёзная авария	Значительный выброс (радиологический эквивалент более нескольких тысяч ТБк I-131): требуется полномасштабное осуществление плановых мероприятий по восстановлению			Авария на ПО «Маяк», СССР, 1957 год
Уровень 5. Авария с риском для окружающей среды	Ограниченный выброс: требуется частичное осуществление плановых мероприятий по восстановлению	Тяжёлое повреждение активной зоны и физических барьеров		Авария на АЭС Три-Майл-Айленд, США, 1979 год Авария в Уиндскейле, Великобритания, 1957 год
Уровень 4. Авария без значительного риска для окружающей среды	Минимальный выброс: облучение населения в пределах допустимого	Серьёзное повреждение активной зоны и физических барьеров; облучение персонала с летальным исходом		Авария на ядерном объекте Токаймура, Япония, 1999 год Авария на Сибирском

Уровень по шкале INES	Критерии оценки безопасности			Примеры событий[1]
	Население и окружающая среда	Радиологические барьеры и контроль	Глубокоэшелонированная защита	
				химическом комбинате 1993 год
Уровень 3. Серьёзный инцидент	Пренебрежительно малый выброс: облучение населения ниже допустимого предела	Серьёзное распространение радиоактивности; облучение персонала с серьёзными последствиями	Аварию удалось предотвратить, но для этого пришлось задействовать все исправные системы безопасности. Также: потеря, похищение или доставка не по адресу высокоактивного источника	Пожар на АЭС Вандельос, Испания, 1989 год
Уровень 2. Инцидент		Значительное распространение радиоактивности; облучение персонала за пределами допустимого	Инцидент с серьёзными отказами в средствах обеспечения безопасности	Многочисленные события
Уровень 1. Аномальная ситуация			Аномальная ситуация, выходящая за пределы допустимого при эксплуатации	Многочисленные события
Уровень 0. Событие с отклонением ниже шкалы	Отсутствует значимость с точки зрения безопасности			Многочисленные события

Формальным критерием обеспечения ядерной безопасности является недопущение инцидентов выше 1-го уровня. При этом инциденты уровней 0 и 1 могут быть связаны с экономическим ущербом. Предлагается шкала возможных ущербов (табл. П2.2), которые нужно рассматривать при анализе рисков ИБ АСУ ТП.

Таблица П2.2. Шкала ущербов (ШУ)

Уровень ущерба	Описание	Примеры
0 (M)	Поломка оборудования, включая АСУ ТП, без влияния на генерацию электроэнергии АЭС с экономическими потерями M руб.	Многочисленные примеры, фиксируемые в сменных журналах АЭС,
1(N)	Останов энергоблока АЭС на N часов приводит к большим экономическим потерям из-за простоя	Многочисленные примеры, фиксируемые в Концерне Росэнергоатом

Уровень ущерба	**Описание**	**Примеры**
2(N)	Останов более 2-х энергоблоков АЭС на N часов приводит к очень большим экономическим потерям из-за простоя и выхода из строя региональной системы электроснабжения.	Инцидент на Ростовской АЭС в ноябре 2014г.
3(D)	Авария уровня 0 по шкале INES с разрушением основного оборудования АЭС, ремонт которого требует D дней ремонта. Приводит к очень большим экономическим потерям из-за простоя, ремонта и необходимости адаптации к потере генерирующей мощности в региональной системе электроснабжения.	Останов 1-го блока ЛАЭС из-за проблем с графитовой кладкой
4	Событие уровня 1 по шкале INES.	См. таблицу 1.1.2
5	Событие уровня 2-7 по шкале INES.	См. таблицу 1.1.2

Принимается, что шкала образует абсолютный порядок: чем выше номер – тем выше ущерб, если два ущерба имеют один номер, то порядок определяется по числу приписанных часов, дней, рублей.

В предложенной шкале приводятся только возможные ущербы, которые могут произойти после принятия АЭС в эксплуатацию. Ущербы, которые могут понести разработчики и подрядчики при строительстве АЭС, не рассматриваются.

Для других объектов других видов, несомненно, должны применяться другие шкалы:

Формализованный способ управления рисками ИБ.

Поддержание уровня ИБ АСУ включает два процесса, указанные на рис. П2.2, куда как составная часть входит оценка рисков.

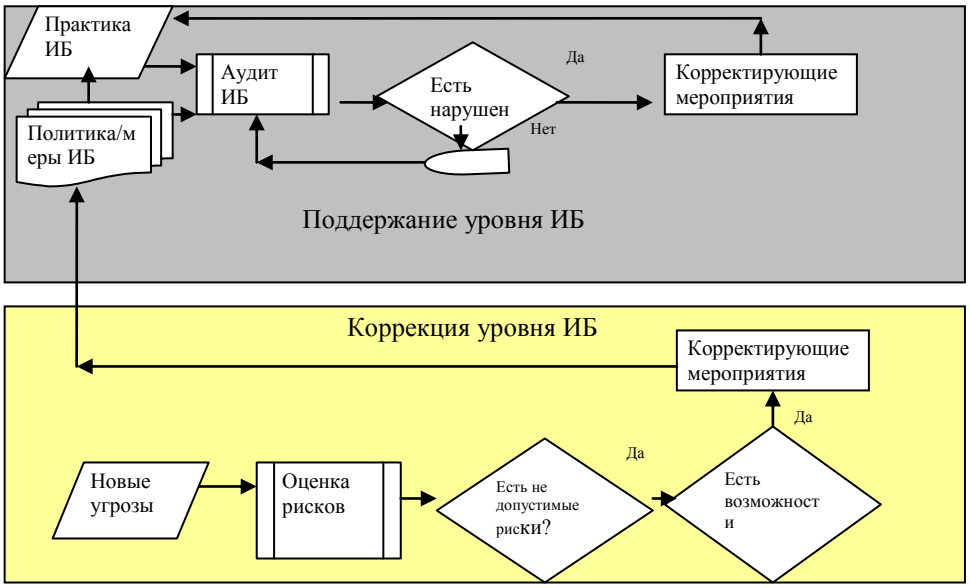

Рис. П2.2. ЖЦ ИБ при эксплуатации

На рис.П2.3 представлена упрощенная блок-схема алгоритма расчета рисков на примере АСУ ТП АЭС.

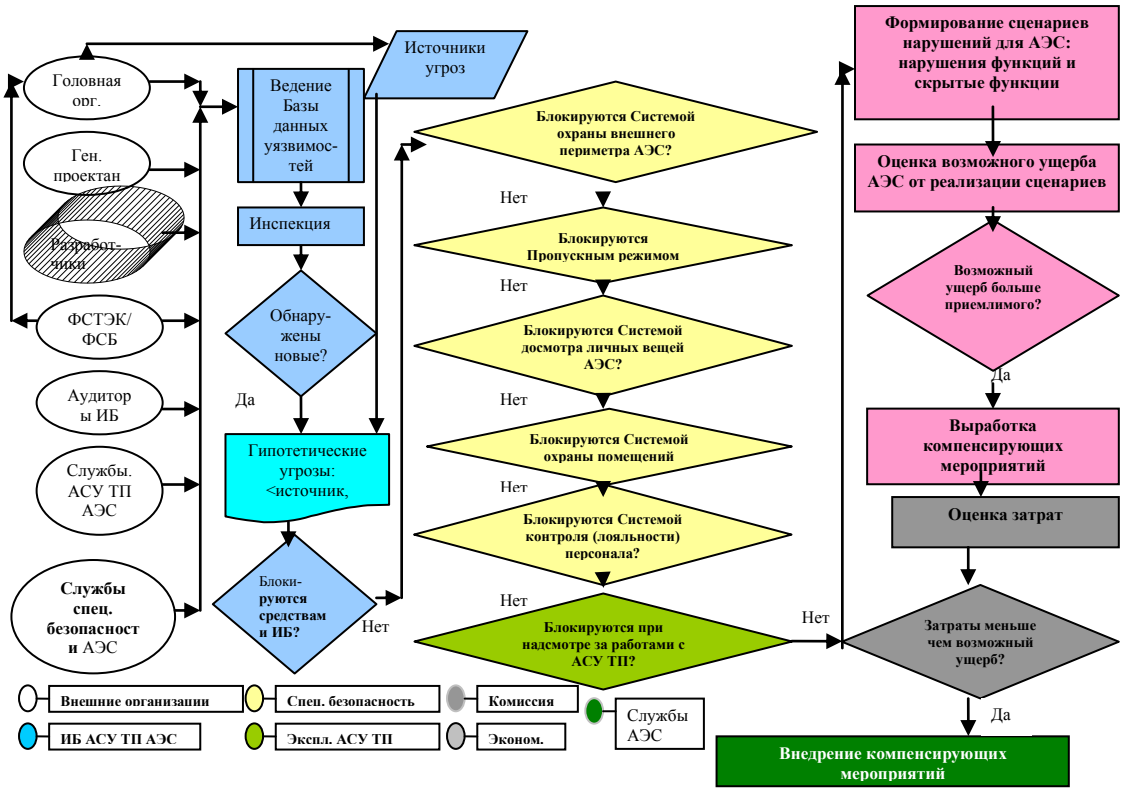

Рис. П2.3. Управление риском ИБ в АСУ ТП АЭС

Информация об уязвимостях поступает в Подразделение ИБ АСУ ТП АЭС из различных источников (часть из низ указана на рис. П2.3) в формализованном виде с атрибутами, которые должны включать следующие:

(1.) Описание уязвимости (обязательно);

(2.) Наименование системы автоматики или Код изделия;

(3.) Ссылка на уязвимость в базе ФСТЭК или ином источнике;

(4.) Производитель оборудования (обязательно);

(5.) Дата выпуска изделия;

(6.) Наличие подтверждения от производителя;

(7.) Характер возможного нарушения ИБ (доступность, целостность, конфиденциальность);

(8.) Сведения о применении;

(9.) Рекомендуемые меры компенсации.

После поступления должна проверяться достоверность сведений об уязвимостях: то, что они касаются установленного на АЭС оборудования, что они ранее не были компенсированы и т.п. Если отсутствуют необходимые сведения, то они должны запрашиваться у производителя оборудования. В результате сведения заносятся в Базу данных уязвимостей (БДУ) и им присваивается статут «Требует рассмотрения», или «Требует рассмотрения немедленно», если имеются сведения о применении уязвимостей на АЭС.

Инспекция БДУ должна проводиться сразу же после появления уязвимости со статусом «Требует рассмотрения немедленно» или раз в месяц (квартал). Инспекция состоит в том, что из базы выбираются все уязвимости с указанными статусами и запускается процессы реагирования, которые проводятся с участием специалистов различных подразделений АЭС: Подразделение ИБ АСУ ТП АЭС, Отдел специальной безопасности, Отдел кадров, Отдел охраны и др. подразделениями, выполняющими охранные функции (на рис. П2.3 указаны не все, и на реальный АЭС названия и состав могут отличаться), подразделения обслуживающие АСУ ТП, технологические подразделения и др. при необходимости.

На основе новых уязвимостей, списка актуальных источников угроз (формируется ФСТЭК/ФСБ и рассылается на АЭС через головную организацию или напрямую) формируются тройки (источник угрозы, уязвимость, программно-технический комплекс (ПТК) АСУ ТП АЭС) для дальнейшего анализа.

Далее производится проверка возможности применения каждым источником угрозы каждой новой уязвимости для нарушения ИБ (доступности, целостности и конфиденциальности) соответствующих ПТК АСУ ТП АЭС с учетом мер информационной и прочих видов безопасности, действующих на АЭС.

Если найдутся источники угрозы, которые способны преодолеть все меры всех видов безопасности и применить новые уязвимости к ПТК АСУ ТП АЭС, то далее рассматриваются возможные сценарии нанесения вреда АЭС. Для этой работы привлекается специальная комиссия из специалистов разного профиля. При необходимости могут привлекаться представители разработчиков АСУ ТП и ПТК АСУ ТП, специалисты по ИБ и прочих организаций. В сценариях должны рассматриваться отказы штатных функций АСУ ТП АЭС (диагностируемые), искажения выполнения штатных функций (не или сложно диагностируемые), активизация скрытых функции, в состав которых входят ложные команды управления, информационные атаки на смежные ПТК и др.

Далее применяется стандартная схема управления рисками: оценка возможного ущерба по шкале, пример которой приведен выше, сравнение с допустимым уровнем; выработка компенсирующих мероприятий; оценка затрат на их реализацию; оценка финансовых возможностей и внедрение.

П2.3. Проект КАЛЬКИБЕР

На основе описанного выше метода в ИПУ РАН был создан программный продукт «Калькулятор кибербезопасности» (КАЛЬКИБЕР).

Структурная схема КАЛЬКИБЕРа показана на рис. П2.4 и включает следующие основные блоки:

- Блок ввода исходных данных,
- Программу расчета,
- Блок формирования результатов анализа угроз и расчета рисков и ИБ АСУ.

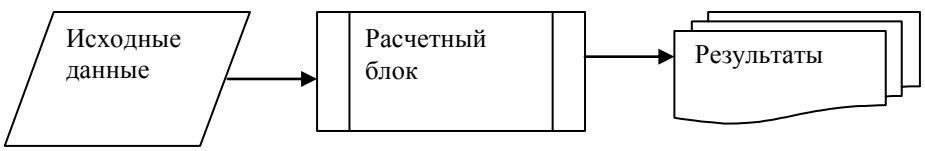

Рис. П2.4. Блок-схема КАЛЬКИБЕР

Один цикл использования КАЛЬКИБЕРа состоит в последовательном вводе исходных данных, настройке и запуске программы расчетов, ожидании и экспертном анализе результатов. Меняя исходные данные, и многократно применяя цикл можно производить моделирование ситуаций, подбор мер ИБ для достижения приемлемых рисков. КАЛЬКИБЕР может быть встроен в алгоритмы мониторинга и управления ИБ.

П.2.3.1. Исходные данные

Исходные данные включают следующие таблицы:

(1.) Таблица наименований помещений (см. пример на рис. П2.5),

(2.) Таблица перечня нарушителей (см. пример на рис. П2.6),

(3.) Таблица типов барьеров (см. пример на рис. П2.7),

(4.) Таблица типов оборудования (см. пример на рис. П2.8),

(5.) Таблица элементов оборудования (см. пример на рис. П2.9),

(6.) Таблица перечня функций (см. пример на рис. П2.10),

(7.) Таблица атак (см. пример на рис. П2.11),

(8.) Таблица защит на уровне предприятия (см. пример на рис. П2.12),

(9.) Таблица защит помещений (см. пример на рис. П2.13),

(10.) Таблица типовых защит оборудования (см. пример на рис. П2.14),

(11.) Таблица индивидуальных защит (см. пример на рис. П2.15).

Следует подчеркнуть, что задача выявления всевозможных способов проведения кибер атак сложна даже для не больших систем типа СВБУ. Для информационной поддержки работы по составлению таблицы атак (рис. П2.11) разработана специальная технология качественного моделирования взаимосвязей в АСУ. В настоящее время она доступна для ознакомления и опробования на сайте omole.ws.

	Обозн.	*Описание*	*Подтв. док.*
1	БПУ	Пульт управления	Схема размещения
3	Кабельная	Спец.помещения для прокладки кабеля	План прокладки кабеля
6	Серверная	Охраняемое помещение для размещения оборудования АСУ	План размещения

Рис. П2.5. Перечень помещений

	Обозн.	*Описание*	*Подтв. док.*
1	Посторонний	Человек, который имеет доступ к оборудованию, но не обучен работе с ним, не имеет злых намерений	Полетыкин

	Обозн.	*Описание*	*Подтв. док.*
6	Разгильдяй	Персонал, который может допускать неумышленные ошибки при работе	Полетыкин
7	Террорист	Посторонний, занимающийся диверсиями	Полетыкин
8	Вред_ОБ	Вредоносное оборудование, замаскированное под штатное	Полетыкин
9	Вред_ПО	Замаскированное вредоносное ПО	Полетыкин
10	Вредитель	Персонал, который может совершать умышленные вредоносные действия	Полетыкин

Рис. П2.6. Виды нарушителей

	Обозн.	*Описание*	*Подтв. док.*
2	ФизЗ	Физическая (заводская) защита оборудования	ТУ
7	Пропуск	Система пропускного режима на территорию и в помещения	Положение о пропускном режиме
9	Видео	Система видеонаблюдения	Схема размещения и порядок работы видеокамер

Рис. П2.7. Перечень барьеров ИБ

	Обозн.	*Описание*	*Подтв. док.*
1	АРМ	Приборная стойка или комплекс для работы персонала	ТУ на ПТС рабочих станций
2	Коммутаторы	Приборные стойки коммутационного оборудования, реализующие сетевой доступ	ТУ на ПТС коммутаторов, схема ЛВС
3	ЛВС	Линия цифровой связи	_
4	Принтер	Печатающее устройство общего назначения	Док. фирмы-изготовителя
5	Сервер	Приборная стойка сервера	ТУ на ПТС сервера

Рис. П2.8. Перечень типов оборудования

	Обозн.	*Тип*	*Размеще-ние*	*Описание*	*Подтв. док.*
9	АРС	Уникальное	Серверная	Приборная стойка с DAT, USB, ресивером GPS/Глонасс. Используется для ввода информации и ПО извне.	ТУ
10	Комм_ИУН1	Коммутаторы	Серверная	Коммутатор основной сети ИУН	РЭ
14	Комм_РО1	Коммутаторы	Серверная	Коммутатор основной сети РО	РЭ
19	ЛВС1	ЛВС	Кабельная	Линии основной ЛВС	КД
20	ЛВС2	ЛВС	Кабельная	Линии резервной ЛВС	КД

	Обозн.	*Тип*	*Размеще-ние*	*Описание*	*Подтв. док.*
21	Принтер_АТПС	Принтер	Серверная	Принтер для операторов - системых администраторов	РЭ

Рис. П2.9. Перечень элементов оборудования

	Обозн.	*Тип*	*Макс. ущерб*	*Описание*	*Подтв. док.*
1	Архивирование	state	500	Запись информации о тех. процессе в архивных файлах	ТУ
2	Искажение_арх	hidden	500	Искажение информации в архивных файлах	Полетыкин
3	Искажение_контр	hidden	2000	Искажение информации, используемой операторами для оперативного управления	Полетыкин
4	Искажение_при_печати	hidden	200	Искажение распечаток	Полетыкин
5	Контроль	state	1000	Контроль за тех. процессом	ТУ
6	Ложн_команда	hidden	3000	Выдача ложных команд в нижний уровень	Полетыкин
7	Управление	state	1000	Управление тех. процессом	ТУ

Рис. П2.10. Перечень функций: state – штатная, hidden – скрытая, ущерб в условных единицах

	В оборудовании (или во всех элементах указанного типа)	*повредить/ изменить*	*чтобы отказала/активировалась функция*
1	АРМ	soft_hard	ALL
2	АРС	soft_hard	ALL
3	Коммутаторы	hardware	ALL
4	ЛВС	hard_d flow	ALL
5	Принтер	hardware	ALL
10	Сервер	soft_hard	ALL

Рис. П2.11. Описание направлений атак

	Барьер	*Защищает от возможных воздей-ствий на*	*Со стороны наруши-теля*	*С достовер-ностью*	*Комментарий*	*Подтв. док.*
4	ФизЗ	hardware	Террорист	medium	Меры ИБ не позволяют вносить изменения в оборудование человеку без прав и спец. паролей	Процеду-ры доступа к оборудова нию
6	ИБ	software	Террорист	medium	Меры ИБ не позволяют изменять	Процеду-ры ИБ

	Барьер	*Защищает от возможных воздей-ствий на*	*Со стороны наруши-теля*	*С достовер-ностью*	*Комментарий*	*Подтв. док.*
					ПО человеку без прав и спец. паролей	
9	Ограж-дение	soft_hard_d flow	Террорист	medium	Ограждение и пропускные пункты не содержат изъянов и защищают от проникновения и проноса вредоносного оборудования и ПО	Положе-ние об охране внешнего периметра
10	Про-пуск	soft_hard_d flow	Террорист	medium	Пропуск выдается по предъявлению справки допуска формы 3 и выше, выданной 1-м отделом	Положе-ние о пропуск-ном режиме

Рис. П2.12. Защита предприятия

	Барьер	*Защищает оборудование в помещении*	*От возможных воздействий на*	*Со стороны нарушителя*	*С достоверностью*	*Комментарий*	*Подтв. док.*
1	ФизЗ	ЛКЦ	soft_hard_d flow	Посторонний	high	Помещение закрыто для доступа без охраны	Положение об охране
5	Пост	ЦТП	soft_hard_d flow	Посторонний	high	Помещение охраняется человеком	План размещения
6	Пост	ЦТП	soft_hard_d flow	Террорист	high	Помещение охраняется человеком	План размещения
13	Пропуск	БПУ	soft_hard_d flow	Посторонний	medium	Вход в помещения только для людей с допуском	Положение об охране на БПУ
26	Сопровождение	БПУ	soft_hard_d flow	Террорист	high	Вход в помещения только для посторонних людей только в сопровождении персонала с допуском	Положение об охране на БПУ
27	Видео	БПУ	soft_hard_d flow	Посторонний	high	Видеоконтроль за действиями на БПУ	Положение об охране на БПУ

Рис.. П2.13. Защита помещений

	Барьер	*Защищает оборудование данного типа*	*От возможных воздействий на*	*Со стороны нарушителя*	*С достоверностью*	*Комментарий*	*Подтв. док.*
1	ФизЗ	soft_hard_d flow	Коммутаторы	Посторонний	high	Металлический шкаф с ключом	РЭ ПТС
3	ФизЗ	soft_hard_d flow	Принтер	Вредитель	medium	Заводская защита, ограниченные возможности для настройки, пароль	ЭД
15	Пломбирование	hardware	ALL	Вред_ОБ	medium	НОВОЕ. Пломбирование упаковок с запасными частями	ЭД

Рис. П2.14. Физическая (заводская) защита

	Барьер	*Защищает оборудование*	*От возможных воздействий на*	*Со стороны нарушителя*	*С достоверностью*	*Комментарий*	*Подтв. док.*
8	ФизЗ	Принтер_ИУН	soft_hard_dflow	Вред_ПО	high	Отсутствие необходимости обслуживания ПО	РЭ
15	ФизЗ	ALL	soft_hard_dflow	ПТК_ТПТС	high	Шлюз с ТПТС представляет собой однозадачную программу, передать код вредоносной программы или данные невозможно ни в одном направлении	ПД на шлюз с ТПТС
20	ИБ	АРМ	soft_hard_dflow	Террорист	high	Диагностика событий ИБ с выводом сигнализации на пульт АТПС	РЭ
26	ИБ	Сервер	soft_hard_dflow	Разгильдяй	high	Диагностика событий ИБ с выводом сигнализации на пульт АТПС	РЭ
29	ИБ	Спутник	soft_hard_dflow	ANY	high	Диагностика событий ИБ с выводом сигнализации на пульт АТПС	РЭ
30	ИБ	АРМ	soft_hard_dflow	ANY	high	Диагностика событий ИБ с выводом сигнализации на пульт АТПС	РЭ
32	ИБ	Сервер	soft_hard_dflow	ANY	high	Диагностика событий ИБ с выводом сигнализации на пульт АТПС	РЭ
46	Сопровождение	АРС	soft_hard_dflow	Вредитель	medium	НОВОЕ. Ввести в регламент охраны контроль всех работ, связанных с остановами ПО АРС	РЭ

Рис. П2.15. Защита отдельного оборудования

Параметрами расчета рисков являются константы, задающие число барьеров, которые препятствуют кибератакам: одни задают число барьеров, которое считается достаточным для полной защиты, вторые – число барьеров, которые делают атаку маловероятной, третьи - число барьеров, которые делают атаку вероятной.

П2.3.2. Выходные данные

Результаты расчетов выводятся в виде двух таблиц:

(12.) Таблицы рисков (см. пример на рис. П2.16),

(13.) Таблицы угроз (см. пример на рис. П2.17).

N	*Возможная величина ущерба*	*От атаки нарушителя*	*Путем воздействия на*	*Оборудования*	*Достоверность*	*Нарушается штатная ИЛИ активируется скрытая функция*	*Стат. действ. барьеров*
1	200	ПТК_СУЗ, Разгильдяй, Вредитель, ПТК_СКУД, ПТК_СРК	data flow	Принтер_АТПС	high	Искажение_при_печати	high-0, medium-1, low-0
2	200	ПТК_СУЗ, ПТК_СКУД, ПТК_СРК	data flow	Принтер_ТО, Принтер_РО, Принтер_ИУН	high	Искажение_при_печати	high-0, medium-1, low-0
3	200	Разгильдяй	data flow	Принтер_ТО, Принтер_РО, Принтер_ИУН	medium	Искажение_при_печати	high-0, medium-2, low-0
4	8200	ПТК_СКУД, ПТК_СРК, ПТК_СУЗ, Вред_ПО	software	АРС	medium	Архивирование, Икажение_арх, Икажение_контр, Искажение_при_печати, Контроль, Ложн_команда, Управление	high-0, medium-2, low-0
5	8200	Вредитель	software	Сервер_РО2, Сервер_РО1, Сервер_общ, АРМ_АТПС, Сервер_ИУН2, Сервер_ИУН1, Сервер_ТО2, Сервер_ТО1	medium	Архивирование, Икажение_арх, Икажение_контр, Искажение_при_печати, Контроль, Ложн_команда, Управление	high-0, medium-2, low-0
6	8200	Вредитель	hardware	Сервер_РО2, АРС, Сервер_РО1, Сервер_общ, АРМ_АТПС, Сервер_ИУН2, Сервер_ИУН1, Сервер_ТО2, Сервер_ТО1	medium	Архивирование, Икажение_арх, Икажение_контр, Искажение_при_печати, Контроль, Ложн_команда, Управление	high-0, medium-2, low-0

Рис. П2.16. Риски: Риск отсутствует, если угрозе противостоят не менее 1 барьеров с достоверностью high ИЛИ не менее 3 барьеров с достоверностью не ниже medium. Достоверность = medium, если угрозе противостоят не менее 2 барьеров с достоверностью не ниже medium.

N	*Нарушитель*	*Оборудование*	*Объект атаки*	*Цель атаки - функция*	*Ущерб*	*Действующие барьеры*
1	Посторонний	АРМ_РО	software	Икажение_контр	2000	АРМ-ИБ-high, БПУ-Видео-high, БПУ-Сопровождение-high, БПУ-Пропуск-medium, PLANT-ИБ-medium, АРМ_РО-ИБ-high,
9	Террорист	АРМ_РО	software	Ложн_команда	3000	АРМ-ИБ-medium, БПУ-Видео-medium, БПУ-Сопровождение-high, БПУ-Пропуск-medium, PLANT-Пропуск-medium, PLANT-Ограждение-medium, PLANT-ИБ-medium, АРМ_РО-ИБ-high,
13	Вред_ОБ	АРМ_ТО	hardware	Икажение_контр	2000	АРМ-Пломбирование-medium, АРМ_ТО-ИБ-high,

Рис. П2.17. Угрозы

П2.3.3. Описание алгоритма

Алгоритм расчета угроз состоит в том, чтобы построить всевозможные способы атак со стороны нарушителей на штатные функции и скрытые функции с учетом таблицы физически возможных видов атак, составленной разработчиками АСУ (рис. П2.10). Атака на штатные функции (обозначены state на рис. П2.9) должна приводить к их отказу – атака на скрытые функции (обозначены hiden на рис. П2.9) к их активизации.

После создания перечня возможных угроз производится анализ, какие из барьеров могут служить препятствием для той или иной атаки: сводка результатов выводятся в правый столбец таблицы угроз, а в по результатам формируется таблица рисков, в которой суммированы величины возможных ущербов.

Приложение 3 Формализованные средства электронной коммуникации СВБУ-2

П3.1. Назначение

Формализованные средства электронной коммуникации предназначены для обеспечения высоких показателей качества и оперативности работы по сопровождению/модернизации СВБУ-2 (эти же средства могут применяться и для сопровождения и других систем АСУ ТП).

П3.2. Автоматизируемые функции сопровождения

1. Контроль внесения изменений,
2. Оказание помощи в случае нештатных ситуаций, включая
   - отказ ПО серверов СВБУ-2 - среднесрочно (если единичный), срочно (если массовый),
   - отказ ПО РС СВБУ-2 - среднесрочно (если единичный), срочно (если массовый),
   - отказ ПТС СВБУ-2, приводящий к сбоям в ПО - почти не срочно, т.к. такой отказ на единичном ТС не влечет обвала системы,
   - пожелания, дополнения, мелкие недочеты - нет срочности.
3. Помощь в случаях потери информации на машинных и бумажных носителях.
4. Экспертная поддержка при планировании реконструкций и модернизаций оборудования, где установлено.

П3.3. Основные обеспечивающие функции

1. Организация безбумажного электронного учета и контроля запросов со стороны АЭС к разработчику (разработчикам) СВБУ.
2. Обеспечение эффективного обмена информацией АЭС – эксперты в виде:
   - текстовых и бинарных файлов, включая коды ПО,
   - звонков по телефону в режиме точка-точка,
   - селекторных совещаний по телефону,
   - видеоконференций,
   - систем типа «Чат» с участием при необходимости представителей смежных организаций.

3. Обеспечение непрерывной доступности и готовности экспертов для выполнения функций сопровождения.
4. Обеспечение возможности автоматизированного формирования целевых экспертных групп.
5. Роботизированная организация работы экспертных групп с использованием методов интерсубъектного аудита.

П3.4. Вспомогательными функциями являются

1. Обеспечение конфиденциальности.
2. Обеспечение целостности информации.

П3.5. Требования к реализации функций

1. Срок службы - 30 лет с возможностью продления до 50 лет.
2. Скорость обмена информацией - не менее 1 Мбит/сек.
3. Режим работы – круглосуточно, с участием экспертов: Пн-Чт. С 9-00 до 18-00.
4. Допустимое время нахождения в неработоспособном состоянии – не более 1 дня в неделю.
5. Должна обеспечиваться защита конфиденциальности и целостности информации от следующих видов нарушителей:
    a. вредоносного ПО,
    b. вредоносного оборудования,
    c. посторонних лиц на АЭС и в вовлеченных организациях,
    d. действий посторонних организаций и спецслужб на потоки информации.

Приложение 4. Тестовое оборудование - виртуальная суперкомпьютерная модель (ВСМ) для модернизации СВБУ-2

П4.1. Особенности модернизации СВБУ

АСУ ТП АЭС представляет собой систему систем, к которым относятся ПТК/подсистемы нижнего уровня, СВБУ, СРВПЭ и др.

Подсистемы можно рассматривать как многомашинные вычислительные комплексы, связанные локальными вычислительными сетями (ЛВС) разных типов. Между элементами комплексов существуют проводные связи и связи через цифровые локальные сети. Но доля этих связей не велика. Подавляющее большинство связей проходят от низовых систем к СВБУ или друг к другу через ЛВС СВБУ.

В отличие от разработки процесс модернизации имеет ограничения по продолжительности пуско-наладочных работ (ПНР). Поэтому модернизация АСУ ТП АЭС может быть только поэтапной и привязанной к графику ППР, а общие решения, затрагивающие сразу несколько (более одной) систем одновременно, изменяться не могут. К ним относятся:

(1.) Система кодирования информации (KKS) – применяется во всех системах,

(2.) Механизм шлюзования – алгоритмы и протоколы передачи информации, реализованные в Интерфейсном программном обеспечении (ИПО) – применяется во всех шлюзах низовых систем для связи с СВБУ, СРВПЭ, ЛКЦ.

(3.) Алгоритмы и их параметры, применяемые для формирования обновлений значений сигналов, передаваемых в СВБУ и в смежные системы – затрагивают СВБУ, СРВПЭ, ЛКЦ, низовые системы, где формируются значения, и куда они передаются через ЛВС СВБУ.

Поэтапность означает, что в определенный момент времени допустима модернизация только одной системы АСУ ТП, после чего производится комплексная проверка ее интегрированности с СВБУ и связанными низовыми системами. Пока эта проверка не закончится успешно, модернизировать прочие системы нельзя – иначе возможен риск «хаоса» из-за сложности взаимодействия участников работ. С учетом указанных выше ограничений по времени, это приводит к требованию, чтобы задача интеграции была решена до этапа монтажа, а этап пуско-наладочных работ был бы сведен к минимуму.

П4.2. Опыт поставки АСУ ТП высокой степени интегрированности

Поскольку монтаж оборудования и ПНР на АЭС «Куданкулам» проводился силами индийских специалистов, перед российскими поставщиками и ИПУ РАН, как системного интегратора ПО, была поставлена задача обеспечить высокий уровень готовности систем АСУ ТП перед поставкой. Готовность подразумевала и интегрированность систем друг с другом.

Эту задачу ИПУ РАН (Разработчик ПО СВБУ/СРВПЭ и интегратор ПО АСУ ТП) и НИИИС (Генеральный конструктор и поставщик СВБУ/СРВПЭ/др.) выполнили успешно. Была доработана технология интеграции, применявшаяся для испытаний ПТК для АСУ ТП АЭС «Бушер-1». В нее входили два этапа:

(1.) интеграция низовых ПТК с ПО СВБУ на заводах-изготовителях и

(2.) интеграция ПО с техническими средствами (ТС) СВБУ/СРВПЭ в НИИИС.

Для этого применялись два вида моделей:

(1.) модели ПО СВБУ – программы, имитирующие работу в части, связанной с определенной низовой подсистемой АСУ ТП:

(2.) модели низовых подсистем – программы, имитирующие работу шлюзов и частично алгоритмов автоматики.

Технология состоит в том, что модели ПО отлаживаются на заводах-изготовителях так, чтобы достичь их полной интеграции с оборудованием и программным обеспечением низовых систем. Затем эти модели «склеиваются» особым образом, в результате чего формируется часть ПО, интегрированная со всеми низовыми подсистемами. Эта часть дополняется человеко-машинным интерфейсом, который отлаживается на поставочном оборудовании СВБУ. Для этого в НИИИС были собраны ПТК СВБУ 1-го и 2-го блоков в полном объеме. Достигнутый результат позволил приступить к использованию СВБУ сразу после монтажа.

Условия модернизации не позволяют собирать целостные ПТК на заводах-изготовителях. Поэтому описанная выше технология напрямую не применима. Но моделирование ПО СВБУ как подход вполне пригоден. На основе работающего ПО предлагается создать полномасштабную модель ПО, которая может функционировать на одном вычислительном устройстве и имитировать работу СВБУ/СРВПЭ и шлюзов низовых систем. Современные технологии виртуализации и компактные суперкомпьютеры позволяют это сделать за приемлемые время и цену.

П4.3. Вероятные ошибки, их поиск и риски при модернизации

При модернизации могут быть нарушены ограничения (1), (2), (3) (см. подраздел П4.1.).

Рассмотрим связанные с этим риски при модернизации низовой подсистемы АСУ ТП.

Если коды сигналов изменятся (нарушение (1)), то СВБУ/СРВПЭ и другие системы, которым передается информация через ЛВС СВБУ, перестанут получать нужные данные, что приведет к отказу функций архивирования, контроля или диагностики. Если это сигналы управления, то будет нарушена функция дистанционного управления. Для нахождения ошибок необходимо проанализировать состав сигналов от модернизированной подсистемы.

С учетом того, что общее число сигналов более 250 тыс., то на работающей СВБУ штатными средствами это сделать затруднительно – необходимо разрабатывать специальные программы поддержки анализа архивов и логов шлюзов. Это неизбежно, но, если эти программы будут устанавливаться на штатное оборудование СВБУ/СРВПЭ, то при их изготовлении придется применять все правила V&V, что радикально увеличивает их стоимость. Для программ, которые будут запускаться несколько раз в несколько десятков лет, это представляется обременительным.

Если при модернизации низовой подсистемы будет нарушено условие (2), то это может вызвать полный или частичный отказ функций СВБУ. При этом нет гарантии, что система диагностики СВБУ позволит выявить причины. Может понадобиться установка специальных отладочных средств, компиляторов и т.п. и/или изготовление специальных программ-ловушек прямо в среде ПО СВБУ/СРПВЭ, что не соответствует правилам обеспечения качества и безопасности и очень рискованно. Необходимо учитывать вероятность непредсказуемых последствий для низовых подсистем, которые получают информацию от модернизируемой системы через ЛВС СВБУ.

Нарушение условия (3) при модернизации может привести к различным отказам СВБУ и функции передачи информации через ЛВС СВБУ. Наиболее вероятными ошибками являются: излишне низкий или высокий темп передачи информации; недостаточная точность или наоборот ненужная детальность значений сигналов; «информационные удары» при включении или при реакциях на внутренние события. Все эти явления могут привести к отказам в СВБУ/СРВПЭ и/или в других низовых подсистемах, которые получают информацию от модернизируемой подсистемы через ЛВС СВБУ. Методы поиска ошибок в этом случае аналогичны описанным для (1)-(2).

Риски от нарушений (1) при модернизации СВБУ аналогичны. Нарушения (2) для СВБУ/СРВПЭ могут привести к отказам ее функций, а также к отказам шлюзов и функции передачи информации через ЛВС СВБУ. Нарушения (3) для СВБУ могут привести к отказам шлюзов, а также к отказам тех частей низовых подсистем, куда поступает информация от СВБУ. Методы поиска ошибок в СВБУ/СРВПЭ и связанные с этим риски аналогичны описанным выше.

Вывод: наибольшие риски связаны с тем, что ошибки при модернизации в одних подсистемах могут привести к отказам других, а для поиска ошибок придется вносить добавления/изменения в системы и их компоненты, напрямую не связанные с модернизацией, что ведет к дополнительным рискам.

П4.4. Решение: отладка с помощью модели СВБУ/СРВПЭ/шлюзов

На рис. П4.1 представлены компоненты виртуальной суперкомпьютерной модели СВБУ/СРВПЭ (ВСМ). Она включает полные виртуальные модели всех компонент ПО СВБУ/СРВПЭ, включая операционную систему, ее настройки, прикладное программное обеспечение и рабочие базы данных. Модели бинарно идентичны ПО, установленному на реальных ТС СВБУ/СРВПЭ, и функционируют на программных имитаторах ТС. Имитаторы ТС реализованы в средах виртуализации, реально размещенных на одном мощном суперкомпьютере (СК).

Модели ТС имитируют работу процессора, графических и сетевых карт, мыши и клавиатуры, тайм-сервера, устройств записи на магнитную ленту, агенты SNMP. Не имитируется функциональная клавиатура, мультиконтрольные блоки, коммутаторы, трансиверы и др.

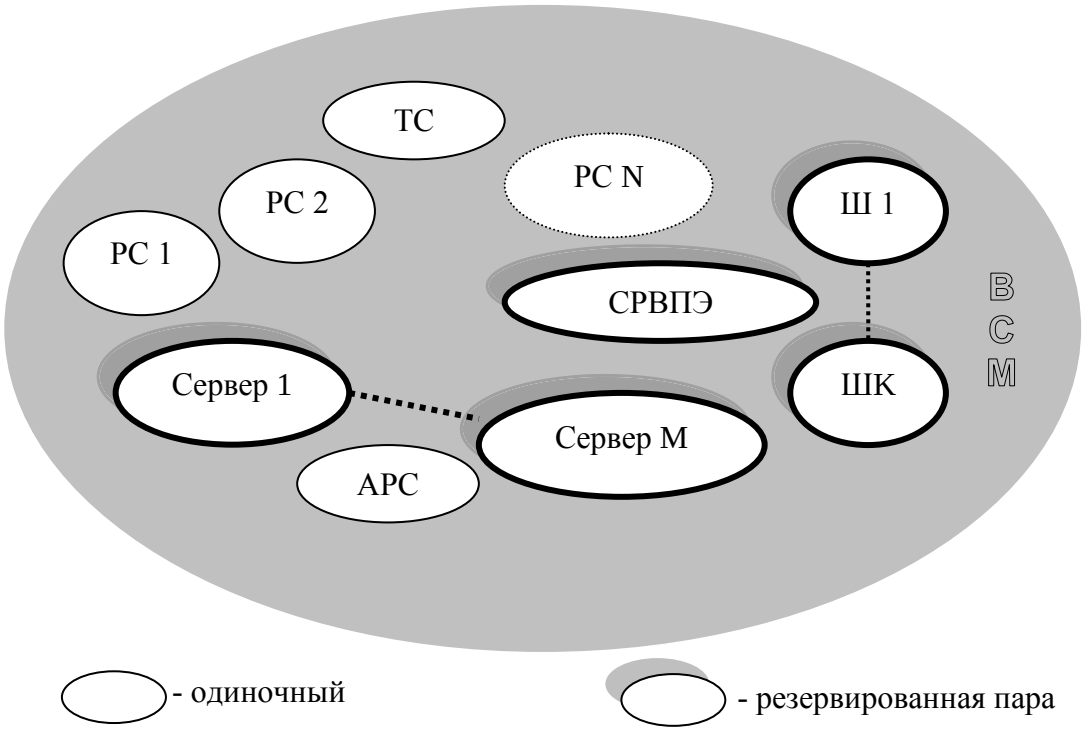

Рис. П4.1. РС 1-N – ПО рабочих станций, Сервер1-М – ПО серверов, ТС – ПО тайм-сервера, АРС – ПО архивного сервера, Ш 1 – К–ПО имитаторов шлюзов.

Компоненты модели могут находиться во включенном и выключенном состояниях. Через сетевые подключения СК с ВСМ может подключаться к системе подготовки данных (СПД), к шлюзам отдельных систем СВБУ или к ЛВС СВБУ, имитируя ее компоненты, подсистемы или их части.

П4.5. ВСМ при модернизации низовых подсистем АСУ ТП

Рассмотрим использование ВСМ для тестирования и поиска ошибок при модернизации низовых подсистем АСУ ТП. Рассмотрим вариант, когда модернизация производится путем замены программируемых компонент приборных стоек без перемонтажа проводных связей с датчиками и исполнительными механизмами. В этом случае, чтобы избежать рисков, указанных в п.3, перед подключением к СВБУ, необходимо убедиться, что:

- соблюдаются условия (1)-(3)
- (4) и соблюдаются все требования Технического задания на модернизацию по объему и параметрам обмена информацией с СВБУ/СРВПЭ и другими подсистемами АСУ ТП через ЛВС СВБУ.

Для этого СК подключается к сетевым разъемам шлюзов модернизируемой подсистемы АСУ ТП, а в ВСМ активизируются модели, имитирующие работу частей СВБУ и шлюзов сторонних подсистем АСУ ТП, получающих и передающих информацию через ЛВС СВБУ (см. рис. П4.2).

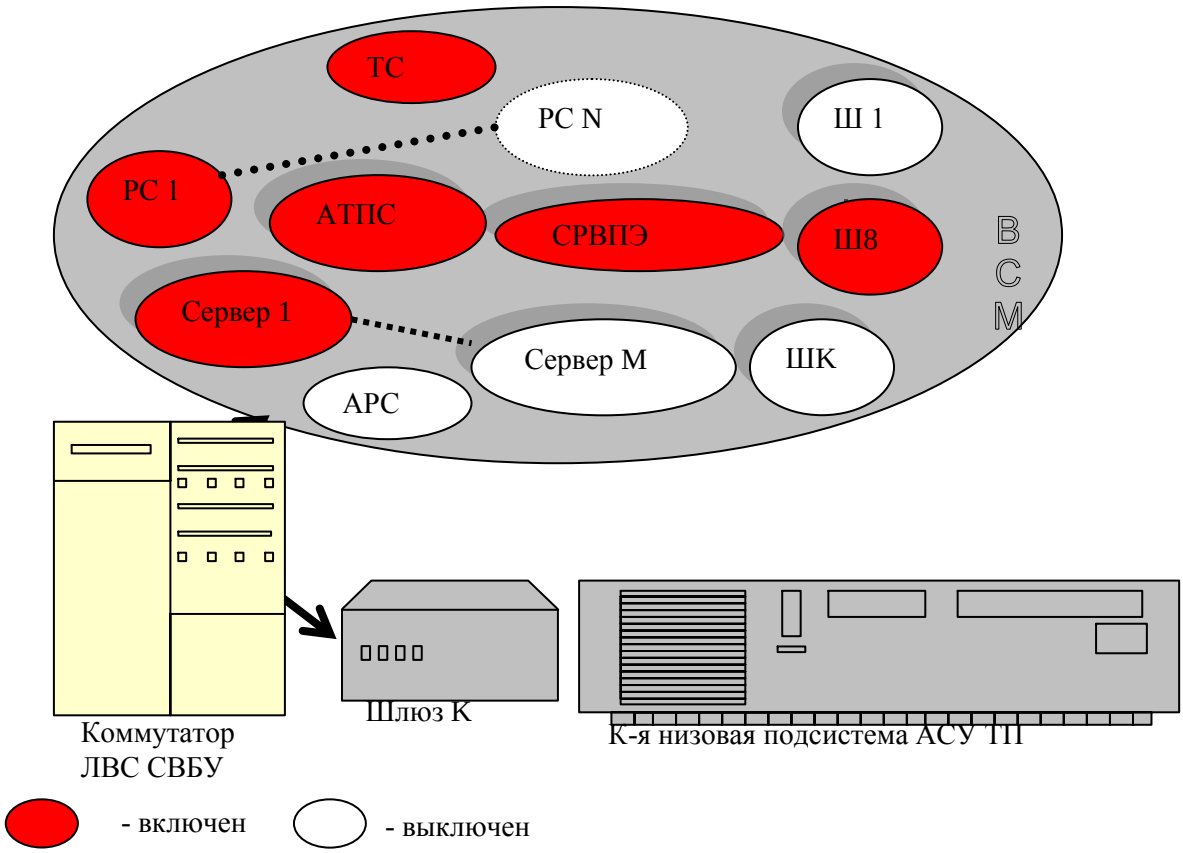

Рис. П4.2. Пример схемы включения компонент и подключения ВСМ к низовой подсистеме

Способы проверки условий (1) и (4) включают анализ архивов (на Сервере 1 рис. П4.2), который не сложен, поскольку в архиве будут содержаться только данные от одного шлюза, а также анализ лог-файлов моделей шлюзов, которые принимают информацию от К-й системы. При этом для проверки каналов управления от СВБУ до оборудования К-й подсистемы можно применять стандартные способы ввода команд управления через рабочие станции СВБУ (РС 1 на рис. П4.2). Проверка синхронизации времени возможна через использование имитаторов тайм-сервера (ТС на рис. П4.2), системы диагностики (АТПС на рис. П4.2). В ходе этих проверок косвенно проверяется и выполнение условий (2)-(3). Но для полного тестирования необходимы методики и их обеспечение в виде тестового ПО в ВСМ. При необходимости тестовое ПО и данные могут размещаться в среде СК вне ВСМ.

Тестирование с использованием ВСМ позволяет снизить риски отказов из-за несовместимости протоколов и аномалий потоков данных к минимуму (условия (1)-(4)). После подключения модернизируемой подсистемы к ЛВС СВБУ комплексное тестирование может сводиться к проверкам правильности сетевой коммутации в ЛВС СВБУ.

П4.6. ВСМ при модернизации СВБУ/СРВПЭ

В проектных решениях СВБУ/СРВПЭ предусмотрена покомпонентная модернизация без выключения и потери функций. Это позволяет разбивать процесс модернизации СВБУ/СРВПЭ на произвольные части, этапы, создавая свободу маневра в ходе общего процесса модернизации АСУ ТП.

Модернизация компонент ТС СВБУ/СРВПЭ включает:

(1.) Выключение и локальное отсоединение от ЛВС,

(2.) Демонтаж старых и установку новых модулей,

(3.) Автономное тестирование,

(4.) Включение в ЛВС,

(5.) Контроль над сигналами диагностики через АТПС.

Автономное тестирование ТС после замен проводится при помощи штатного тестового программного обеспечения, расположенного на временно подключаемом тестовом мобильном компьютере. Оно позволяет тестировать отдельные компоненты ТС без связи друг с другом и СВБУ/СРВПЭ в целом. Для автономного тестирования ПО штатных средств не предусмотрено, поскольку ПО не изменяется в процессе эксплуатации, ремонтов и замен с использованием ЗИП. Поэтому для автономного тестирования ПТС при модернизации необходимо разработать новые средства.

ВСМ может служить основой для таких средств. Для этого в ВСМ нужно включить модели ПО, с которыми взаимодействует модернизируемое ТС, подключить ВСМ к его внутренним сетевым интерфейсам и провести проверку работы ПО.

На рис. П4.3 представлена схема подключения ВСМ к модернизируемой рабочей станции (РС). При помощи модели ПО тайм-сервера (ТС на рис. П4.3) проверяется правильность работы системы синхронизации времени. При помощи моделей ПО сервера (Сервер 1 на рис. П4.3), шлюзов (Ш 1-Ш К на рис. П4.3) проверяется правильность конфигурации логических каналов передачи информации, основные функции контроля и управления, работоспособность схем резервирования и другие вспомогательные функции РС. При помощи модели ПО АТПС проверяются параметры работы ТС, включая сигналы

диагностики от установленных компонент электроники и ПО. При помощи модели ПО архивного сервера (АРС на рис. П4.3) проверяются функция сохранения лог-файлов. При помощи моделей ПО РС, входящих в одну группу с модернизируемой (РС 1 на рис. П4.3), проверяются синхронизация квитирования сигнализации. При этом могут применяться методики тестирования на полигонах СВБУ/СРВПЭ, упомянутых в п.2.

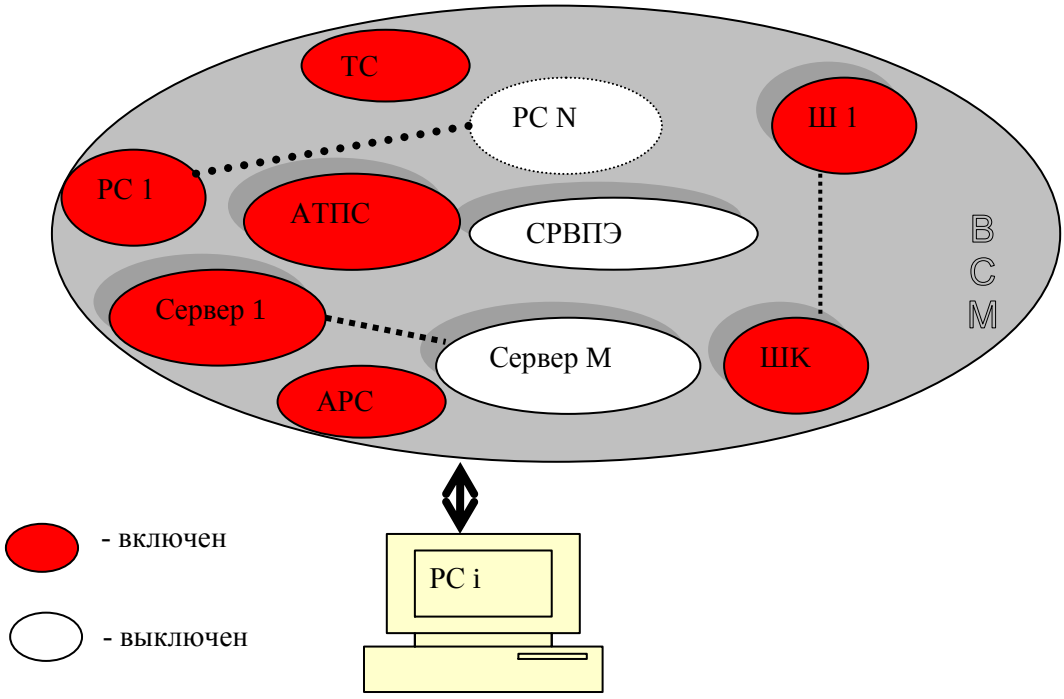

Рис. П4.3. Пример схемы включения компонент и подключения ВСМ к модернизируемой i-й рабочей станции

П4.7. Хостинг на СК

СК может использоваться для реализации новых неоперативных функций, например:

- углубленного анализа архивов через SQL-сервер.
- моделирования кибербезопасности,
- выполнение функций СПД,
- просмотр архивных данных в режиме имитации потоков через видеокадры СВБУ в реальном или ускоренном времени,Отработка с участием персонала АЭС новых версий ПО, ЧМИ и т.д.

Приложение 5 Системное программное обеспечение и стратегия его обновления

П5.1. Введение

Выбор СПО[3] для системы верхнего уровня АСУ ТП АЭС обусловлен рядом специфических требований, определяемых характеристиками объекта управления. Общие требования для программного обеспечения АЭС изложены в стандартах международной электротехнической комиссии (IEC61513), руководствах МАГАТЭ. Основными из них являются:

- надежность функционирования;
- высокое качество функций, предоставляемых ОС;
- обеспечение необходимой эксплуатационной документации;
- отсутствие ограничений на поставку на объект управления, как со стороны разработчиков программы, так и законов страны происхождения.
- соответствие жизненного цикла программного обеспечения жизненному циклу объекта управления (длительность эксплуатации и возможность модификации).

В качестве дополнительных функциональных требований собственно к СПО верхнего уровня АСУ ТП АЭС выделим:

- обеспечения интерфейса между прикладной программы и техническими средствами АСУ ТП:
- поддержка многозадачности:
- наличие необходимого набора средств разработки и отгадки прикладного программного обеспечения:
- наличие пакета программ (СУБД, редакторы, средства коммуникаций и т.д.) для обеспечения функционирования прикладных программ.

[3] Следует заметить, что часто термин ОС, заменяется на термин системное программное обеспечение (СПО), как более широкий класс, чем ОС. СПО это программное обеспечение, разработанное для специфической вычислительной системы или семейства систем, для облегчения эксплуатации и обслуживания системы. СПО обычно состоит из ОС и вспомогательных программных средств, например, компилятор, отладчик, СУБД. В разделе оба термина будут использоваться равноправно.

В АСУ ТП атомной энергетики России Linux пришел в 2000 г. авторы были в числе пионеров этого процесса. В 90-х годах Linux никто не рассматривал как серьезную альтернативу известным, надежным версиям семейства ОС UNIX и другим ОС общего пользования, например, MS Windows (Microsoft) MacOS (Apple). Это в основном высококачественные системы со значительным набором прикладных программ разработанных сторонними производителями.

Но у них было два недостатка. Первый – надежно они функционировали на ограниченном наборе сертифицированного оборудования, а второй – наличие лицензионных ограничений. Лицензионные ограничения являлись важнейшим фактором, заставившими разработчиков программного обеспечения для АСУ ТП АЭС обратить свое внимание на свободное программное обеспечение[4], обычно ассоциированное с Linux.

Появление Linux определялось как объективными, так и субъективными причинами. В АСУ ТП АЭС вышли на качественно новый уровень развития, связанный с возросшим уровнем автоматизации объектов управления. Произошедший качественный скачок в составе решаемых задач заставил пересмотреть и методы построения АСУ ТП и существенно повысить роль ОС как уровня, позволяющего, как предполагалось, изолировать прикладную рабочую программу от условий ее выполнения на конкретном техническом средстве. Ранее, в СССР в составе АСУ ТП на АЭС поставлялись отечественные ОС, однако в связи с их моральным устареванием, а еще больше из–за прекращения выпуска отечественных ЭВМ (типа СМ и ЕС), они не могли более служить основой современных средств АСУ ТП АЭС. Встал вопрос о приемнике ОС для верхнего уровня АСУ ТП АЭС нового поколения. В СВБУ функциональные требования к ОС близки к требованиям, предъявляемым к ОС общего назначения, в отличие от нижнего уровня, который тяготеют к использованию ОС реального времени со своими специфическими требованиями.

Функционирует Linux на широком классе компьютеров, включая мобильные, многопроцессорные и промышленные. Linux в значительной мере совместим с UNIX, и на него можно легко портировать ранее созданные для этой ОС программы. Кроме того, правовые характеристики Linux позволяют применять его без ограничений, а также вносить в него изменения и дополнения без чьего-либо разрешения.

Linux не имел документации, выполненной по российским нормам, не прошел положенных испытаний и не имел разрешения применения на АЭС. Поэтому многие

[4] Термин свободное программное обеспечение означает программное обеспечение, разработанное и распространяемое по GPL (или аналогичной) лицензии, с доступным исходным кодом.

фирмы начали создавать свои дистрибутивы на основе ядра Linux (ИПУ РАН (продукт LICS), ВНИИЭМ, НИКИЭТ и др.), либо использовать готовые дистрибутивы третьих фирм. Однако Linux имел, родовые, присущие ему и всему свободному ПО, которое он олицетворят проблемы.

П5.2. Проблемы с применением свободного программного обеспечения

Большое количество ошибок, обнаруживаемое в свободных программах, приводит к тому, что популярные дистрибутивы Linux кардинально обновляются (приблизительно два раза в год), а мелкие изменения происходят практически ежедневно. Особенностью является, то, что обновления трудно локализуемы и затрагивают как системные утилиты (драйверы) так и прикладные библиотеки. Совместимость носит условный характер – разработчикам прикладных программ предлагается адаптировать свои программы, по мере изменений в ОС. Если сменить один дистрибутив Linux на другой, то, есть высокий риск, что новые версии дистрибутива не будут совместимы с разработанным ранее прикладным программным обеспечением. Эта нестабильность – чрезмерно частое обновление, различие в дистрибутивах, - является основным недостатком Linux для применения в промышленности вообще, а для АСУ ТП АЭС в частности. Они приводят к следующим трудностям поддержки функционирования РПО:

- Новые технические средства требуют модификации СПО,
- Обновление СПО требуют обновления РПО,
- Полный цикл заводских и ведомственных испытаний,
- Большие сроки внедрения,
- Частичная потеря референтности РПО,
- На некоторых серверах и рабочих станциях работают компоненты рабочего программного обеспечения разных производителей, что приводит к необходимости согласования и кооперации всех участников и производителей технических и программных средств при проведении модификации.

Суммируя вышесказанное, можно сказать, что существует глубокая взаимозависимость жизненного цикла СПО и РПО (см. рис. П5.1).

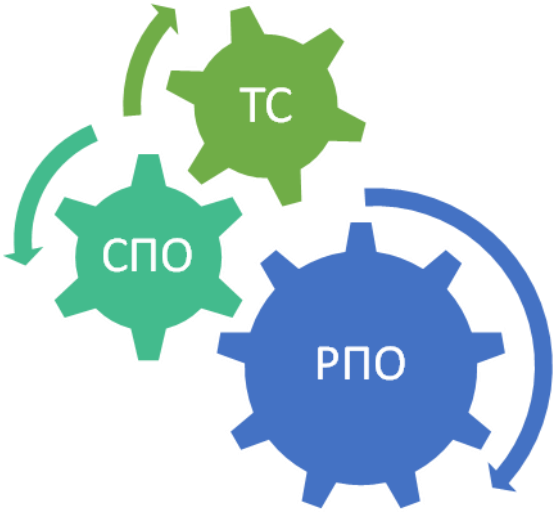

Рис. П5.1. Зависимость жизненного цикла модификации ПО СВБУ для РПО и СПО

П5.3. Особенности жизненного цикла СПО на основе свободного программного обеспечения без виртуализации

Модификация СПО является неотъемлемой частью жизненного цикла на этапе эксплуатации. Причиной этого как в большом объеме обнаруживаемых ошибок, так и изменении условий выполнения программы при изменении ТС. Большое количество взаимосвязей между компонентами (пакетами) из состава СПО приводит к тому, что изменения в одном компоненте, ведут к изменениям большого количества других. Наш опыт показывает, что средний объем модификации в каждом случае составляет не менее 30% от исходного объема СПО. Значительный объем изменения ведет к необходимости значительного тестирования и верификации разнородного исходного кода. Под разнородностью кода понимается то, что тексты программ написаны разными стилями, различны по алгоритмическому рисунку, т.к. разрабатывались совершенно независимыми группами разработчиков. Данная особенность сильно затрудняет процедуру верификации программы, и требует привлечения большого числа квалифицированных специалистов, по различным технологиям программирования.

Затраты в течение всего жизненного цикла СПО на основе свободного программного обеспечения могут превышать затраты на коммерческое СПО. Данные затраты имеют особенность в том, что на этапе эксплуатации они продолжают составлять значительную часть, по нашим оценкам, около трети начальной стоимости разработки. Затраты достаточно равномерно распределены на все этапы жизненного цикла (разработка – эксплуатация).

П5.4. Пути уменьшения стоимости жизненного цикла ПО СВБУ

Мы видим два пути уменьшения стоимости жизненного цикла:

(1.) Организационные, такие как обеспечение переиспользования компонентов, примененных в одних приложениях АСУ ТП АЭС в других проектах. Это достижимо при организации более тесного взаимодействия пользователей свободного программного обеспечения в АСУ ТП АЭС, допустим в виде создания ассоциации или иного координирующего центра.

(2.) Технические: Виртуализация связи СПО и РПО, например, с применением технологии виртуализации Docker[5] на основе контейнеров. Контейнеры несут в себе много привлекательных преимуществ как для разработчиков, так и для эксплуатационного персонала. Некоторые из наиболее заманчивых преимуществ перечислены ниже:

- Абстрагирование основное-СПО (СПО взаимодействующее с ТС) от контейнеризованных приложений,
- Простота масштабирования,
- Простота управления конфигурацией,
- Изолированные среды выполнения от среды взаимодействия с реальным оборудованием,
- и др.

Технология Docker основана на контейнерах. Контейнеры задуманы быть полностью стандартизованными элементом среды. Это означает, что контейнер соединяется с ТС или чем-либо внешним по отношению к нему при помощи определенных интерфейсов. Контейнеризованное приложение не должно полагаться или каким-то образом зависеть от ресурсов или архитектуры ТС, на котором оно работает. Это упрощает предположения о среде выполнения приложения в процессе разработки. Аналогично, с точки зрения ТС, каждый контейнер представляет собой "черный ящик". ТС нет дела то того, что за приложение внутри.

Контейнеры позволяют разработчику связать приложение или компонент приложения со всеми его зависимостями и дальше работать с ними как с единым целым. Основное СПО не знает о зависимостях, необходимых для запуска конкретного приложения. Если основное СПО может запустить уровень виртуализации Docker, он может запустить любой Docker-контейнер. Это облегчает управление конфигурацией.

[5] https://www.docker.com

Основное СПО больше не должны отвечать за управление зависимостями РПО, потому что, за исключением случаев зависимости одних контейнеров от других контейнеров, все зависимости должны содержаться в самом контейнере (см. рис. П5.2). Фактически каждое РПО в пределах своего контейнера взаимодействует со своим СПО.

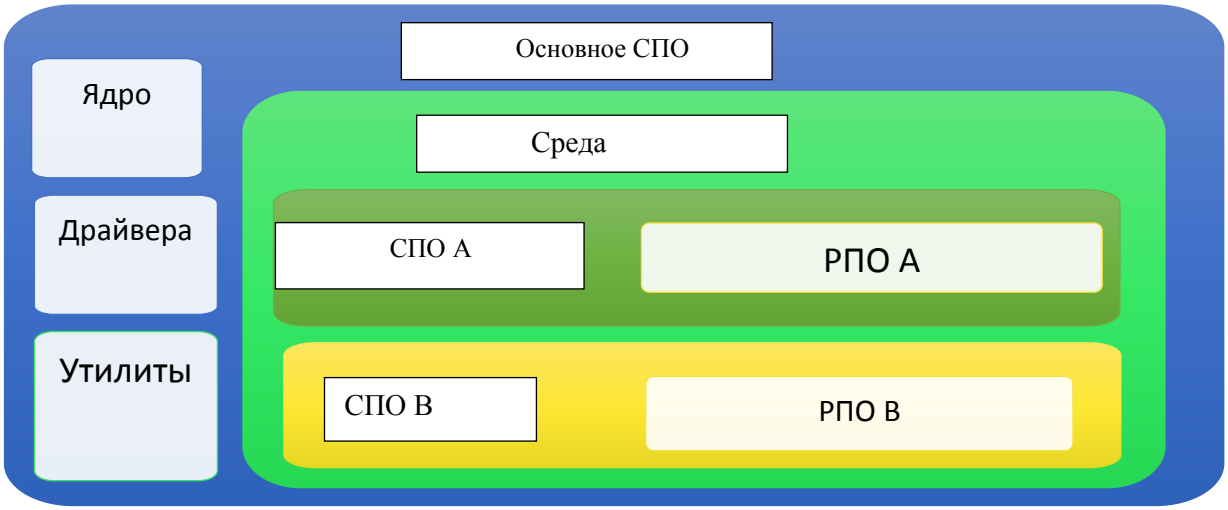

Рис. П5.2. Архитектура СВБУ с применением уровня виртуализации технологии Docker

Разработчик может запустить несколько контейнеров на ТС, где проводиться разработка, при этом та же система может быть горизонтально масштабирована, например, на тестовой конфигурации. Когда контейнеры запускаются в эксплуатацию, они снова могут быть масштабированы. Преимуществ абстрагирования между основным СПО и контейнерами является то, что при правильном проектировании приложения, масштабирование может быть простым и прямолинейным.

Несмотря на то, что контейнеры не предоставляют такого же уровня изоляции и управления ресурсами, как технологии полной виртуализации (например, виртуальная машина), они обладают чрезвычайно лёгкой средой исполнения. Контейнеры изолированы на уровне процессов, работая при этом поверх одного и того же ядра основной СПО. Это значит, что контейнер не включает в себя полную ОС, что определяет эффективность его взаимодействия с основным СПО.

Данные особенности определяют особенности совместного жизненного цикла СПО и РПО (см. рис. П5.3) при применении технологии виртуализации:

- Возможность работы разнородного РПО с различными версиями системного программного обеспечения на одном техническом средстве,

- Исключения или сокращение необходимости модификации рабочего программного обеспечения при смене ТС,
- Уменьшение объема интеграционного тестирования и согласования с разработчиками РПО,
- Сохранение полной референтности РПО.

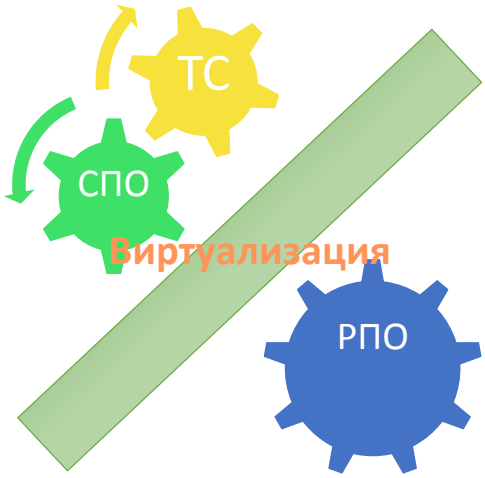

Рис. П5.3. Процессы жизненного цикла модификации ПО СВБУ с уровнем виртуализации

П5.5. Заключение

Основными проблемами в поддержании работоспособности СВБУ являются:

- взрывное развитие ТС, с полной заменой их в течение короткого, в пределах пяти лет, периода, нестабильность состава и большой объем изменяемого ПО из состава СПО, в ходе устранения ошибок и улучшения его функциональности,
- большая зависимость РПО и прикладных библиотек из состава СПО, что ведет к фактически необходимости проведения полного цикла разработки при изменении СПО для РПО.

Просматривается два возможных пути уменьшения затрат на поддержание работоспособности СВБУ в течение его жизненного цикла:

1. создание единого продукта СПО с централизованной поддержкой с учетом особенностей жизненного цикла АЭС и требованиями к качеству,
2. использование технологий виртуализации: выделение системных и прикладных библиотек, используемых РПО в отдельный уровень (с абстрагированием среды выполнения РПО от конкретной конфигурации СПО и технических средств).