Канд.физ.-мат. наук А.О. Мирошник

ОСОБЕННОСТИ ВЕРИФИКАЦИИ И ВАЛИДАЦИИ ПРОГРАММНО-ТЕХНИЧЕСКИХ КОМПЛЕКСОВ ВТОРОГО КЛАССА БЕЗОПАСНОСТИ В СОСТАВЕ ЭЛЕКТРООБОРУДОВАНИЯ СУЗ РЕАКТОРОВ ВВЭР

Введение

В ранее опубликованной статье [1] был рассмотрен один из возможных подходов к достижению целостности программного обеспечения (программных средств) в составе компонентов электрооборудования СУЗ, построенных с применением средств вычислительной техники (СВТ) и относящихся к третьему классу безопасности в соответствии с [2]. Применимость данного подхода была продемонстрирована в процессе проведения процедур верификации и валидации шкафов контроля положения и управления органами регулирования реактора (ШКУ), шкафов автоматического регулирования мощности (АРМ) и разгрузки реактора (РОМ), шкафов групповой индикации (ШГИ). Все вышеперечисленное оборудование успешно прошло описанную процедуру верификации и валидации, было принято представителями уполномоченных надзорных органов по ядерной и радиационной безопасности (ГАН РФ, ВО «Безопасность») и успешно эксплуатируется на отечественных АЭС – Калининской, Нововоронежской и зарубежных – Тяньвань (КНР), Бушер (ИРИ), оснащенных водо-водяными энергетическими реакторами (ВВЭР).

Однако современная концепция создания оборудования управления и защиты перспективных реакторных установок с реакторами ВВЭР предполагает широкое использование вычислительных систем (ВС), состоящих из программно-технических комплексов (ПТК), построенных с применением СВТ и имеющих программные средства (ПС) в своем составе. При этом, по крайней мере, в качестве одного из двух обязательных комплектов инициирующей части аварийной защиты реакторной установки

предполагается использование ПТК на базе СВТ. С целью обеспечения возможности реализации таких проектов в НПП ВНИИЭМ ведется разработка базовых аппаратно-программных средств цифровой системы аварийной защиты реактора ВВЭР [3]. В связи с этим, встает вопрос о практической реализации процедур верификации и валидации (ВВ) для ПС в составе оборудования второго класса безопасности. Учитывая опыт, накопленный в процессе проведения процедур ВВ для оборудования третьего класса безопасности [1], и ограниченный объем данной статьи, представляется целесообразным остановиться только на принципиальных моментах процедуры ВВ для оборудования второго класса безопасности.

Естественно по своему объему данная статья не может охватить всей проблематики вопросов, связанных с выполнением работ по ВВ ПС в составе оборудования второго класса безопасности. Имеется ряд отечественных нормативных документов гораздо большего объема и более подробно, освещающих данную тематику [4, 5]. Цель статьи заключается в попытке обобщить имеющийся практический опыт проведения работ по ВВ для оборудования второго класса безопасности, выделив этапы работ, выполнение которых является принципиально важным для оборудования второго класса, но которые могли выполняться не в полном объеме для оборудования третьего класса безопасности [1].

Этапы жизненного цикла программных средств

Современная технология разработки, внедрения и эксплуатации СВТ опирается на модель жизненного цикла ВС и входящих в их состав программных средств (программных изделий) [6]. Жизненный цикл разбивается на ряд крупных фаз или этапов, каждый из которых характеризуется достаточно определенными целями и результатами. Цели и задачи, решаемые в процессе разработки вычислительной системы, определяют ее архитектуру и структуру компонентов, регламентируют конкретные функции, выполняемые системой.

Жизненный цикл включает в себя описание исходной информации, способов и методов выполнения операций и работ, устанавливает требования к результатам и правилам их контроля, а

также определяет содержание технологических и программных документов. Он определяет организационную структуру коллектива, обеспечивает распределение и планирование работ, а также контроль за ходом разработки.

В случае разработки программных средств, входящих в состав ПТК второго класса безопасности, являющегося частью электрооборудования СУЗ реактора (далее вычислительной системы - ВС), жизненный цикл ПС должен состоять из следующих этапов (см. таблицу).

Если в случае ВС третьего класса безопасности часть этапов могла быть пропущена или совмещена [1], то для систем второго класса безопасности все этапы являются обязательными и минимально необходимыми.

План проведения работ по верификации и валидации

Перед началом работ по ВВ ПС ПТК (см. таблицу, этап 1) должны быть выпущены планы работ по верификации и валидации (допускается выпуск единого плана работ по верификации и валидации).

План верификации должен определять [7, 8]:

– цели верификации (спецификация требований, содержащая перечень требований и решений предыдущего этапа жизненного цикла, выполнение которых на текущем этапе жизненного цикла должно быть проверено);

– критерии достижения цели для каждого этапа верификации (порядок оценки результатов верификации);

– рекомендуемые методы проверок, аппаратные средства и программные средства, необходимые для проведения проверок, должностных лиц, выполняющих верификационные проверки и испытания;

– вид, требования к оформлению и содержанию документов, оформляемых по результатам проверок и испытаний (верификации);

– организацию работ (графики выполнения работ, оценку требуемых ресурсов, распределение обязанностей и ответственность).

Отдельные части плана верификации, имеющие самостоятельное значение (программы, методики испытаний и т.п.), могут быть выпущены в виде самостоятельных документов.

Этап разработки ПС	Продукт разработки	Этап верификации
1	2	3
1.Постановка задачи	Спецификация требований к вычислительной системе (техническое задание и технический проект на ВС)	Планирование и организация работ по верификации и валидации
		Подготовка планов верификации и/или валидации разрабатываемых ПТК в составе ВС
2.Спецификация требований к ПС ПТК	Спецификация требований к ПС ПТК (техническое задание на ПС ПТК)	Верификация спецификации требований к ПС ПТК (технического задания на ПС ПТК)
	Предварительная редакция программы тестирования ПС ПТК	Верификация предварительной редакции программы тестирования ПС ПТК
3. Разработка проекта ПС ПТК	Проектные спецификации ПС ПТК (алгоритмы)	Верификация проекта ПС ПТК (алгоритмов)
	Предварительная программная документация ПС ПТК	Верификация предварительной программной документации на ПС ПТК
	Скорректированная программа тестирования ПС ПТК	Проверка скорректированной программы тестирования ПС ПТК
4. Программирование ПС ПТК	Исходные тексты	Верификация исходных кодов ПС ПТК
	Откорректированная программная документация на ПС ПТК	Верификация откорректированной программной документации на ПС ПТК
	Окончательный вариант программы тестирования ПС ПТК	Верификация окончательного варианта программы тестирования ПС ПТК

Продолжение табл.

1	2	3
5. Интегрирование ПС ПТК	Интегрированные ПС ПТК	Верификация интегрированных ПС ПТК
	Программа тестирования ПС ПТК	Верификация результатов тестирования ПС ПТК
6. Автономное тестирование ПТК	Инсталляционный пакет	Верификация инсталляционного пакета
	Окончательный вариант программной документации ПС ПТК	Верификация окончательного варианта программной документации ПТК
	Программа тестирования ПТК (план валидации)	Отчет о валидации (тестировании) ПТК
7. Комплексные испытания ПТК в составе ВС и ввод в эксплуатацию на объекте	Программа комплексного тестирования (план валидации) ПТК в составе ВС	Отчет о валидации (комплексных испытаниях) ПТК в составе ВС
	Завершение работ по верификации и валидации на территории предприятия изготовителя	
	Проведение пусконаладочных работ на площадке АЭС, выпуск отчета о верификации и валидации	
8. Эксплуатация и сопровождение ПС ПТК	Изменения в ПС и программной документации ПТК	При необходимости повторение вышеуказанных мероприятий

План валидации ПТК должен включать:

– окружение (состав комплекса технических средств (КТС) и ПС), в котором выполняется тестирование;

– процедуры тестирования;

– критерии приемки, т.е. детальное изложение критериев, которым должен удовлетворять ПТК;

– процедуры обнаружения ошибок;

– список необходимой документации, которая должна быть подготовлена при выполнении валидации.

План валидации (либо соответствующий раздел плана проведения работ по верификации и валидации) должен включать подтверждение правильности функционирования ПТК:

– в статическом и в динамическом режимах;

– нормальном режиме эксплуатации;

– в предаварийном режиме работы и аварийных ситуациях (необходимо предусмотреть различные эксплуатационные ситуации).

В плане валидации необходимо указать требуемые входные сигналы и их значения, предполагаемые выходные сигналы и критерии их приема.

Правильность выполнения каждой функции должна быть подтверждена представительными тестами по каждому входному параметру, причем выполнять это необходимо как для отдельных параметров, так и для их комбинаций.

Рекомендуется, чтобы в процессе испытания:

– охватывались все диапазоны изменения сигналов, а также диапазоны вычисляемых или расчетных параметров;

– полностью охватывались логические процедуры и комбинации логических процедур;

– использовалась штатная конфигурация системы для всех случаев аномальных сигналов;

– охватывались все диагностические функции ПС и системы;

– обеспечивался контроль временных характеристик ПС, выполнения функций и контроль загрузки КТС;

– обеспечивалось подтверждение точности измерений и времени реакции, а также правильность действий в случае любого отказа оборудования или комбинации отказов.

Спецификация требований к вычислительной системе

Спецификация требований к вычислительной системе (см. таблицу, этап 1) – это описание объединенной системы КТС и ПС с указанием целей создания и функций ВС. Назначение спецификации требований к ВС заключается в том, чтобы [9–11]:

– указать общее назначение ПС с определением точных ограничений и с указанием того, что ПС не должно выполнять;

– перечислить ожидаемый объем и производительность ПС и точно указать, что является просто плановыми (намеченными) цифрами, а что абсолютно необходимо для системы;

– указать качественные характеристики системы в форме математического ожидания для значений ее параметров (например требуемую точность);

– привести требования к загруженности ВС при работе ПС во всех проектных режимах работы энергоблока;

– привести требования к КТС;

– привести требования к режимам взаимодействия с абонентами системы;

– классифицировать цели создания ВС в соответствии с их приоритетом.

В спецификации требований к ВС описываются функции, которые должна выполнять ВС. Документ должен содержать описание функций и начальных условий для различных режимов функционирования АЭС. В описании должна быть указана связь этих функций с общей концепцией функционирования АЭС и функциями управления другими системами.

Документ «Спецификация требований к ВС» является основополагающим документом при проведении работ ПО ВВ и, в зависимости от конкретного проекта и требований заказчика, может охватывать стадии работ с 1-й по 5-ю в соответствии с [12, п.2.1.] и состоять из комплекта отдельных документов в соответствии с [13].

Содержание и структура отдельных документов в составе «Спецификации требований к вычислительной системе» определяется требованиями [15, 16], что вполне соответствует зарубежным стандартам [9–11]. «Спецификация требований к вычислительной системе» должна включать в себя следующие разделы:

– конфигурация вычислительной системы;
– требования к человеко-машинному интерфейсу;
– внутренние и внешние интерфейсы;
– описание функций системы;
– структура и взаимосвязь данных;
– описание разграничения функций между КТС и ПС;
– описание специальных рабочих условий;
– требования к самоконтролю ВС;
– требования к надежности ПС.

Наиболее полная и подробная трактовка содержания каждого из вышеприведенных разделов наряду с [15] содержится в документе [4].

Спецификация требований к программным средствам

Требования к ПС ПТК в составе ВС (см. таблицу, этап 2) должны быть разработаны с учетом требований, предъявляемых к системам, важным для безопасности АЭС, и являются частью спецификации вычислительной системы. Документ «Спецификация тре-

бований к ПС», разрабатывается на 4-й стадии работ в соответствии с [12, п.2.1.] и выполняется в соответствии с [14, 15].

В требованиях к ПС должны быть описаны требования к ПС как к изделию. В них должно быть указано, что необходимо делать, а не как делать. Функциональные требования к ПС должны быть представлены в виде, понятном для каждой группы пользователей. Документ должен быть подготовлен до начала реализации этапа проектирования и программирования.

Требования должны быть недвусмысленными, поддающимися легко реализуемым испытаниям или проверке. В документе, содержащем требования к ПС, должно быть проведено четкое разграничение между существенными требованиями и менее жесткими (второстепенными) требованиями.

Применение формального языка спецификаций может обеспечить наглядность согласованности и полноты функциональных требований к ПС.

Для удовлетворения требованиям [17] «Спецификация требований к ПС» должна включать в себя следующие разделы:

- спецификация вычислительной системы;
- конфигурация вычислительной системы;
- требования к человеко-машинному интерфейсу;
- требования к внутренним и внешним интерфейсам;
- описание функций системы;
- структура и взаимосвязь данных;
- описание разграничения функций между ВС и ПС;
- требования к специальным условиям работы ПС;
- требования к надежности ПС.

Основные требования к программным средствам

Основные требования к ПС в составе оборудования второго класса безопасности сформулированы в документах [9–11], в соответствии с требованиями которых:

– ПС должно проектироваться в соответствии с принципами структурного или объектно-ориентированного программирования. ПС, как правило, должно выполняться в виде законченных модулей смыслового характера (один модуль - одна функция). Текст модуля должен содержать, как правило, не более 100 операторов исходного языка;

– должна быть предусмотрена возможность периодического тестирования, например во время останова АЭС. Тестированию должна

подвергаться каждая функция системы. Должна быть предусмотрена возможность самопроверки. Самопроверка не должна увеличивать время задержки реакции системы выше допускаемых пределов, а также негативно влиять на обеспечение безопасности АЭС;

– ПС должно быть разделено таким образом, чтобы программы, обслуживающие оператора, были отделены от прикладных программ. Программы различного функционального назначения должны быть снабжены защитными устройствами от возможных взаимных искажений при сбоях и ошибках;

– в ПС должны быть предусмотрены:

- программные средства защиты от искажений входной информации, поступающей от измерительных средств и по каналам связи от смежных систем;
- программные средства защиты от сбоев и частичных отказов вычислительных средств, в том числе по общей причине;
- средства, предотвращающие несанкционированный доступ к программам и информации;
- средства защиты программ и информации от ошибочных действий персонала;
- средства операторского подтверждения запроса на вмешательство в работу программ, влияющих на безопасность;
- программные средства защиты от искажений информации в аварийных режимах работы энергоблока;
- средства тестирования и самопроверки;

– программное и информационное обеспечение должно строиться на единой системе программных средств (программных библиотек), иметь единую структуру и организацию данных, снабжаться соответствующей программной документацией.

Задача практической верификации алгоритмов функционирования и исходных кодов программных средств

Являясь основополагающими документами по вопросам ВВ ПС в системах безопасности АЭС [9–11], данные документы не содержат практических пошаговых схем выполнения процедур верификации на различных этапах жизненного цикла ПС. К сожалению, аналогичная ситуация имеет место и для большинства отечественных нормативных документов по ВВ, что порождает формальные трудности как при проведении собственно процесса верификации, так и при предъявле-

нии результатов верификации представителям уполномоченных надзорных органов по ядерной и радиационной безопасности.

В связи с этим, представляется целесообразным использовать в качестве руководящего документа при проведении работ по верификации (см. таблицу, этапы 1–6) документ [18], содержащий детализированные контрольные таблицы для всех этапов верификации.

В качестве наиболее часто встречающегося примера, рассмотрим применение данного документа [18] на этапе верификации алгоритмов функционирования (проектных спецификаций ПС) и исходных кодов ПС ПТК (см. таблицу, этапы 3, 4).

С точки зрения автора, столь обширное цитирование является оправданным в связи с малой доступностью документа [18] и актуальностью рассматриваемой проблемы верификации.

Ниже приведены основные вопросы, которые должны быть освещены в процессе верификации алгоритмов функционирования и исходных текстов ПС и детализация этих вопросов до уровня, предполагающего конкретный однозначный ответ. Принимая такой подход, удается избежать субъективных оценок как со стороны специалистов, выполняющих процесс верификации, так и со стороны представителей уполномоченных надзорных органов, принимающих результаты работ.

Верификация алгоритмов функционирования ПС ПТК

Соответствуют ли проектные спецификации ПС требованиям стандартов по документации?

а) имеются ли все необходимые разделы;

б) содержит ли каждый из разделов всю необходимую информацию;

в) выполняются ли требования к форме документа.

Соответствуют ли проектные спецификации ПС техническому заданию?

а) все ли требования реализованы в проекте;

б) все ли свойства проекта соответствуют требованиям;

в) позволяют ли числовые методы, реализованные в проекте, решить поставленные задачи;

г) позволяют ли алгоритмы, определенные проектом, решить поставленные задачи;

д) соответствует ли разбиение проекта программы на части поставленным задачам;

е) будет ли программа, выполненная по рассматриваемому проекту, соответствовать требованиям.

Является ли проект полным?

а) реализовано ли в проекте требуемое поведение программы относительно каждого из ее интерфейсов;

б) все ли необходимые входные и выходные данные программы и элементы баз данных определены и описаны так, как требуется для кодирования программы;

в) описана ли в проектных спецификациях ПС операционная среда, в которой должна устанавливаться программа;

г) включены ли все необходимые этапы обработки данных;

д) учтены ли в алгоритмах все возможные варианты ведения программы;

е) учтены ли в проекте все ожидаемые ситуации и условия;

ж) определено ли в проекте оптимальное поведение программы при непредусмотренных или несовместимых входных данных и других ненормальных условиях;

з) имеются ли в спецификациях ссылки на все использованные при разработке проекта стандарты по программированию.

Правилен ли проект?

а) представляется ли проект логичным, т. е. будет ли программа выполнять то, для чего она предназначена;

б) соответствует ли проект документированным описаниям и известным свойствам операционной среды, в которой должна устанавливаться программа;

в) правильно ли размещены в проекте все входные и выходные данные и элементы базы данных, формат которых, а также содержание, скорость передачи данных и т.д. не определяются разработчиками;

г) соответствуют ли примененные в проекте модели, алгоритмы и числовые методы существующим стандартам.

Являются ли компоненты проекта совместимыми между собой?

а) не имеется ли в проекте внутренних противоречий;

б) являются ли модели, алгоритмы и предусмотренные соответствующие числовые методы математически совместимыми;

в) являются ли совместимыми форматы входных и выходных данных;

г) обеспечивается ли в проекте совместимость сходных или связанных функций;

д) совместима ли точность входных и выходных данных и элементов базы данных, используемых совместно для вычислений или принятия логических решений;

е) являются ли стиль оформления и уровень детализации одинаковым во всем документе.

Является ли проект четким и недвусмысленным?

а) вся ли проектная информация понятна;

б) одним ли только образом может быть истолкована проектная информация;

в) организован ли и представлен ли проект в форме, способствующей повышению их ясности (например с использованием таблиц и перечней вместо обычного текста);

г) достаточно ли детализирован проект, чтобы предотвратить неправильное его толкование.

Выполним ли Проект программы?

а) являются ли модели, алгоритмы и предусмотренные соответствующие числовые методы оптимальными и современными;

б) могут ли они быть реализованы при имеющихся системных ограничениях и возможностях разработчика;

в) возможна ли реализация требуемых функций при располагаемых ресурсах.

Проверка Исходного кода ПС ПТК

Соответствует ли исходный код требованиям установленных стандартов и методик?

а) соответствует ли исходный код стандартам ЕСПД. ГОСТ 19.xxx;

б) соответствует ли исходный код стандартам ЕСПД. ГОСТ 19.xxx по языкам программирования, если такие стандарты имеются;

в) соответствует ли исходный код другим специальным стандартам по разработке программ.

Являются ли предусмотренные операторы комментариев достаточными для надлежащего описания каждой из подпрограмм?

а) правильно ли описаны входные и выходные переменные;

б) описаны ли используемые в подпрограммах постоянные;

в) все ли вычисления и задачи объяснены;

г) четко ли объяснены процедуры чтения и записи файлов входных/выходных данных.

Легко ли понимается исходный код?

а) удалось ли избежать неоднозначной или излишне сложной кодировки;

б) использовано ли структурированное расположение текста для более легкого его понимания;

в) не использован ли самоизменяющийся код.

Является ли исходный код логически соответствующим проектным спецификациям?

а) все ли свойства проекта полностью и правильно реализованы в коде;

б) все ли свойства закодированного ПС ПТК основаны на проектных спецификациях.

Все ли переменные должным образом определены и использованы?

а) отсутствуют ли в программе неиспользуемые переменные;

б) для всех ли переменных заданы начальные значения;

в) совместимы ли индексы массивов;

г) не выходят ли значения переменных цикла за пределы массивов;

д) правильно ли определены постоянные;

е) соответствующие ли единицы измерения использованы для каждой из переменных.

Имеется ли соответствующий контроль ошибок?

а) проверяются ли входные данные на соответствие принятому для них диапазону значений;

б) проверяются ли внешние файлы данных на правильность формата записанных в них данных;

в) проверяются ли вычисления на достоверность полученных результатов;

г) завершается ли процесс выявления ошибки соответствующими процессами сообщения об ошибке и устранения ошибки.

Всеми ли подпрограммами правильно вызываются переменные переноса данных?

а) являются ли количество переменных и тип каждой из переменных одинаковыми, как в вызывающей, так и в вызываемой подпрограммах;

б) совпадают ли во всем тексте программы имена переменных, помеченных как общие, а также типы, размещение и размеры массивов.

Совпадают ли данные, считываемые из каждого из файлов, с данными, записываемыми в данный файл?

а) совпадают ли количество и тип переменных;

б) совпадают ли номера блоков.

Показывают ли результаты тестирования блоков следующее?

а) что каждый из главных логических путей подпрограммы был протестирован;

б) что каждая из подпрограмм была проверена на минимальное, максимальное и среднее множества переменных;

в) что результат работы подпрограммы одинаков при одинаковых входных данных.

При этом для систем второго класса безопасности работы по аудиту исходных текстов ПС и проверке его соответствия разработанным алгоритмам функционирования желательно проводить в сторонней экспертной организации, организационно и финансово независимой от разработчика ПС и алгоритмического обеспечения.

При выборе сторонней организации для выполнения функций независимого эксперта в качестве критерия должны выступать требования:

– наличия у организации лицензии надзорных органов (Ростехнадзора) на разработку программного обеспечения для АЭС;

– опыт проведения ранее аналогичных работ по верификации программного обеспечения;

– наличие кадрового потенциала, обладающего квалификацией не ниже разработчиков программного обеспечения.

При обнаружении в исходных текстах программ участков кода, вызывающих трудности в понимании или неоднозначности в трактовке [19, 20] по рекомендации сторонней организации, по отдельным программам-методикам проводятся автономные испытания модулей, в которые входят данные фрагменты кода.

Результаты испытаний предоставляются в экспертную организацию, проводившую аудит исходных текстов программ, и включаются в подготавливаемый ею отчет о верификации исходных текстов ПС.

Проекты и работы, связанные с разработкой ПС, рекомендуется оформлять в соответствии с требованиями, предъявляемыми Единой Системой Программной Документации (ЕСПД, ГОСТы 19.ххх) [14, 21]. ЕСПД является набором стандартов, который определяет:

– стадии и этапы разработки, виды и обозначения программных документов;

– общие требования к оформлению текстовых программных документов;

– требования к содержанию и оформлению отдельных программных документов;

– схемы алгоритмов.

Стандарты ЕСПД упорядочивают процесс документирования программных средств. Предусмотренный стандартами ЕСПД состав программных документов не определяет однозначной "жесткой" схемы документирования, ограничивающей проведение работ по ВВ, стандарты позволяют вносить в комплект документации на программные системы дополнительные виды документов, кроме того, исходя из требований заказчика (при ссылке на них в договоре на разработку (поставку) программных средств и систем), допустимы изменения, как в структуре, так и в содержании установленных видов программной документации.

Валидация программно-технических комплексов

Цель валидации (соответствующих функциональных испытаний ПТК) состоит в подтверждении:

– правильности функционирования ПТК;

– соответствия ПТК требованиям к функциональным и эксплуатационным свойствам, а также требованиям к интерфейсам.

Валидацию ПТК необходимо проводить в соответствии с отдельным планом валидации (либо соответствующим разделом плана проведения работ по верификации и валидации).

Результаты испытаний ПТК должны быть документально оформлены в виде отчета о валидации. Отчет о валидации должен содержать следующие разделы:

– конфигурация, используемая при тестировании (КТС и ПС, которые использовались в процедуре валидации);

– оборудование, используемое при испытаниях, и сведения о его калибровке;

– используемые имитационные модели;

– список тестируемых входных данных;

– список тестируемых выходных данных;

– используемые методы имитации энергетической установки и ее систем или интерфейсных компонентов, которые использовались в процедуре верификации;

– дополнительные данные (синхронизация, последовательность событий и др.);

– соответствие критериям приемки, указанным в плане валидации;

– протокол регистрации выявленных отклонений, в котором приводится описание типа ошибки и выполненные корректирующие действия.

Фактически, отчет о валидации допустимо представлять в виде комплекта документов, состоящего из программ-методик испытаний и протоколов по результатам проведенных испытаний, так как все вышеприведенные пункты отчета о валидации должны в той или иной форме содержаться в этих документах. При этом отчеты о валидации должны быть представлены в виде, который позволяет проверить их лицам, непосредственно не участвовавшим в процедуре валидации [9–11].

Для удобства проведения валидационные испытания удобно разделять на:

– автономные испытания разрабатываемого ПТК с использованием универсального испытательного и отладочного оборудования;

– автономные испытания разрабатываемого ПТК с использованием специализированного тестового оборудования (комплектов проверки шкафов);

– комплексные испытания ПТК, проводимые в условиях стендовых и полигонных фрагментов вычислительных систем;

– автономные и комплексные испытания ПТК в процессе пусконаладочных работ на площадке АЭС.

Приемосдаточные и приемочные испытания разрабатываемого ПТК должны включаться в состав валидационных испытаний либо как самостоятельные испытания, либо в виде части одного из типов испытаний, перечисленных выше.

Заключение

Изложенная ранее [1] и дополненная в данной статье методика проведения работ по ВВ оборудования второго класса безопасности была применена для проведения процедур ВВ каналов контроля положения органов регулирования реактора (ККПОР) в составе электрооборудования системы группового и индивидуального управления (СГИУ) 5-го, 6-го блоков АЭС «Козлодуй»», которые в соответствии с требованиями болгарского заказчика разрабатывались и аттестовывались по второму классу безопасности [2].

В состав ККПОР входят одноплатный технологический контроллер ОМК24 шкафа контроля и управления (SHKU1N) и подключаемый к нему индикатор положения органов регулирования реактора (IP261N).

Контроллер ОМК24 осуществляет непосредственное взаимодействие с датчиками положения органов регулирования реактора ДПШ (датчик положения шаговый), выполняет функции диагностики датчиков и блоков питания датчиков (БП ДПШ), является источником первичной информации о положении органов регулирования для электрооборудования СГИУ и смежных систем, а также, совместно с индикаторами положения органов регулирования IP261N, обеспечивает представление информации по положению ОР на блочный и резервный пульты управления АЭС.

В процессе проведения работ по верификации и валидации:

– был выпущен план проведения работ по ВВ и программа обеспечения качества разработки и изготовления оборудования, включая ПС;

– выполнены работы, предусмотренные методикой ВВ, изложенной в [1] и в данной статье;

– проведен аудит исходных текстов ПС в сторонней экспертной организации (ООО «Аскит-Атом» - дочернее предприятие ФГУП «НИКИЭТ»);

– проведены испытания алгоритмов функционирования ПС, автономные и комплексные испытания оборудования на территории ФГУП «НПП ВНИИЭМ»;

– проведены автономные и комплексные испытания в процессе пусконаладочных работ на площадке АЭС «Козлодуй»;

– подготовлен итоговый комплект документов по ВВ, включая отчет по ВВ, прошедший экспертизу в сторонней экспертной организации и принятый уполномоченными надзорными органами (ГАН РФ) и Заказчиком.

По завершении работ по ВВ оборудование ККПОР было аттестовано по второму классу безопасности в соответствии с [2].

Аналогичный подход предполагается использовать и при проведении работ по ВВ базовых аппаратно - программных средств цифровой системы аварийной защиты реактора ВВЭР [3], разрабатываемых в настоящее время в ФГУП «НПП ВНИИЭМ».

Литература

1. Мирошник А.О. Вопросы верификации и валидации программно-технических комплексов в составе систем управления и защиты реакторов ВВЭР / А.О. Мирошник // Труды НПП ВНИИЭМ. – М., 2004. – Т. 101. – С. 109-116.

2. ПНАЭ Г-1-011-97. Общие положения обеспечения безопасности атомных станций (ОПБ-88/97).

3. Протопопов М.В. Базовые аппаратно-программные средства цифровой системы аварийной защиты реактора ВВЭР / М.В. Протопопов, В.Б. Иванчук, М.М. Рахматуллин. – [См. наст. том].

4. Верификация и валидация программных средств управляющих систем, важных для безопасности атомных станций. Общие требования. Руководящий документ. 58413824.23512.001-390.РД-01-2002.М.

5. Атомные станции. Управляющие системы, важные для безопасности. Создание, модернизация и эксплуатация. Общие положения. РД ЭО 0554-2005.

6. ГОСТ Р ИСО МЭК 12207-99**.** Информационные технологии. Процессы жизненного цикла программного обеспечения.

7. IEEE Std 1012. IEEE Standard for Software Verification and Validation Plans.

8. IEEE Std 1059. IEEE Guide for Software Verification and Validation Plans.

9. IEC 60880. Программное обеспечение компьютеров в системах безопасности атомных электростанций.

10. IEC 60880-2. Аспекты защиты программного обеспечения от отказов по общей причине. Использование программных средств и предварительно разработанного программного обеспечения.

11. IEC 61940. Ядерное приборостроение. Анализ применения МЭК 60880.

12. ГОСТ 34.601. Автоматизированные системы стадии создания.

13. ГОСТ 34.201. Виды, комплектность и обозначение документов при создании автоматизированных систем.

14. ГОСТ 19.201. Техническое задание. Требования к содержанию и оформлению.

15. РД 50-34.698. Автоматизированные системы. Требования к содержанию документов.

16. ГОСТ 34.602. Техническое задание на создание автоматизированной системы.

17. IEEE Std 830. IEEE Recommended Practice for Software Requirements Specifications.

18. ANSI/ANS10.4. Руководящие указания по Аттестации и верификации научных и инженерных программ для атомной промышленности.

19. IEEE Std 1028. IEEE Standard for Software Reviews and Audits.

20. IEEE Std 1044. IEEE Standard Classification for Software Anomalies.

21. ГОСТ 19.xxx. Единая система программной документации.

– ГОСТ 19.102. Стадии разработки.
– ГОСТ 19.101. Виды программ и программных документов.
– ГОСТ 19.201. Техническое задание. Требования к содержанию и оформлению.
– ГОСТ 19.202. Спецификация. Требования к содержанию и оформлению.
– ГОСТ 19.401. Текст программы. Требования к содержанию и оформлению.
– ГОСТ 19.402. Описание программы.
– ГОСТ 19.502. Общее описание. Требования к содержанию и оформлению.