НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ «Ядерная и радиационная безопасность», №4, 2002 г.
10-12/2002

УДК 621.039.5

Н.В.Афанасьев[1], О.М.Белохин[2], О.Бренман[3], В.М.Гольдрин[4], В.Н.Васильченко[4], Л.Н.Корчагин[1], В.Ф.Редько[5], Ю.В.Розен[4], М.А.Чернышов[2], М.А.Ястребенецкий[4]

ОБЕСПЕЧЕНИЕ И ОЦЕНКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ ЭНЕРГОБЛОКА АЭС С РЕАКТОРОМ ВВЭР-1000

[1] Южноукраинская АЭС
[2] ООО“Вестрон”
[3] Westinghouse Electric Corporation
[4] Государственный научно-технический центр по ядерной и радиационной безопасности
[5] Государственный комитет ядерного регулирования Украины

Начиная с 2002 года журнал «Ядерная и радиационная безопасность» публикует серию статей, посвящённых опыту обеспечения и оценки безопасности новых информационных и управляющих систем, внедрённых на АЭС Украины. В настоящей статье, продолжающей эту серию, рассматриваются результаты работ по реконструкции информационно-вычислительной системы энергоблока №1 Южноукраинской АЭС с использованием комплекса технических средств “Вулкан”, изготовленного предприятием «Вестрон» (г. Харьков) на базе оборудования фирмы Westinghouse Electric Corporation (США).

ВВЕДЕНИЕ

Информационно-вычислительная система (ИВС) «Уран-2М», которая эксплуатировалась на энергоблоке №1 ЮУ АЭС с 1982 года, физически и морально устарела и перестала соответствовать возросшим требованиям, которые предъявляются к современным информационным системам, важным для безопасности АЭС. Дефициты безопасности ИВС «Уран-2М» определялись:

- недостаточным объёмом отображаемых и архивируемых данных;
- плохим качеством отображения информации и устаревшим интерфейсом «человек-машина»;
- неудовлетворительной глубиной диагностирования;
- низкой надёжностью технических средств;
- значительным превышением фактического срока эксплуатации изделий по сравнению со сроком, регламентированным в технической документации;
- невозможностью пополнения полностью исчерпанного комплекта запасных частей в связи с прекращением производственной деятельности их изготовителей.

Для устранения указанных дефицитов безопасности ЮУ АЭС приняла решение о реконструкции ИВС, которое предусматривало замену центральной части системы «Уран-2М» и аппаратуры контроля генератора А701-3 на технические средства, использующие современные информационные технологии. Предложено сохранить при реконструкции существующие датчики, кабели связи, кабельные проходки, системы электропитания и кондиционирования.

Реконструкция ИВС, проведенная в 1998г, ставила целью:

- увеличение объема и улучшение качества выполнения вычислительных и иных функций (представления оперативному персоналу всей необходимой информации о протекании технологических процессов и состоянии оборудования энергоблока, регистрации, архивирования, технического диагностирования и т.п.);
- поддержку современного человеко-машинного интерфейса;
- достижение более высоких эксплуатационных характеристик (точности, надежности, устойчивости к внешним воздействиям, электромагнитной совместимости и др.);
- обеспечение достаточного запаса вычислительной мощности для возможного наращивания выполняемых функций в процессе эксплуатации системы.

ТЕХНИЧЕСКАЯ БАЗА

Центральной частью реконструированной ИВС является *программно-технический комплекс* – ПТК [2], разработанный предприятием (ООО) «Вестрон» (г. Харьков) на базе оборудования фирмы Westinghouse Electric Corporation (США).

Фирма Westinghouse (один из учредителей ООО «Вестрон») имеет большой и успешный опыт работы в области управления технологическими процессами в различных отраслях промышленности. В 1982 году фирма выпустила семейство аппаратуры WDPF (Westinghouse Distributed Process Family), основанное на полностью распределенной архитектуре и магистрали данных с детерминированным протоколом. Следуя за развитием

информационных технологий, Westinghouse в 1990 году разработала семейство WDPF-II с усовершенствованной магистралью данных (Westnet II) и расширенным составом периферийного оборудования, поставляемого ведущими мировыми фирмами [3].

WDPF-II - организованная совокупность технических средств, ориентированная на применение в качестве технической базы при компоновке (разработке и изготовлении) ПТК для информационных и управляющих систем в различных отраслях промышленности и удовлетворяющая требованиям к совместимости и полноте (для предусмотренной сферы применения). В соответствии с терминологией, принятой в отечественной литературе и нормативных документах, WDPF-II следует рассматривать как *агрегатный комплекс технических средств* [4].

Использование апробированных аппаратных и программных средств агрегатного комплекса WDPF-II, поставляемых в Украину фирмой Westinghouse, обеспечивает гибкость компоновки, оперативность изготовления, высокое качество и эксплуатационную надёжность ПТК. Участие специалистов «Вестрон» в проведении входного контроля получаемой аппаратуры, разработке ПТК для конкретных заказчиков, испытаниях, приёмке, выпуске конструкторской документации, а также в проведении пуско-наладочных работ и опытной эксплуатации на АЭС позволило обеспечить адаптацию ПТК к обязательным требованиям действующих в Украине нормативных документов (в ряде случаев отличающихся от требований национальных стандартов США, на которые ориентировались разработчики WDPF-II).

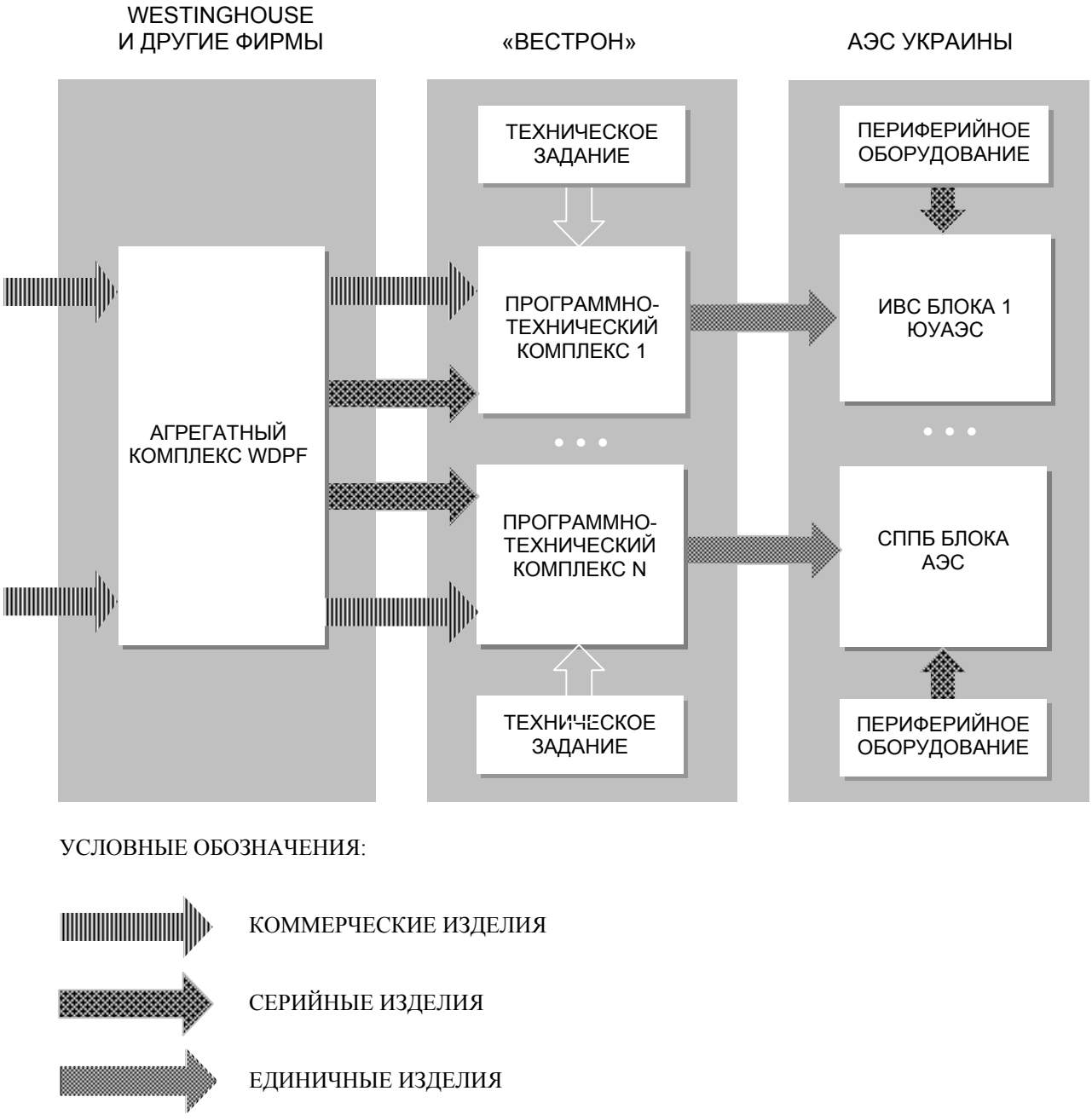

Рисунок 1 – Трансформация вида поставляемой продукции

Принятая концепция поставки (рис. 1) фактически предусматривает трансформацию *серийных* (аппаратных и программных средств WDPF-II) и *коммерческих* изделий ведущих мировых фирм – производителей электронного оборудования в *единичные* изделия (ПТК с программным обеспечением, сервисным оборудованием и эксплуатационной документацией).

В связи с этим следует особо отметить три обстоятельства, существенные для оценки безопасности применения таких ПТК на АЭС Украины:

- разработку групповых технических условий (ТУ) на комплекс технических средств автоматизированных систем (КТС) «Вулкан» (под этим общим названием «Вестрон» выпускает ПТК различного назначения, скомпонованные на базе агрегатного комплекса WDPF-II);
- сертификацию в системе УкрСЕПРО ряда типовых ПТК, выпускаемых по ТУ на КТС «Вулкан»;
- организацию спецтехприёмки ПТК на площадке предприятия – поставщика.

Необходимость проведения этих работ обусловлена тем, что наличие ТУ и проведение спецтехприёмки продукции, поставляемой на АЭС Украины, являются требованиями Регулирующего органа [6], а обязательность сертификации такой продукции установлена в Законе Украины «Про дозвільну діяльність».

ТУ на КТС «Вулкан» прошли государственную экспертизу ядерной и радиационной безопасности. После корректировки (с учётом замечаний и рекомендаций экспертов ГНТЦ ЯРБ, вытекающих из обязательных требований норм, правил и стандартов, действующих в Украине), ТУ были согласованы Регулирующим органом в качестве документа, устанавливающего общие требования к производству, приёмке, транспортированию, хранению, монтажу и эксплуатации ПТК, как компонентов информационных и управляющих систем нормальной эксплуатации, отнесенных к классу безопасности 3.

СОСТАВ И СТРУКТУРА ПТК

Структура ПТК (рис. 2) обусловлена требованиями заказчика (ЮУ АЭС), которые содержались в техническом задании на реконструкцию ИВС энергоблока №1:

- к составу выполняемых информационных и вспомогательных функций;
- к составу и размещению рабочих мест оперативного персонала;
- к видам, параметрам и числу электрических аналоговых и дискретных сигналов, принимаемых от датчиков;
- к организации обмена информацией с другими системами и применяемым интерфейсам связи.

ПТК имеет иерархическую (двухуровневую) распределенную структуру, которая включает специализированные субкомплексы, объединенные локальной сетью. Узел сети, предоставляющий некоторый ресурс другим узлам, именуется сервером данного ресурса. Узлы нижнего уровня выполняют ввод непрерывных и дискретных сигналов от датчиков, приём данных от других систем энергоблока и первичную обработку полученной информации. Узлы верхнего уровня производят более сложные расчёты, обеспечивают поддержку человеко-машинного интерфейса, осуществляют хранение, отображение, регистрацию и архивирование данных, выполняют подготовку и выдачу информации для общестанционной автоматизированной системы управления (АСУ АЭС).

Обмен данными между составными частями ПТК производится:

- по локальной сети Westnet II (обеспечивает передачу данных между узлами верхнего и нижнего уровня);
- по информационной магистрали Ethernet (обеспечивает передачу данных между узлами верхнего уровня).

Локальная сеть Westnet II образована двумя взаимно резервирующими магистралями, по которым передаются текущие значения технологических параметров энергоблока. Передача производится отдельными посылками, периодически (с интервалом 0,1 или 1,0 с) или по запросу. Периодические посылки содержат данные о «стандартных» параметрах, которые имеют системный идентификатор SID. Посылки, передаваемые по запросу, несут дополнительную информацию, например, о параметрах, отображаемых по вызову, которым присвоен расширенный системный идентификатор EXSID.

Обе магистрали Westnet II функционируют одновременно; при отказе одной из магистралей ПТК сохраняет работоспособность без какого-либо ухудшения функциональных характеристик.

Используется широковещательный метод передачи: узел, получивший право доступа к магистрали, выдает в течение предоставленного ему (гарантированного) интервала времени весь набор порождаемых данных, в то время как все другие узлы, подключённые к магистрали, принимают эти данные, осуществляют просмотр полученной информации и выбирают только ту ее часть, которая относится к данному узлу (необходима ему для выполнения предписанных функций). Номинальная скорость передачи единичных элементов цифрового сигнала данных по коаксиальному кабелю магистрали Westnet II (2 Мбод) позволяет передавать до 16000 значений «стандартных» параметров в секунду и до 16000 дополнительных параметров по запросу.

По магистрали Ethernet производится передача информации, не критичной ко времени:

- загрузка файлов из сервера программ в рабочие станции;
- обмен файлами между серверами архивирования (для восстановления при потере данных в одном из них);
- передача данных по запросу от сервера архивирования в рабочие станции, на сетевые принтеры и т.п.

Номинальная скорость передачи единичных элементов цифрового сигнала данных по коаксиальному кабелю Ethernet (10Base-2) составляет 10 Мбод. Используется метод доступа к магистрали с контролем несущей и обнаружением столкновений (стандарт IEEE 802) и протокол обмена TCP/IP.

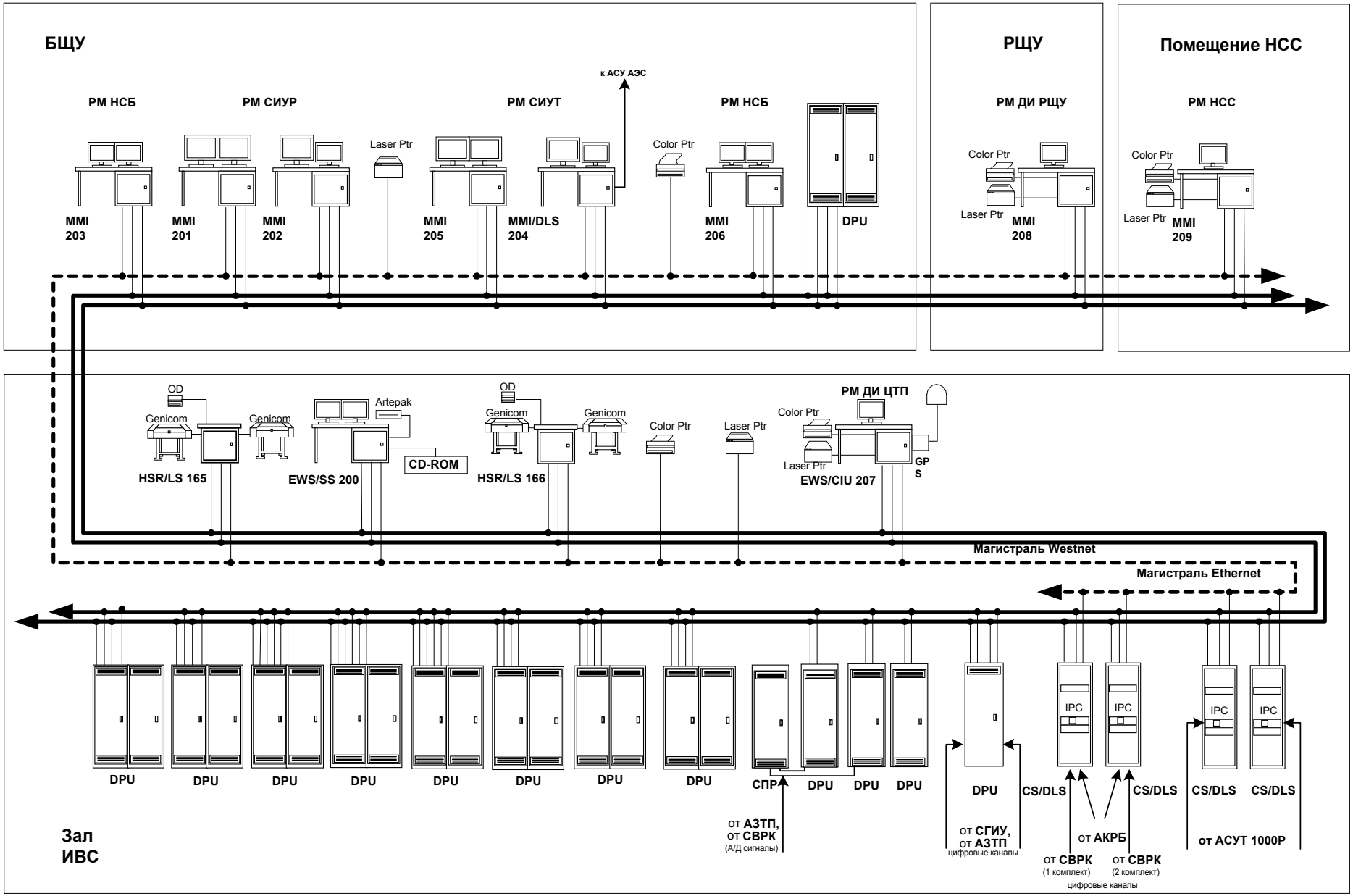

Рисунок 2 - Структура ПТК

Узлы нижнего уровня - субкомплексы сбора и обработки данных, реализованные на базе серийно выпускаемого Westinghouse Electric Company устройства сбора и распределенной обработки сигналов DPU (Distributed Processing Unit). DPU представляет собой двухканальную (дублированную) микропроцессорную систему, каждый канал которой содержит:

- микропроцессор Intel 80486DX;
- математический сопроцессор Intel 80487DX;
- специализированный логический сопроцессор (Gate-array chip);
- сторожевой таймер;
- электрически стираемое программируемое запоминающее устройство (flash-память) ёмкостью 384 Кбайт;
- оперативное запоминающее устройство;
- контроллер локальной сети Westnet II (с выходами для подключения к обеим магистралям Westnet II);
- последовательный порт RS-232 для подключения сервисной портативной ЭВМ;
- внутреннюю шину Multibus I;
- внутреннюю (локальную) шину расширения памяти;
- один или два контроллера внешней шины ввода-вывода (DIOB);
- вторичный источник питания (12 и 5 В постоянного тока).

Один, два или три отдельных DPU располагается в напольном шкафу. Модули ввода/вывода размещаются в том же шкафу DPU (до 36 модулей) и/или в шкафах расширения (до 48 модулей в каждом) и подключаются к шинам DIOB. Питание модулей постоянным током (13 В) осуществляется от двух вторичных источников (основного и резервного), установленных в шкафах DPU и в шкафах расширения.

Дополнительно к модулям ввода/вывода аналоговых и дискретных сигналов, которые поставляются Westinghouse Electric Corporation в составе DPU, «Вестрон» разработал и изготовил специальные модули (программируемые логические контроллеры) для ввода в DPU данных по цифровым каналам от других систем энергоблока (СГИУ и АЗТП). Несущие конструкции процессорных шкафов DPU и шкафов расширения, а также стойка преобразователей СПР (с модулями гальванического разделения цепей аналоговых и дискретных сигналов от АЗТП и СВРК) также изготовил «Вестрон».

DPU осуществляет сбор информации, преобразование входных сигналов в унифицированный цифровой формат, первичную обработку (контроль выхода параметров за границы предельных значений, анализ аварийных ситуаций, формирование предупредительных и аварийных сообщений) и выдачу данных в сеть Westnet II. Предусмотрены также техническое диагностирование, автоматический рестарт, возможность конфигурирования, контроля и изменения настроек DPU в автономном режиме (через последовательный порт RS-232) и в процессе работы (по магистрали Westnet II).

Узлы верхнего уровня реализованы на базе рабочих станций фирмы Sun Microsystems с операционной системой реального времени Solaris^{TM} семейства UNIX. Базовая рабочая станция содержит:

- RISK-процессор Sun 4640-MP с производительностью до 80 млн.операций в секунду;
- оперативное запоминающее устройство ёмкостью 64 или 128 Мбайт (расширяемое до 512 Мбайт);
- дисковую память ёмкостью 1,3 Гбайт (расширяемую до 5,2 Гбайт);
- два последовательных порта для подключения клавиатур и манипулятора;
- два параллельных порта для подключения принтеров;
- акустический порт;
- контроллер информационной магистрали Ethernet.

Материнская плата базовой рабочей станции имеет свободные позиции (слоты) для установки дополнительных модулей, сопрягаемых с внутренней интерфейсной шиной SBUS:

- одного или двух графических контроллеров (видеокарт) SBUS/TGX для подключения видеомониторов;
- контроллера - согласователя интерфейсов SBUS/SCSI для подключения внешних дисководов и накопителей;
- адаптера локальной магистрали SBUS/Ethernet для подключения промышленной персональной ЭВМ.

На одной из свободных позиций в несущей конструкции (крейте) базовой рабочей станции установлен контроллер локальной сети Westnet II (из состава WDPF-II). На других позициях могут устанавливаться:

- модуль дополнительной памяти (накопитель) на жёстком магнитном диске ёмкостью 2,0 Гбайт;
- комплект оборудования для связи со спутниковой системой глобального позиционирования (GPS).

Крейт базовой рабочей станции размещается в типовой конструкции, выполненной в виде стола, тумбы или шкафа, с встроенными панелями вентиляторов и распределителей электропитания, шинами питания, заземления и коммутационными элементами для подключения внешних цепей.

В шкафах размещают крейты базовой рабочей станции и промышленные персональные ЭВМ (IPC), которые выполняют вычислительные операции, требующие большого быстродействия, значительного объёма оперативной памяти и доступа к базе данных в реальном времени (теплотехнические, технико-экономические и другие расчёты, контроль защит и блокировок и др.). В состав IPC входят:

- встраиваемый системный блок с процессором PENTIUM-300, оперативным запоминающим устройством ёмкостью от 32 до 128 Мбайт, дисковой памятью (2 или 4 Гбайт) и 14 свободными позициями (слотами) для установки модулей расширения, сопрягаемых с шиной ISA и/или PCI;
- адаптер локальной магистрали PCI/Ethernet, установленный в системном блоке;

- встраиваемый видеомонитор;
- встраиваемая символьная клавиатура.

Для ввода данных по цифровым каналам от смежных систем (АСУТ-1000Р, АКРБ и СВРК) предусмотрены соответствующие интерфейсные адаптеры, которые поставляет «Вестрон» (устанавливаются на свободные позиции в системных блоках IPC). Типовые конструкции узлов верхнего уровня, функциональная клавиатура и оборудование для связи с GPS также изготовил «Вестрон».

Узлы верхнего уровня - операторские станции MMI, установленные в помещении блочного щита управления (БЩУ), образуют автоматизированные рабочие места (РМ):

- MMI 203 и MMI 206 - начальника смены блока (РМ НСБ);
- MMI 201 и MMI 202 - старшего инженера управления реактором (РМ СИУР);
- MMI 205 и MMI/DLS 204 - старшего инженера управления турбиной (РМ СИУТ).

MMI/DLS 204 выполняет также функции сервера связи с АСУ АЭС. Обмен данными производится по интерфейсу Ethernet через адаптер локальной магистрали SBUS/Ethernet в MMI/DLS и персональную ЭВМ, подключённую к локальной сети АСУ АЭС.

Операторская станция MMI 208, установленная в помещении резервного щита управления (РЩУ), служит рабочим местом дежурного инженера РЩУ (РМ ДИ РЩУ); операторская станция MMI 209 - рабочим местом начальника смены станции (РМ НСС). Установленная в зале ИВС инженерная станция EWS/CIU 207 является рабочим местом дежурного инженера центра технической поддержки (РМ ДИ ЦТП) и, одновременно, сервером связи со спутниковой системой глобального позиционирования.

Все операторские станции поддерживают стандартный интерфейс «человек–машина» и обеспечивают удобное и надёжное взаимодействие персонала с оборудованием ПТК при помощи развитой системы экранных меню, отдельные поля которых могут быть вызваны с помощью манипулятора или функциональной клавиатуры. При конфигурировании каждой операторской станции предусмотрена возможность ограничения доступа оператора к отдельным функциям (вводу данных, изменению статуса и т.п.). При попытке доступа к заблокированной функции оператор получает сообщение об ошибке.

Два сервера архивирования/документирования HSR/LS 165 и HSR/LS 166 (основной и резервный) предназначены для архивного хранения данных (получаемых от узлов нижнего и верхнего уровня по локальной сети Westnet II и интерфейсной магистрали Ethernet), вывода данных в виде отчётов (по запросам персонала и автоматически – при возникновении определённых событий), а также регистрации действий оперативного персонала.

Для конфигурирования ПТК, включая узлы верхнего уровня, локальную сеть Westnet II и устройства DPU, применяются стандартные методы управления конфигурацией, которые реализуются программными средствами инженерной станции EWS/SS 200. Предусмотрена возможность изменения конфигурации в процессе работы (при необходимости). EWS/SS 200 является также сервером программного обеспечения (обеспечивает хранение резервных копий программ и создание архивных файлов).

Состав каждого из узлов верхнего уровня определён с учётом его назначения (таблица 1). Программы, поддерживающие функционирование каждого узла, компонуются при инсталляции программного обеспечения.

Табл. 1 Состав узлов верхнего уровня

НАИМЕНОВАНИЕ И ОБОЗНАЧЕНИЕ СОСТАВНЫХ ЧАСТЕЙ	ОБОЗНАЧЕНИЕ УЗЛА (см. рисунок 2)											
	MMI 201	MMI 202	MMI 203	MM 205	MMI/DLS	MMI 206	MMI 208	MMI 209	HSR/LS	EWS/SS	EWS/CIU	CS/DLS
Стол	–	–	–	–	–	1	–	–	–	1	–	–
Тумба	1	1	1	1	1	–	1	1	1	–	1	–
Шкаф	–	–	–	–	–	–	–	–	–	–	–	1
Базовая рабочая станция Sun Microsystems	1	1	1	1	1	1	1	1	1	1	1	1
Графический контроллер (видеокарта) SBUS/TGX	2	2	2	2	2	2	1	1	–	2	1	–
Контроллер - согласователь интерфейсов SBUS/SCSI	–	–	–	–	–	–	–	–	1	1	–	–
Адаптер локальной магистрали SBUS/Ethernet	–	–	–	–	1	–	–	–	–	–	–	1
Контроллер локальной сети Westnet II	1	1	1	1	1	1	1	1	1	1	1	1
Накопитель на жёстком магнитном диске (2,0 Гбайт)	1	1	1	1	1	1	1	1	1	1	1	–
Комплект оборудования для связи с GPS	–	–	–	–	–	–	–	–	–	–	1	–
Видеомонитор SONI с диагональю экрана 20″	–	1	2	–	1	2	1	1	–	2	1	–
Видеомонитор EDL с диагональю экрана 27″	2	1	–	2	1	–	–	–	–	–	–	–
Стандартная клавиатура SUN TYPE 5C	1	1	1	1	1	1	1	1	–	1	1	–
Манипулятор TRAKBALL	1	1	1	1	1	1	–	–	–	1	–	–
Функциональная клавиатура[1)]	1	1	1	1	1	1	1	1	–	–	1	
Цветной струйный принтер HP 1200C	–	–	–	–	–	–	1	1	–	–	1	–

Одноцветный лазерный принтер Laser Jet 4M Plus	–	–	–	–	–	–	1	1	–	–	1	–
Матричный принтер Genikom 3480 одноцветный[2)]	–	–	–	–	–	–	–	–	1	–	–	–
Матричный принтер Genikom 3480 цветной[3)]	–	–	–	–	–	–	–	–	1	–	–	–
Дисковод магнито-оптических дисков HP 1300T	–	–	–	–	–	–	–	–	1	–	–	–
Дисковод 3.5″/привод накопителя на ленте ARTEPAK	–	–	–	–	–	–	–	–	–	1	–	–
Дисковод оптических компакт-дисков CD-ROM	–	–	–	–	–	–	–	–	–	1	–	–
Акустические колонки SP 330	–	2	2	–	2	–	–	–	–	–	–	–
Промышленная персональная ЭВМ	–	–	–	–	–	–	–	–	–	–	–	1

[1)] 169 клавиш мембранного типа, программируемых “под заказ”
[2)] используется для печати отчётов
[3)] используется для печати аварийных сообщений

Примечание:

MMI	-	Операторская станция
MMI/DLS	-	Операторская станция/Сервер связи
HSR/LS	-	Сервер архивирования/документирования
EWS/SS	-	Инженерная станция/Сервер программного обеспечения
EWS/CIU	-	Инженерная станция/ Сервер связи со спутниковой системой GPS
CS/DLS	-	Вычислительный сервер/Сервер связи

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Программное обеспечение (ПО) ПТК можно классифицировать следующим образом:

- стандартное программное обеспечение WDPF-II, разработанное для применения в информационных и управляющих системах, в том числе в атомной энергетике (серийная продукция Westinghouse);
- заимствованное программное обеспечение (коммерческая продукция других зарубежных разработчиков);
- программное обеспечение, разработанное специально для ИВС (единичная продукция «Вестрон»).

Отличительной особенностью ПО ПТК является наличие сервера программного обеспечения (EWS/SS 200), который является хранителем эталонного комплекта всех программ. Загрузка программ в память DPU и рабочих станций осуществляется с EWS/SS 200 по локальной сети Westnet II. Программное обеспечение инженерных станций (EWS/SS 200 и EWS/CIU 207) обеспечивает функционирование ПТК.

Структура ПО ПТК представляет собой традиционную композицию системного (заимствованного) и прикладного программного обеспечения. Системное ПО включает:

- операционную систему iRMX;
- операционную систему MS-DOS версии 6.22;
- операционную систему Solaris версии 2.3;
- драйверы поддержки протокола TCP/IP;
- драйверы периферийных устройств (Laser Jet 4M Plus, ARTEPAK, HP 1300T и др.);
- драйверы интерфейсных модулей (SBUS/SCSI, SBUS/Ethernet и др.);
- программы русификации.

Структура прикладного ПО отражает архитектуру ПТК, основной особенностью которой является использование глобальной распределенной базы данных для формирования информационных потоков. Благодаря этому все прикладные программы обмениваются информацией через базу данных, т.е. имеют только один обязательный интерфейс (с базой данных) и располагаются в структуре ПО на одном иерархическом уровне. Каждый комплекс прикладных программ основывается на «стандартном» (конфигурируемом) программном обеспечении WDPF-II, но содержит также и оригинальные программы, называемые файлами проектных данных (ФПД), представляющие собой единичную продукцию «Вестрон». ФПД - это символьные файлы, структурированные в соответствии с синтаксисом стандартного ПО, которые содержат входную информацию для прикладных программ. В отличие от конфигурационных данных стандартного ПО, определяющих логику функционирования программ, ФПД содержат данные, которые интерпретируются соответствующими стандартными программами при их запуске и используются ими в процессе выполнения заданных функций.

Прикладное ПО представлено комплексами программ функциональных подсистем:

- подсистемы локальной автоматики;
- подсистемы внешних интерфейсов;
- подсистемы отображения информации;
- подсистемы архивирования;
- подсистемы документирования;
- инженерной подсистемы;
- вычислительной подсистемы.

Комплекс программ подсистемы локальной автоматики выполняется процессорами DPU. Он включает операционную систему iRMX, библиотеку стандартных программ, предоставленных Westinghouse, и прикладные программы каждого DPU, состоящие из трех разделов:

- оригинальных программ, разработанных на основе стандартных алгоритмических модулей (для DPU, выполняющих обработку данных, которая не может быть реализована стандартными программами);
- конфигурационного раздела, который содержит необходимые общесистемные настройки и настройки для выполнения стандартных и оригинальных программ;
- раздела базы данных, содержащего атрибуты параметров базы данных этого DPU.

Комплекс программ подсистемы внешних интерфейсов выполняется при обмене данными по цифровым каналам со смежными системами энергоблока (АСУТ-1000Р, СВРК, АКРБ, СГИУ-М, АЗТП) и АСУ АЭС.

Комплекс программ процессора рабочей станции CS/DLS для связи с АСУТ-1000Р, СВРК и АКРБ представляет собой стандартный программный пакет Westinghouse (WESGate 1.4), дополненный файлами проектных данных (конфигурирования, запуска и останова сервера связи и др.).

Комплекс программ промышленной персональной ЭВМ для связи с АСУТ-1000Р, СВРК и АКРБ включает операционную систему MS-DOS, драйверы протокола TCP/IP и интерфейсных модулей, программы связи и конфигурационные файлы.

Комплекс программ логических контроллеров (в DPU 25/75) для связи с АЗТП и СГИУ-М включает операционную систему MS-DOS, стандартную программу DLMODBUS.EXE, реализующую логический протокол Modbus, и конфигурационный файл этой программы**.**

Комплекс программ подсистемы отображения информации выполняется процессорами рабочих станций в узлах MMI**,** MMI/DLS и EWS/CIU и поддерживает интерфейс «человек – машина».

Включает оригинальные прикладные программы (видеокадры, библиотеку графических символов, графический векторный шрифт) и файлы проектных данных (ФПД конфигурации, настройки параметров, инициализации мембранной клавиатуры и др.).

Комплекс программ подсистемы архивирования выполняется процессорами рабочих станций в узлах HSR/LS и обеспечивает сбор данных по информационной магистрали Ethernet и локальной сети Westnet II и их хранение на жестком диске (для оперативного использования) и на магнитооптических дисках.

Комплекс программ подсистемы документирования выполняется процессорами рабочих станций в узлах HSR/LS и обслуживает запросы на подготовку и вывод печатных копий документов.

Комплекс включает библиотеки макросов и отчетов, скрипт печати заявок, пиктограммы пользовательского интерфейса и другие файлы проектных данных.

Комплекс программ инженерной подсистемы выполняется процессорами рабочих станций в узлах EWS/CIU и EWS/SS и формирует среду для создания новых прикладных программ и управления системным и прикладным ПО.

Включает стандартные программы инструментального ПО (текстовые и графический редакторы, генераторы отчётов, компилятор языка «С», редактор электронных таблиц Applix версии 4.0, адаптированный к работе в среде WDPF-II, компиляторы баз данных), а также необходимые файлы проектных данных.

Комплекс программ вычислительной подсистемы включает стандартные программы и программы, разработанные специально для ИВС. Стандартные программы обеспечивают среду для выполнения расчетных задач, контролируют критические ситуации при выполнении расчетов, осуществляют учет задач, управляют резервированием вычислительных серверов и выдают сообщения оператору. В комплекс стандартных программ входят:

- системные программы;
- программа управления данными;
- программа отображения данных;
- программы архивирования;
- программа усреднения по времени;
- программа коррекции результатов измерений расходов и уровней;
- программа расчета скоростей;
- программа обработки данных резервированных измерительных каналов;
- программа «распаковки» дискретных параметров;
- библиотека программ ядерных расчетов.

Специально разработанные программы вычислительной подсистемы обеспечивают:

- расчет и анализ ТЭП;
- контроль водно-химического режима;
- анализ коэффициентов энерговыделения и контроль датчиков СВРК;
- расчет водообмена первого контура и прогноз выхода на МКУ;
- расчет непосредственно не измеряемых параметров;
- специальные расчеты энергоблока;
- отображение важных параметров энергоблока;
- отображение режимов работы энергоблока;

- определение состояния оборудования;
- определение состояния критических функций безопасности;
- определение допустимых режимов эксплуатации;
- расчет обобщенных параметров безопасности;
- расчет координат областей и линий для Р-Т диаграммы.

ЭТАПЫ РЕКОНСТРУКЦИИ

Реконструкция ИВС на блоке №1 ЮУ АЭС осуществлялась поэтапно. В первую очередь была внедрена система контроля температурных режимов работы турбогенератора, в которой использовался сокращённый набор средств WDPF-II, работающих в «пилотном» режиме (параллельно с центральной частью действующей системы «Уран-2М»). Опытная эксплуатация первой очереди ИВС (с июня 1996 г. по апрель 1998 г.), подтвердила работоспособность и правильность функционирования аппаратных и программных средств системы, позволила апробировать основные технические решения, положенные в основу реконструкции, способствовала освоению персоналом АЭС новых методов и средств отображения информации.

На втором этапе ИВС внедрена в полном объёме, предусмотренном техническим заданием (ТЗ) на реконструкцию. В июне 1998 г. проведены предварительные и приемочные испытания ИВС на энергоблоке №1 ЮУ АЭС. Испытания проводились по программе и методике, утвержденной НАЭК “Энергоатом” и согласованной с Регулирующим органом Украины. Приемочная комиссия, назначенная приказом НАЭК “Энергоатом”, в состав которой входили представители заказчика (ЮУ АЭС), основного потребителя (НАЭК), разработчика («Вестрон»), проектировщика (ХИЭП) и Регулирующего органа, рассмотрев конструкторскую и эксплуатационную документацию, материалы заводских испытаний ПТК, результаты пусконаладочных работ и предварительных испытаний системы, а также выводы и рекомендации, содержащиеся в Заключениях государственной экспертизы ядерной и радиационной безопасности, признала реконструированную информационно-вычислительную систему энергоблока №1 ЮУ АЭС соответствующей современному техническому уровню и удовлетворяющей требованиям ТЗ. Состав конструкторской документации признан соответствующим требованиям нормативных документов, а эксплуатационная документация - пригодной для обеспечения промышленной эксплуатации системы. Комиссия сочла возможным принять ИВС в постоянную (промышленную) эксплуатацию. В технологический регламент эксплуатации блока №1 ЮУ АЭС внесены соответствующие изменения, связанные с реконструкцией ИВС.

Метрологическая аттестация измерительных каналов ИВС проведена по согласованной методике в кампанию 1998-99 гг. Результаты аттестации подтвердили соответствие метрологических характеристик всех измерительных каналов ИВС требованиям ТЗ.

Завершающим этапом стало создание в 1999 г. на энергоблоке №1 ЮУ АЭС интегрированной системы, объединяющей ИВС с системой представления параметров безопасности (СППБ), также реализованной на базе КТС «Вулкан». Успеху такой интеграции способствовали открытая структура ИВС, допускающая возможность функционального «наращивания», однотипность архитектуры обеих систем, простота обмена данными между локальными сетями ИВС и СППБ, а также опыт разработки, внедрения, оценки безопасности и эксплуатации ИВС, накопленный специалистами организаций, участвовавших в реконструкции.

Обеспечение безопасности

Сделанный приёмочной комиссией вывод о соответствии реконструированной ИВС техническому уровню лучших зарубежных систем аналогичного назначения обусловлен:

- широким охватом функций информационной поддержки оперативного и эксплуатационного персонала;
- распределённой иерархической структурой и использованием локальных сетей для обмена данными между территориально рассредоточенными узлами системы;
- распределённой базой данных;
- дублированием микропроцессорных систем во всех узлах нижнего уровня (DPU);
- дублированием наиболее ответственных узлов верхнего уровня (серверов архивирования/документирования, вычислительных серверов/серверов связи, инженерных станций);
- резервированием магистралей локальной сети Westnet II и применением дополнительной информационной магистрали Ethernet для передачи данных между узлами верхнего уровня;
- полезной избыточностью средств ручного ввода и отображения данных в операторских станциях БЩУ;
- использованием цветных видеомониторов с большим экраном и высокой разрешающей способностью;
- наличием инженерных станций и сервера программного обеспечения, как инструментов сопровождения ПО (подготовки прикладных программ, конфигурирования, хранения резервных копий и т.п.);
- развитыми функциями технического диагностирования (с глубиной до сменного модуля) и отображением результатов диагностирования на видеомониторах операторских и инженерных станций;
- высокой надежностью основных технических и программных компонентов ПТК, поставляемых ведущими зарубежными фирмами и апробированных многолетним применением, в том числе в атомной энергетике.

Однако прогрессивность принципов, положенных в основу построения системы, сама по себе ещё не гарантирует безопасность её применения на АЭС. Под *обеспечением безопасности* имеется в виду соответствие процесса реконструкции, а также её продукта (реконструированной ИВС) регулирующим требованиям. Для систем нормальной эксплуатации, отнесенных к классу безопасности 3 (классификационное обозначение – 3Н) в качестве регулирующих принимались обязательные требования действовавших в Украине нормативных документов ([7-13] и др.), а также требования международных документов по безопасности ([14] и др.). Для удобства дальнейшего изложения регулирующие требования классифицированы согласно [15]:

- к надежности выполнения функций;
- к качеству выполнения функций;
- к независимости;
- к подтверждению соответствия;
- к устойчивости выполнения функций.

Требования, которые не являются регулирующими для информационных систем класса безопасности 3 и их компонентов, принимались во внимание в том случае, если они были сформулированы в ТЗ на ИВС и/или в ТУ на КТС «Вулкан», согласованных с эксплуатирующей организацией и Регулирующим органом.

Требования к надежности выполнения функций включали:

- требования к показателям надежности;
- соблюдение принципа резервирования;
- требования к структуре и элементам программного обеспечения;
- требования к защите от отказов по общей причине;
- требования к техническому диагностированию.

Показатели надёжности ПТК заданы в ТУ исходя из условий обеспечения требуемых характеристик безотказности и ремонтопригодности основных функций ИВС, регламентированных в техническом задании на реконструкцию. Надёжность ПТК обусловлена:

- высоким качеством применяемых компонентов;
- принятыми мерами поэлементного резервирования (в DPU), дублирования отдельных узлов верхнего уровня и магистралей сети Westnet II;
- аппаратной избыточностью операторских станций;
- развитыми функциями технического диагностирования;
- взаимозаменяемостью составных частей и удобством доступа к ним при техническом обслуживании и восстановлении.

Необходимый уровень надёжности обеспечивался также комплексом мер по планированию и контролю качества работ на этапах проектирования, изготовления, поставки ПТК, монтажа, наладки, испытаний и эксплуатации ИВС, предусмотренных организациями – участниками реконструкции в Программах обеспечения качества.

Оценка надёжности (безотказности), проведенная на стадии проектирования, подтвердила соответствие ПТК требованиям технического задания и Общим техническим требованиям к АСУ ТП АЭС с реактором ВВЭР-1000. Анализ эксплуатационной надёжности, проведенный с учётом данных об отказах за период с сентября 1998 по август 2001 года, подтвердил, что показатели безотказности ПТК находятся на уровне или выше проектных оценок, а по сравнению с ранее эксплуатировавшейся аппаратурой «Уран-2М» надёжность повышена на несколько порядков.

Резервирование является одной из главных архитектурных особенностей ПТК, обеспечивающей сохранение его работоспособности без ухудшения или с незначительным ухудшением функциональных характеристик при отказе любого из основных компонентов.

Локальная сеть Westnet II имеет две параллельно работающие магистрали, по которым одновременно передаются одни и те же данные. Отказ одной из них не нарушает возможности обмена данными, который осуществляется по другой (исправной) магистрали.

При отказе основного вычислительного сервера формируется идентификатор отказа, основной сервер автоматически переводится в автономный режим, а резервный – в основной режим. Аналогичным способом обеспечивается живучесть DPU при отказе одного из двух резервированных каналов.

Поскольку оба сервера архивирования собирают и хранят данные независимо друг от друга, после отказа и последующего восстановления отказавшего сервера потерянные им данные воссоздаются до полного соответствия с данными сервера, сохранявшего работоспособность, при этом алгоритм восстановления учитывает и предполагаемые сбои при передаче и копировании файлов во время операции восстановления.

Если отказал основной сервер документирования, получаемые им заявки на регистрацию будет автоматически выполнять резервный сервер. При отказе резервного сервера генерируется соответствующее диагностическое сообщение, отображаемое на видеомониторах операторских станций.

Средства ручного ввода и отображения данных в операторских станциях БЩУ формально не резервированы, однако при отказе какого-либо из них сохраняется возможность наблюдения и управления благодаря их избыточности и разнообразию на каждом рабочем месте.

Информационная магистраль Ethernet не резервирована, поскольку передаваемые по ней данные не критичны ко времени, и в случае их потери или искажения (например, при отказе магистрали или контроллера) эти данные могут быть переданы повторно после восстановления связи.

Экономические соображения не позволили резервировать модули ввода, преобразования и гальванического разделения цепей аналоговых и дискретных сигналов в составе DPU и СПР. Следует, однако, иметь в виду, что отказ какого-либо из этих модулей не приводит к полному отказу соответствующего устройства, а лишь к потере информации от группы датчиков, сигналы которых должны были вводиться через отказавший модуль, притом, только в течение времени, необходимого для его замены. Средства технического диагностирования ПТК и принятые конструктивные решения обеспечивают возможность быстрого обнаружения отказов и оперативного восстановления работоспособности любого узла. В частности, замена отказавших модулей в DPU может производиться без выключения питания и не требует инсталляции после замены.

Программное обеспечение ПТК имеет ясную модульную структуру. Его основу составляет системное и прикладное ПО, ранее разработанное и апробированное Westinghouse Electric Company, и ПО других ведущих фирм, адаптированное Westinghouse для агрегатного комплекса WDPF-II. Использование в ПТК заимствованных программных средств практически не потребовало их модификации. При разработке новых программных модулей их надёжность и совместимость с другими частями ПО обеспечивались в соответствии с требованиями [14].

Отказы по общей причине устраняются принятыми мерами по резервированию, стойкостью технических средств к возможным нарушениям условий эксплуатации и воздействию аномальных природных явлений (см. ниже), достаточно простым и удобным интерфейсом «человек – машина», а также высоким качеством подготовки оперативного и эксплуатационного персонала энергоблока,.

В качестве одной из вероятных общих причин рассматривалось исчезновение напряжения на питающем фидере. Устойчивость DPU к таким прерываниям электропитания обеспечена тем, что каждый канал (основной и резервный) питается от своего вторичного источника, причём эти источники подключаются к двум разным сетям первичного электропитания. Так же резервируется питание модулей ввода – вывода аналоговых и дискретных сигналов. В этом случае отказ любой сети не приводит к нарушению функционирования DPU, поскольку питание одного из каналов сохраняется. С той же целью резервированные узлы верхнего уровня, питающиеся непосредственно от сети 220 В переменного тока, подключены к разным сетям первичного электропитания. Питание нерезервированных операторских станций организовано так, что при отказе любой из сетей на каждом рабочем месте сохраняется работоспособность какой-либо одной из двух операторских станций (подключённой к исправной сети).

Техническое диагностирование DPU реализуется аппаратными средствами (сторожевыми таймерами) и диагностическими программами в составе библиотеки стандартных программ, предоставленных Westinghouse (глубина диагностирования - до одного сменного модуля). Техническое диагностирование узлов верхнего уровня реализуется программными средствами рабочих станций и промышленных персональных ЭВМ. Диагностические сообщения передаются по локальной сети и отображаются на видеомониторах рабочих станций, в том числе на рабочем месте дежурного инженера центра технической поддержки.

Требования к качеству выполнения функций включали:

- требования к точности;
- требования к временным характеристикам;
- требования к человеко-машинному интерфейсу.

Точность выполнения информационных функций ИВС определяется, в основном, точностью датчиков с непрерывными (аналоговыми) выходными сигналами и модулей ввода аналоговых сигналов в составе DPU. Линии связи датчиков с DPU при правильном проектировании увеличивают погрешность очень незначительно, а влиянием остальных звеньев измерительных каналов (осуществляющих обработку, хранение, передачу, отображение и регистрацию данных в цифровой форме) можно пренебречь.

Для ввода и преобразования в цифровой код сигналов от термоэлектрических датчиков (термопар) с градуировками ХА и ХК, работающих в температурном диапазоне 0-400°С, а также унифицированных сигналов постоянного тока (0-5 и 4-20 мА) и напряжения (0-5 В) применяются модули QAX, входящие в состав семейства модулей ввода-вывода Q-Line, разработанного Westinghouse. В модуле QAX предусмотрены трансформаторная гальваническая развязка каждой из 12 входных цепей, коррекция температуры «свободных» концов термоэлектрических датчиков, нормализация и параллельное преобразование всех входных сигналов в частоту, преобразование частоты в цифровой 13-разрядный код (включая бит полярности), которое производится четыре раза в секунду в течение 0,2 с. Цифровые данные вместе с диагностическими признаками выводятся на шину DIOB в 16-разрядном формате. Каждые 8 секунд встроенная в модуль однокристальная микроЭВМ осуществляет автоматическую калибровку «нуля» и коэффициента преобразования всех каналов. Погрешность преобразования с доверительной вероятностью 99,7% не превышает ±0,1% от верхнего значения диапазона (±1/2 младшего разряда). Дрейф «нуля» не превышает 0,002% в месяц и не выходит за пределы 0,02% в течение более длительного срока.

Для ввода и преобразования в цифровой код сигналов от терморезисторных датчиков (термометров сопротивления) с градуировками 50 М и 50 П, применяются модули QRT семейства Q-Line. В модуле QRT предусмотрены измерительные мосты для подключения четырёх датчиков (по трех или четырех проводной схеме), трансформаторная гальваническая развязка каждой из входных цепей, нормализация и параллельное преобразование всех входных сигналов в частоту, преобразование частоты в цифровой 12-разрядный код (производится два раза в секунду в течение 0,4 с). Цифровые данные, включая диагностические признаки, выводятся на шину DIOB в 16-разрядном формате. Каждые 9 секунд встроенная в модуль однокристальная микроЭВМ осуществляет автоматическую калибровку «нуля» и коэффициента преобразования всех каналов. Погрешность преобразования не превышает ±0,1% от верхнего значения диапазона (±1/2 младшего разряда), дрейф «нуля» не более 0,002% за месяц (долговременный - не более 0,02%).

Предусмотрены аппаратные средства и программное обеспечение, поддерживающие автоматизированную поверку измерительных каналов ПТК.

Высокие метрологические характеристики модулей Q-Line позволили повысить точность измерительных каналов при реконструкции ИВС, несмотря на то, что в новой системе сохранены действующие датчики. В ТЗ на реконструкцию ИВС установлены требования к основной приведенной погрешности:

- измерительных каналов с термоэлектрическими и терморезисторными датчиками – не более 0,5%;
- измерительных каналов с датчиками (преобразователями) с унифицированными сигналами - не более 0,25%.

Соответствие метрологических характеристик требованиям ТЗ подтверждено результатами их экспериментального исследования при испытаниях ПТК на предприятии-изготовителе, во время пуско-наладочных работ на ЮУ АЭС и в процессе метрологической аттестации измерительных каналов ИВС на работающем энергоблоке.

Временные характеристики ИВС полностью определяются свойствами ПТК:

- длительность цикла ввода данных от датчиков непрерывных и дискретных сигналов (при детерминированном доступе) – 0.1 и 1,0 с;
- разрешающая способность по времени при вводе непрерывных и дискретных сигналов – не более 0,02 с;
- задержка вызова данных на отображение – не более 4 с;
- задержка выбора данных из архива для отображения или регистрации - не более 2,5 с (для данных от датчиков) и 4,0 с (для данных от смежных систем);
- скорость обновления данных, отображаемых на экранах видеомониторов – 1 раз в секунду;
- скорость передачи данных по локальной сети Westnet II – 16 000 параметров в секунду.

Человеко-машинный интерфейс реконструированной системы существенно отличается от ранее принятого в ИВС «Уран-2М». Основной формой организации интерфейса является отображение на экранах видеомониторов рабочих станций специальным образом обработанной информации о ходе технологического процесса и состоянии оборудования (включая оборудование самой ИВС), а также справочной и архивной информации, с использованием многооконной графики и разветвлённой системы меню в операционной среде Solaris™. Обработка информации предусматривает её представление в виде, наиболее удобном для восприятия и анализа оперативным персоналом. Каждому оператору по его выбору представляется обобщенная и/или детальная информация в форме видеокадров, содержащих технологические мнемосхемы, гистограммы, графики, таблицы, текстовые сообщения.

Вызов любого из 4 000 возможных видеокадров (организованных в виде иерархической системы с неограниченным числом уровней детализации) производится с использованием манипулятора TRAKBALL, стандартной клавиатуры, а также с помощью программируемой функциональной клавиатуры (для наиболее часто вызываемых видеокадров). На экране видеомонитора могут одновременно отображаться до 4 видеокадров, при этом предусмотрены меры защиты от потери информации из-за наложения или перекрытия видеокадров при их вызове, а также при изменении оператором размеров и/или положения окон, в которых отображаются видеокадры. Переменные данные, отображающие текущие значения параметров и состояние технологического оборудования, автоматически обновляются.

Кроме контроля текущего состояния технологического процесса и оборудования, предусмотрена возможность вызывать видеокадры, отображающие тренды и/или отклонения от заданных значений любой из 200 возможных групп технологических параметров, оперативно формировать эти группы и изменять заданные значения параметров.

Для отображения информации на рабочих местах оперативного персонала используются цветные видеомониторы с диагональю экрана 20’’ и 27’’, разрешающей способностью 1152×900 точек, количеством цветов 256, что существенно превышает характеристики видеомониторов «Уран-2М». Для ввода, отображения и регистрации данных применяются условные обозначения (в том числе – сокращения и аббревиатуры), удобные и понятные для персонала и не требующие дополнительной расшифровки.

Требования к независимости включали:

- соблюдения принципа независимости;
- требования к электромагнитной совместимости (уровню излучаемых помех);
- требования к изоляции;
- требования к пожаробезопасности.

Независимость подразумевает способность ПТК к выполнению основных функций при отказе или преднамеренном выводе из работы любой резервированной части (канала) ПТК или любой связанной с ним системы. Из числа мер, обеспечивающих соблюдение принципа независимости, реализованы:

- гальваническое разделение входных цепей ПТК;
- питание резервированных каналов от разных источников;
- экранирование кабелей питания;
- физическое разделение резервированных каналов DPU, которые размещаются в разных крейтах;
- физическое разделение оборудования на рабочих местах оперативного персонала в помещении БЩУ;
- размещение резервированных серверов (CS/DLS, HSR/LS, EWS) в отдельных несущих конструкциях;
- размещение сетевых принтеров в разных помещениях;
- выбор магистральной структуры (топологии) локальной сети Westnet II, сетевых интерфейсов и протоколов, обеспечивающих при отказе любого узла возможность безошибочного обмена данными между остальными узлами.

Излучаемые помехи, вызванные электромагнитными процессами при включении, работе, нарушениях в работе и/или отключении изделий, не должны оказывать неблагоприятного влияния на другие изделия по общим или электрически связанным цепям, а также по пространству помещений. Уровень излучаемых помех не должен превышать значений, установленных для оборудования класса А по ГОСТ 29216-91. Аналогичные требования установлены в ТУ на КТС «Вулкан» и подтверждены результатами заводских испытаний ПТК.

Изоляция между корпусом и всеми изолированными от корпуса по постоянному току электрическими цепями, а также между гальванически разделенными или разделяющимися в процессе работы электрическими цепями любого эксплуатационно-автономного изделия (составной части ПТК) выдерживает в течение одной минуты действие испытательного напряжения 500 В при верхних рабочих значениях температуры и влажности. Сопротивление электрической изоляции между этими же цепями превышает 40 МОм при нормальных условиях испытаний, 10 МОм при верхнем рабочем значении температуры и 2 МОм при верхнем рабочем значении влажности.

Пожаробезопасность ПТК достигается применением:

- негорючих и трудно горючих материалов и кабелей, не распространяющих горение;
- комплектующих изделий, в которых при перегрузках по току, коротких замыканиях или отказах не образуются источники зажигания;
- средств контроля и сигнализации превышения температуры в шкафах DPU.

Требование к подтверждению соответствия включали:

- требования к апробации;
- требования к испытаниям и приёмке;
- требования к верификации ПО.

Апробация основных технических решений проводилась во время опытной эксплуатации первой очереди ИВС на энергоблоке №1 ЮУ АЭС.

Испытания, включенные в программу обеспечения качества и проведенные в процессе реконструкции, охватывали:

- подтверждение заданных требований в процессе отработки системотехнических, схемных, конструктивных и программных решений;
- предварительные испытания поставочного комплекта ПТК на предприятии-изготовителе (заводские испытания);
- входной контроль поставочного комплекта на площадке заказчика;
- автономные и комплексные испытания ПТК при проведении пуско-наладочных работ на энергоблоке;
- предварительные испытания ПТК в составе ИВС;
- приемочные испытания ИВС.

Кроме того, характеристики применённых в ПТК изделий Westinghouse и ряда других зарубежных изготовителей проверены и подтверждены материалами испытаний, проведенных независимыми зарубежными испытательными центрами.

На всех этапах испытания проводились в соответствии с разработанными программами и методиками, утвержденными в установленном порядке. Результаты испытаний документировались. Регулирующему органу представлены материалы, подтверждающие соответствие объекта испытаний (ПТК, ИВС) требованиям нормативных документов по критериям приемлемости результатов испытаний, которые установлены в соответствующих программах и методиках.

Принятая концепция последовательных многоступенчатых испытаний обеспечила достаточную глубину и достоверность их результатов.

Верификация ПО проводилась:

- на этапах разработки ТЗ (выработки требований к ПО);
- на этапе создания (проектирования и кодирования) ПО;
- на этапе отработки ПО в процессе заводских испытаний поставочного комплекта ПТК;
- на этапах испытаний и ввода в эксплуатацию ИВС.

Результаты верификации ПО отражены в документах, представленных Регулирующему органу. Анализ этих документов показал, что в них отражены все стадии процесса разработки и испытаний ПО, и для всех стадий имеются отчеты по результатам верификации. Требования, предъявляемые к процессу верификации ПО, в окончательной версии документов выполнены полностью, и результаты верификации признаны положительными.

Требования к устойчивости выполнения функций включали:

- требования по стойкости к внешним воздействиям;
- требования по стойкости к изменению параметров электропитания;
- требования к электромагнитной совместимости (помехоустойчивости);
- требования к защите от несанкционированного доступа.

Оценка устойчивости выполнения функций проводилась на основании требований нормативных документов по ядерной безопасности, действующих в Украине к моменту внедрения ИВС. Позднее аналогичная оценка проводилась в отношении тех же средств КТС «Вулкан», на базе которых реализована СППБ, но уже с учетом регулирующих требований утверждённого к этому времени документа [16]. Ниже изложены результаты последней оценки.

Стойкость к внешним воздействиям обеспечивает выполнение предусмотренных функций (в заданном объеме и с регламентированными характеристиками) в рабочих условиях эксплуатации ПТК и при нарушениях рабочих условий, вызванных:

- отказами технологических систем, обеспечивающих рабочие условия эксплуатации;
- нарушениями режима работы мощных электротехнических агрегатов;
- аномальными природными явлениями (землетрясения).

Внешние воздействующие факторы (ВВФ) окружающей среды характеризуются рабочими значениями (соответствующими рабочим условиям в местах эксплуатации аппаратуры) и предельными значениями, которые могут возникать в течение ограниченного времени, например, при отказах систем вентиляции, кондиционирования и т.п. Обобщенные рабочие и предельные значения ВВФ окружающей среды определяются (согласно [16]) в зависимости от группы условий эксплуатации. Для помещений электротехнического оборудования зоны свободного режима предусмотрена группа условий эксплуатации 2.2, для помещений щитов управления - 2.3. Обобщенные рабочие и предельные значения ВВФ окружающей среды для таких помещений представлены в таблице 2. Там же приведены значения ВВФ, регламентированные в ТУ на КТС «Вулкан» для узлов нижнего уровня (DPU) и верхнего уровня (рабочих станций).

Сопоставление этих значений с требованиями нормативного документа [16] показывает, что в рабочих условиях эксплуатации, характерных для зала ИВС и помещений БЩУ и РЩУ, в которых размещены узлы нижнего и верхнего уровня, ВВФ окружающей среды не могут повлиять на их работоспособность и технические характеристики. Однако необходимость размещения аппаратуры в зале ИВС потребовала принятия компенсирующих мер для того, чтобы предельные значения температуры и влажности в этом помещении не превышали допускаемые для рабочих станций согласно ТУ на КТС «Вулкан».

В местах размещения оборудования ПТК вибрация и механические удары в рабочих условиях эксплуатации отсутствуют, однако они могут возникать как сейсмические воздействия, передаваемые через строительные конструкции во время землетрясений. В соответствии с [16] ПТК, как компонент ИУС класса безопасности 3, отнесен к категории сейсмостойкости II и должен выполнять предусмотренные функции в заданном объеме с характеристиками, регламентированными в ТУ, после воздействия вибрации и механических ударов, вызванных проектным землетрясением на площадке АЭС. Интенсивность проектного землетрясения для площадки ЮУ АЭС определена в 6 баллов согласно ГОСТ 6249-92. В ТУ на КТС «Вулкан» установлены значительно более жёсткие требования к сейсмостойкости DPU – 8 баллов при установке на уровне до 10 м. Соответствие этим требованиям подтверждено материалами испытаний, представленных Westinghouse. Для коммерческих изделий (рабочих станций, видеомониторов, периферийного оборудования и др.), применённых в составе узлов верхнего уровня, данные по сейсмостойкости отсутствуют, что требует организации и проведения дополнительных испытаний. В качестве компенсирующего мероприятия было предусмотрено дополнительное крепление изделий, установленных на рабочих поверхностях столов и тумб.

Табл. 2 Характеристики ВВФ окружающей среды

Наименование и единица измерения	Значения ВВФ для группы условий эксплуатации				Значения ВВФ для ПТК	
	2.3 [16]		2.2 [16]		Узлы верхнего уровня	Узлы нижнего уровня
	Рабочие	Предельные	Рабочие	Предельные		
Температура, °С - нижнее значение - верхнее значение	 18 27	35	 15 30	50	 5 35	 5 40
Скорость изменения температуры, °С/ч верхнее значение		5		5		
Влажность, %: - нижнее значение - верхнее значение	20 80 при 27°С	90 при 35°С	10 75 при 30°С	100 при50°С	20 90 при 35°С	20 90 при 35°С
Барометрическое давление, кПа - нижнее значение - верхнее значение	 86 108		 86 108		 84 107	 84 107
Массовая концентрация пыли, мг/м^3 верхнее значение			1		1	1

Для изделий, которые отнесены к группам условий эксплуатации 2.2 и 2.3, требования по стойкости к электрическим полям и воздействию специальных сред не предъявляются.

Стойкость к изменению параметров электропитания регламентирована в [16] для изделий, подключаемых непосредственно к сети первичного питания, которые должны быть устойчивыми к изменениям параметров сети:

- отклонениям установившегося напряжения от минус 15% до плюс 10% без ограничения времени;
- отклонениям частоты от плюс 2% до минус 2% без ограничения времени и до минус 6% в течение 10 с;
- искажениям формы кривой напряжения (коэффициент гармонической составляющей – до 10%).

Прерывание электропитания (на время до 20 мс) при переключении источников питания не должно:

- вызывать отказы;
- требовать вмешательства персонала, например, для перезагрузки и/или перезапуска ПО;
- приводить к потерям информации в памяти ПТК.

Аналогичные требования установлены в ТУ на КТС «Вулкан». Соответствие этим требованиям подтверждено результатами заводских испытаний ПТК.

Электромагнитная совместимость подразумевает устойчивость всех составных частей ПТК к воздействию помех из сети питания, из спецконтура заземления, по цепям передачи сигналов и команд, линиям связи, локальным сетям, а также по пространству помещений.

Согласно [16] для изделий, отнесенных к классу безопасности 3 и предназначенных для работы в условиях электромагнитной обстановки средней жёсткости (характерной для помещений БЩУ, РЩУ и зала ИВС), должна устанавливаться группа исполнения по помехоустойчивости П3. Для этой группы исполнения степень жесткости при испытаниях на устойчивость к воздействию помех каждого вида должна соответствовать указанной в таблице 3.

В ТУ на КТС «Вулкан» установлены требования устойчивости по отношению к следующим видам помех:

- разрядам статического электричества на корпус, органы управления и внешние экраны кабелей;
- микросекундным импульсным помехам в цепях питания;
- наносекундным импульсным помехам на информационные цепи и цепи питания;
- магнитным полям промышленной частоты.

Соответствие ПТК указанным требованиям подтверждено результатами заводских испытаний.

По причине отсутствия на момент разработки отечественной нормативной базы, в ТУ на КТС «Вулкан» не были регламентированы требования по устойчивости к излученным радиочастотным помехам, динамическим изменениям напряжения электропитания, импульсным магнитным полям, кратковременным синусоидальным и микросекундным импульсным помехам в цепях защитного и сигнального заземления. После выхода нормативного документа [16] в ТУ были внесены соответствующие изменения и проведена дополнительная проверка, подтвердившая соответствие ПТК установленным требованиям.

Табл. 3 Степени жёсткости при испытаниях на помехоустойчивость

Вид помехи	Степень жёсткости при испытаниях	
	В соответствии с [16]	В соответствии с ТУ
Разряды статического электричества	3	3
Микросекундные импульсные помехи в цепях питания	3	2
Наносекундные импульсные помехи	3	2
Излученные радиочастотные помехи	2	–
Динамические изменения напряжения питания	3	–
Магнитные поля промышленной частоты: • непрерывные • кратковременные	 4 4	 4 –
Импульсные магнитные поля	4	–
Помехи в цепях заземления: кратковременные синусоидальные микросекундные импульсные	 3 3	 – –

Защита от несанкционированного доступа в ПТК обеспечена:

- введением идентификационных кодов, определяющих полномочия санкционированных пользователей и перечень устройств и функций, доступных каждому из них;
- архивированием и регистрацией всех действий персонала, связанных с изменением ПО и базы данных;
- использованием паролей (шифров) для разрешения наиболее ответственных действий;
- применением специальных замков на дверях несущих конструкций и их пломбированием.

Оценка безопасности

Лицензирование деятельности, связанной с реконструкцией ИВС, предусматривала оценку безопасности с целью обоснования возможности и определения условий выдачи разрешения на проведение каждого очередного этапа реконструкции. По поручению Регулирующего органа оценка безопасности проводилась Государственным центром по ядерной и радиационной безопасности (ГНТЦ ЯРБ) в процессе экспертизы документов, обосновывающих безопасность.

Следует заметить, что реконструкция ИВС совпала по времени с созданием основополагающих нормативных документов Украины, регламентирующих требования по ядерной безопасности и методику оценки соответствия информационных и управляющих систем (ИУС) и их компонентов этим требованиям [16, 17]. В процессе реконструкции отрабатывался и весь процесс лицензирования ИУС для украинских АЭС.

Целью экспертизы было установление соответствия реконструированной системы и её компонентов установленным для них регулирующим требованиям, перечень которых был сформирован на основе сравнительного анализа действующих в Украине и разрабатываемых нормативных документов, а также международных стандартов и руководств по безопасности АЭС. С другой стороны, в процессе экспертизы проходили проверку и практическую апробацию и сами разрабатываемые нормативные документы, что, без сомнения, способствовало повышению их качества.

По результатам экспертизы «Технического решения ЮУ АЭС о реконструкции ИВС блока 1» и «Концепции реконструкции» был разработан и утверждён Регулирующим органом документ «Порядок и содержание работ для получения разрешения на ввод в эксплуатацию информационно-вычислительной системы (ИВС) на блоке 1 ЮУ АЭС».

При проведении экспертизы был принят следующий подход:

- составлен перечень регулирующих требований, которые установлены действующими в Украине нормативными актами, стандартами, другими нормативными документами и относятся к системе в целом и к ее компонентам (программно-техническим комплексам, техническим средствам и программному обеспечению);
- рассмотрено соответствие технического задания на реконструкцию ИВС энергоблока №1 ЮУ АЭС и технических условий на КТС “Вулкан” регулирующим требованиям (по результатам экспертизы разработчиками внесены необходимые изменения в текст документов, после чего ТЗ и ТУ были согласованы Регулирующим органом);
- рассмотрены доказательства соответствия системы и ее компонентов регулирующим требованиям, а также требованиям ТЗ и ТУ (с учетом проведенных в них изменений).

Такие доказательства должны были содержаться в документах, которые являлись предметом экспертизы:

- программе обеспечения качества;
- проектной документации;
- материалах (плане, отчете) по верификации и валидации;
- отчете по анализу безопасности;
- материалах заводских испытаний ПТК;
- материалах предварительных испытаний ПТК на площадке заказчика и приемочных испытаний ИВС.

В таблице 4 дан перечень регулирующих требований, требований ТЗ и ТУ, а также подтверждение соответствия этим требованиям реконструированной системы и её компонентов (ПТК, ПО), приведенные в документах, обосновывающих безопасность.

Табл. 4 Подтверждение соответствия ИВС регулирующим требованиям, требованиям ТЗ и ТУ

Требования	Подтверждение соответствия в документах					
	Программе обеспечения качества	Проектной документации	Материалах заводских испытаний ПТК	Отчете по анализу безопасности	Материалах по верификации и валидации	Материалах приемочных испытаний ИВС
К выполняемым функциям		+	+	+	+	+
К показателям надежности			+	+		+
К соблюдению принципа резервирования		+		+		
К структуре и элементам ПО				+	+	
К защите от отказов по общей причине		+		+		
К диагностированию и самоконтролю			+	+	+	+
К точности			+	+		+
К временным характеристикам			+	+		+
К человеко-машинному интерфейсу		+	+	+		+
По стойкости к внешним воздействиям:						
• окружающей среды			+	+		
• механическим			+	+		
• параметров электропитания		+	+	+		
К электромагнитной совместимости			+	+		
К соблюдению принципа независимости		+		+		
К изоляции			+	+		
К пожаробезопасности		+	+	+		

К защите от несанкционированного доступа		+	+	+	+	+
К апробации	+			+		
К испытаниям и приемке	+		+	+		+
К верификации программного обеспечения	+			+	+	
К разработке программного обеспечения	+			+	+	
К качеству выполнения работ	+			+		
+ является обязательным						

Результаты проведенных экспертиз изложены в экспертных заключениях ГНТЦ ЯРБ:

- по техническому решению ЮУ АЭС о реконструкции блока №1 и концепции реконструкции;
- по техническим условиям на комплекс технических средств «Вулкан»;
- по техническому заданию на реконструкцию информационно-вычислительной системы блока №1 ЮУ АЭС;
- по документации проекта информационно-вычислительной системы (ПТК) блока №1 ЮУ АЭС;
- по программе обеспечения качества информационно-вычислительной системы блока №1 ЮУ АЭС;
- по плану верификации программного обеспечения комплекса «Вулкан-ИВК» энергоблока №1 ЮУ АЭС;
- по отчету по анализу безопасности информационно-вычислительной системы блока №1 ЮУ АЭС;
- по документации испытаний информационно-вычислительной системы на площадке поставщика;
- по программе и методике приемочных испытаний информационно-вычислительной системы блока №1 ЮУ АЭС;
- по документации испытаний и метрологической аттестации информационно-вычислительной системы блока №1 ЮУ АЭС.

Указанные экспертные заключения содержали замечания, которые устранены в новых редакциях документов или приняты разработчиками и учтены в рабочем порядке, что отмечено в соответствующих протоколах (отдельные замечания экспертов были сняты после предоставления разработчиками необходимых обоснований).

На основании оценки документации и результатов испытаний, изложенных в экспертных заключениях ГНТЦ ЯРБ, был сделан вывод о том, что информационно-вычислительная система энергоблока №1 ЮУ АЭС после реконструкции удовлетворяет требованиям по ядерной и радиационной безопасности, требованиям ТЗ на реконструкцию ИВС и ТУ на КТС “Вулкан-ИВК” и может быть принята в постоянную эксплуатацию.

ЗАКЛЮЧЕНИЕ

Впервые на украинских АЭС центральная часть информационной системы энергоблока заменена программно-техническим комплексом, который разработан украинскими специалистами на основе передовых информационных технологий с использованием технических средств мирового уровня, и сертифицирован для применения на АЭС Украины.

Реконструированная ИВС энергоблока №1 ЮУ АЭС впервые в Украине прошла полный цикл лицензирования. ИВС была признана соответствующей требованиям нормативных документов по ядерной безопасности, действующих в Украине к моменту внедрения системы, и руководствам международных организаций по безопасности.

Успешный опыт эксплуатации ИВС блока №1 ЮУ АЭС в течение четырех лет подтвердил правильность принятых решений, которые могут быть использованы при реконструкции аналогичных систем на других атомных энергоблоках Украины.

ЛИТЕРАТУРА

1 В.Т.Безсалый, В.Н.Васильченко, А.И.Волошин и др. Обеспечение и оценка безопасности цифровой системы управления оборудованием машзала АСУТ-1000М. Ядерная и радиационная безопасность, №1, 2001.

2 М.А.Ястребенецкий, Ю.В.Розен, В.Н.Васильченко. Нормирование и оценка безопасности информационных и управляющих систем АЭС (1): объекты, цели, задачи. Ядерная и радиационная безопасность, №1, 2001.

3 Westinghouse Distributed Process Family WDPF-II. Проспект фирмы Westinghouse Electric Corporation.

4 ДСТУ 3451-96 Технічні засоби для розподілених автоматизованих систем керування технологічними процесами. Загальні вимоги до спряження виробів.

5 М.А.Ястребенецкий, Ю.В.Розен, В.Н.Васильченко. Нормирование и оценка безопасности информационных и управляющих систем (6): регулирующие требования к техническим средствам. Ядерная и радиационная безопасность, №4, 2001.

6 Перелік чинних норм та правил з ядерної та радіаційної безпеки. Затверджено наказом Міністерства охорони навколишнього середовища та ядерної безпеки України від 04.01.1998 р. №1.

7 ПНАЭ Г-1-011-89. Общие положения обеспечения безопасности атомных станций. (ОПБ-88).

8 ПНАЭ Г-1-024-89. Правила ядерной безопасности реакторных установок атомных станций. (ПБЯ РУ АС-85).

9 ПНАЭ Г-5-006-87. Нормы проектирования сейсмостойких атомных станций.
10 ГОСТ 24.104-85. Автоматизированные системы управления. Общие требования.
11 ГОСТ 29075-91. Системы ядерного приборостроения для атомных станций. Общие требования.
12 ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
13 ГОСТ 24.701-86. ЕСС АСУ. Надежность АСУ.
14 IEC 60880-86. Software for computers in the safety systems of nuclear power stations.
15 М.А. Ястребенецкий, Ю.В. Розен, В.Н. Васильченко. Нормирование и оценка безопасности информационных и управляющих систем АЭС (2): принципы нормирования. Ядерная и радиационная безопасность, №2, 2001.
16 НП 306.5.02/3.035-2000. Требования по ядерной и радиационной безопасности к информационным и управляющим системам, важным для безопасности атомных станций.
17 ГНД 306.7.02/2.041-2000. Методика оценки соответствия информационных и управляющих систем, важных для безопасности атомных станций, требованиям по ядерной и радиационной безопасности.

Н.В. Афанасьев, О.М.Белохин, О.Бренман, В.М.Гольдрин, В.М. Васильченко, Л.М.Корчагин, В.Ф. Редько, Ю.В. Розен, М.А.Чернишов, М.О.Ястребенецький

ЗАБЕЗПЕЧЕННЯ ТА ОЦІНКА БЕЗПЕКИ ІНФОРМАЦИЙНО-ОБЧІСЛЮВАЛЬНОЇ СИСТЕМИ ЕНЕРГОБЛОКА АЕС З РЕАКТОРОМ ВВЕР-1000

Починаючі с 2002 року журнал «Ядерна та радіаційна безпека» публікує серію статтей, присвячених досвіду забезпечення і оцінки безпеки нових інформаційних і керуючих систем, які впроваджено на АЕС України. У цій статті, що продовжує серію, розглядаються результати робіт щодо реконструкції інформаційно-обчислювальної системи енергоблоку №1 Южноукраїнської АЕС із використанням комплексу технічних засобів "Вулкан", що виготовлен підприємством Вестрон (м. Харків) на базі обладнання фірми Westinghouse Electric Corporation (США).

N.Afanasiev, O.Belokhin, O.Brenman, V.Goldrin, V.Vasilchenko, L.Korchagin, V.Redko, Y.Rozen, M.Chernyshov, M.Yastrebenetsky

ASSURANCE AND SAFETY ASSESSMENT OF I&C SYSTEM OF NPP POWER UNIT WITH VVER-1000 REACTOR

Since 2002 a set of articles devoted to the experience of the assurance and safety assessment of new instrumentation and control systems implemented at Ukrainian NPPs is been published in the magazine "Nuclear and Radiation Safety. In this article continuing this set the results of works on reconstruction of computer information system of power unit № 1 of Uzgnoukrainskaya NPP with use of hardware complex "Vulkan" manufactured by Company "Westron" (Kharkov) on the basis of equipment of Westinghouse Electric Corporation (USA) are considered.

Назад на страницу
Масс-медиа о Вестроне