УДК 621.039.058

В.В. СКЛЯР[1], М.А. ЯСТРЕБЕНЕЦКИЙ[1], В.С. ХАРЧЕНКО[2]

[1]*Государственный НТЦ по ядерной и радиационной безопасности, Украина*
[2]*Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина*

ОЦЕНКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ И УПРАВЛЯЮЩИХ СИСТЕМ АЭС ПРИ ЭКСПЕРТИЗЕ ЯДЕРНОЙ И РАДИАЦИОННОЙ БЕЗОПАСНОСТИ

Проведен анализ опыта экспертов Государственного научно-технического центра по ядерной и радиационной безопасности (ГНТЦ ЯРБ) в области оценки безопасности программного обеспечения (ПО) информационных и управляющих систем (ИУС) АЭС. Проанализированы требования международных стандартов к ПО ИУС АЭС. Приведены результаты экспертной оценки ПО ИУС АЭС, включая статический анализ пограммного кода.

экспертиза, программное обеспечение, информационные и управляющие системы АЭС

1. Экспертная оценка ПО. Постановка задачи

Экспертиза ядерной и радиационной безопасности (ЯРБ) – это научно-техническая деятельность, целью которой являются исследование, проверка и оценка соответствия объекта экспертизы требованиям ядерной и радиационной безопасности с целью подготовки обоснованного заключения для принятия решений Регулирующим органом [1].

Объектом экспертизы может быть как АЭС в целом, так и различные системы АЭС (например, ИУС), включая их компоненты (например, ПО и технические средства).

Целью экспертизы является оценка полноты и достаточности документов, обосновывающих ЯРБ при осуществлении деятельности с ядерными установками с точки зрения возможности выдачи соответствующего разрешения (лицензии).

Обязательным является независимость экспертной организации от заказчиков экспертизы (участников разработки документации, эксплуатирующей организации и т. п.). Государственную экспертизу ЯРБ в Украине, как правило, проводит ГНТЦ ЯРБ.

В монографии [1] детально рассмотрены регулирующие требования по ЯРБ к ИУС АЭС и их компонентам, а также методы оценки соответствия ИУС АЭС и их компонентов требованиям по ЯРБ. Однако, за последние несколько лет сотрудниками ГНТЦ ЯРБ получены новые результаты [2 - 9] в области оценки безопасности, обусловленные:

– развитием международной и национальной нормативной базы в области ПО ИУС АЭС;

– значительным объемом выполненных экспертиз ЯРБ, предметом которых являлось ПО новых ИУС АЭС;

– применением инструментальных средств статического анализа для оценки ПО.

Целью статьи является анализ опыта украинских экспертов в области оценки безопасности ПО ИУС АЭС.

2. Анализ нормативной базы

Регулирующие требования Украины к ИУС АЭС и их компонентам изложены в нормативном документе НП 306.5.02/3.035-2000 «Требования по ядерной и радиационной безопасности к информационным и управляющим системам, важным для безопасности атомных станций». В указанный нормативный документ включены следующие требования к ПО:

– требования ПО, как к продукту:

– требования к функциям, структуре и элементам ПО;

– требования к диагностированию и самоконтролю;

– требования к обеспечению защиты от отказов, искажений, ошибочных и несанкционированных действий;

– требования к процессам жизненного цикла ПО:

– требования к разработке ПО (включая требования к процессам поддержки ЖЦ);

– требования к верификации ПО.

С момента подготовки первой редакции НП 306.5.02/3.035-2000 произошли существенные изменения в международной нормативной базе, определяющей требования к ПО ИУС АЭС [2].

В 2000 г. Международное агентство по атомной энергии (МАГАТЭ) выпустило стандарт NS – G - 1.1 «Программное обеспечение для компьютерных систем, важных для безопасности АЭС. Руководство по безопасности».

Технический подкомитет 45А «Реакторное приборостроение» Международной электротех-нической комиссии (МЭК) разработал стандарты:

– МЭК 60880:2006 (2-я редакция) «Атомные электростанции – Информационные и управляющие системы важные для безопасности – Программные аспекты компьютерных систем, выполняющих функции категории А»;

– МЭК 62138:2004 «Атомные электростанции – Информационные и управляющие системы важные для безопасности – Программные аспекты компьютерных систем, выполняющих функции категорий В и С».

Проведенный анализ показал, что новые стандарты МАГАТЭ и МЭК содержат группы требований, не в полной мере учтенных в национальном документе НП 306.5.02/3.035-2000 (рис. 1). Указанные требования учитываются при выполнении экспертиз ЯРБ.

3. Результаты экспертной оценки ПО

В последнее десятилетие развитие атомной энергетики в Украине характеризуется интенсивной модернизацией ИУС АЭС. Силами сотрудники ГНТЦ ЯРБ выполнены все экспертизы, относящиеся к ПО новых ИУС АЭС. В ходе таких экспертиз оцениваются документы по верификации ПО (рис. 2).

В настоящее время на АЭС Украины внедрены и успешно эксплуатируются следующие новые программно-технические комплексы (ПТК) ИУС:

– ПТК системы аварийной и предупредительной защиты (ПТК АЗ-ПЗ);

– ПТК системы автоматического регулирования, разгрузки и ограничения мощности реактора и ускоренной предупредительной защиты (ПТК АРМ-РОМ-УПЗ);

– ПТК управляющей системы безопасности (ПТК УСБ);

– ПТК системы группового и индивидуального управления приводами органов регулирования системы управления и защиты реактора (ПТК СГИУ);

– аппаратура контроля нейтронного потока (АКНП);

– ПТК системы внутриреакторного контроля (ПТК СВРК);

– ПТК информационно-вычислительной системы (ПТК ИВС).

ИУС АЭС Украины имеют следующие особенности, которые необходимо учитывать при рассмотрении особенностей ПО [5]:

– разработка и внедрение центральной части ИУС проводилась с помощью ПТК – совокупности технических средств автоматизации (ТСА), поставляемых в комплекте с ПО, необходимым сервисным оборудованием и эксплуатационной документацией, которые интегрируются на площадке АЭС с периферийным оборудованием и/или другими ПТК в составе конкретной ИУС; поэтому, далее при рассмотрении особенностей ПО речь фактически речь идет о ПО ПТК;

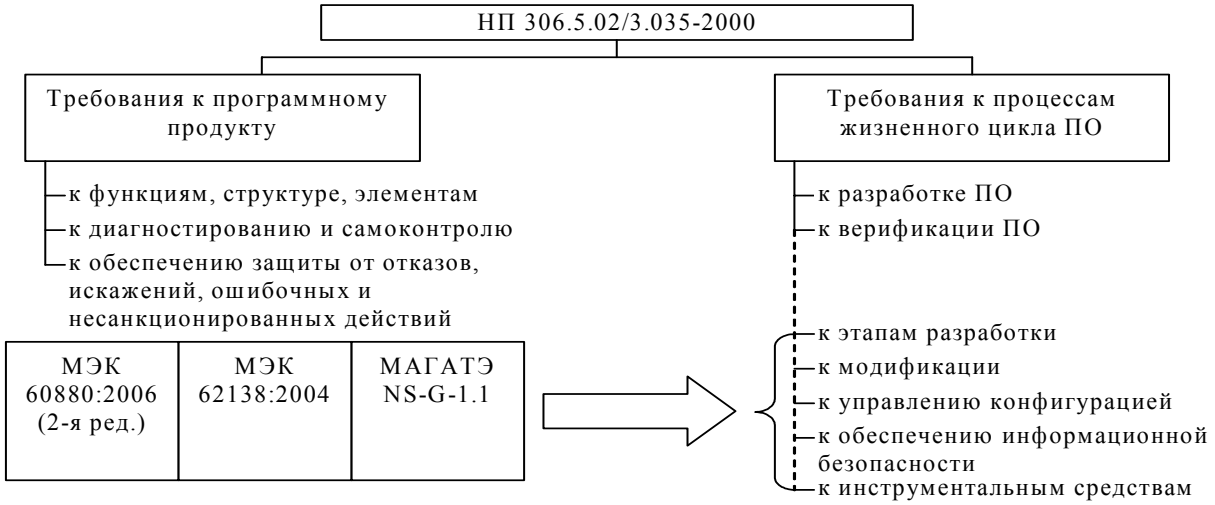

Рис. 1. Структура национальных и международных регулирующих требований к ПО ИУС АЭС

Рис. 2. Обобщенная структура процесса верификации ПО ИУС АЭС

– ИУС, в большинстве своем, разработаны украинскими предприятиями на основе широкой интеграции разработчиков ПТК, ТСА и ПО;

– при разработке ИУС учитывались регулирующие требования украинского нормативного документа НП 306.5.02/3.035-2000, а также требования стандартов МАГАТЭ и МЭК;

– архитектура ПТК и ПО ПТК включает в себя нижний уровень (включая устройства связи с объектом – УСО для сбора данных и центральный программируемый логический контроллер – ПЛК для цифрового управления) и верхний уровень (рабочие станции операторского управления, архивирования, документирования) (рис. 3 и табл. 1); сравнительный анализ ПО ИУС АЭС Украины выполнен в работе [5];

– ПО базируется на апробированных проектных технологических алгоритмах управления;

– для построения ПО широко применяются ранее разработанные компоненты, как собственной разработки производителей ИУС, так и коммерческие (COTS – Commercial Off The Shelf);

– впервые в Украине для систем аварийной защиты реактора применен принцип диверсности (табл. 2);

– НПП «Радий» применяет в качестве программируемых компонентов программируемые логические интегральные схемы (ПЛИС), проекты которых, с одной стороны, могут рассматриваться как разновидность ПО, а с другой, – обладают определенной спецификой, которая накладывает отпечаток на процесс оценки безопасности ИУС АЭС, построенных на базе ПЛИС [6] (табл. 3).

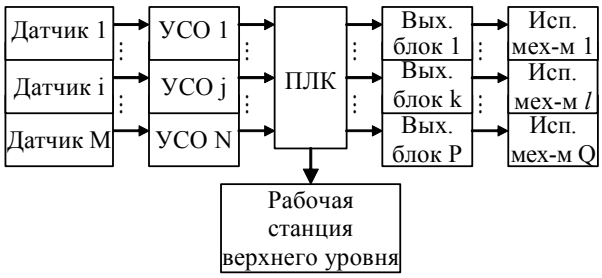

Рис. 3. Типовая структура ИУС АЭС

Таблица 1

Особенности программного обеспечения новых ПТК, внедренных на энергоблоках АЭС Украины

Составляющая ПО	Язык программирования
ПО УСО	Assembler
ПО ПЛК	C\C++, PASCAL, проблемно-ориентированный язык технологических алгоритмов
ПО РС ВУ	C++

Таблица 2

Анализ различий между основным и диверсным комплектами ПТК АЗ-ПЗ

Способ реализации разнообразия	Основной комплект ПТК АЗ-ПЗ	Диверсный комплект ПТК АЗ-ПЗ
Аппаратная диверсность:		
– диверсность программируемых компонентов для реализации алгоритмов защиты реактора	ПЛИС Altera Cyclone	ПЛИС Altera Cyclone II
– диверсность программируемых компонентов для реализации функций ввода\вывода сигналов, диагностики, информационного обмена	Микропроцессоры Texas Instruments	ПЛИС Altera Cyclone в среде которых реализуются эмуляторы процессоров Nios
Программная диверсность:		
– диверсность языков программирования	Assembler	C
– диверсность инструментальных средств	IAR Systems Assembler KickStart	Altera Quartus, Altera SOPC Builder, GNUPro Toolkit
Субъектная диверсность	ПО основного и диверсного комплектов ПТК АЗ-ПЗ разрабатывается различными группами программистов	

Таблица 3

Особенности разработки ИУС на базе ПЛИС

Характеристики ПЛИС	Реализация в ИУС АЭС
Применяемые кристаллы	Altera Cyclone, Altera Cyclone II
Применяемые инструментальные средства	Altera Quartus, Altera SOPC Builder
Этапы разработки	1) разработка исходных схем; 2) разработка проекта ПЛИС; 3) интеграция проекта ПЛИС; 4) имплементация проекта в кристалл
Методы разработки	1) разработка графической схемы; 2) разработка кода на языке описания цифровых устройств (VHDL, AHDL, Verilog и др.); 3) разработка программного кода, реализуемого в среде эмулятора микропроцессора
Методы верификации	Функциональное и временное моделирование в среде САПР
Преимущества по сравнению с ПО	Детерминированные временные характеристики ИУС за счет распараллеливания процессов обработки. Упрощение процесса верификации за счет замены программного кода схемой, сопоставимой с исходными данными для разработки

4. Статический анализ программного кода

Статическим анализом программного кода (САПК) называется процесс рассмотрения программных листингов без непосредственного выполнения программы, в ходе которого опре-деляются различного рода параметры программного кода, позволяющие продемонстрировать со-ответствие кода установленным требованиям либо обнаружить потенциальные проблемы, связанные с проявлением дефектов ПО [3, 4].

Положительные результаты САПК позволяют сделать выводы о соответствии разработанного программного кода проекту ПО и требованиям к ПО, а также о возможности перехода к этапу интеграции программных модулей. Таким образом, САПК является существенной составляющей процесса верификации, что подчеркивается в международных стандартах, в том числе, и в стандартах по атомной энергетике. Методики САПК применяются сотрудниками ГНТЦ ЯРБ при выполнении экспертиз [4] (табл. 4).

Таблица 4

Данные о применении САПК в ходе выполнения экспертиз ядерной и радиационной безопасности

Дата	Наименование ПТК	Наименование модулей ПО, для которых выполнялся САПК	Разработчик ПО	Применяемые методики САПК
2005 г.	ПТК УСБ блока №1 ЮУАЭС	ПО библиотеки нижнего уровня	ЗАО «Радий» (г. Кировоград)	Анализ соответствия правилам кодирования Метрическая оценка сложности Анализ потока данных
2006 г.	ПТК САР-1 РО (СНЭ) блока №1 ХАЭС	Программа «Сервер обмена информацией между верхним и нижним уровнем»	ХГПЗ им. Т.Г. Шевченко (г. Харьков)	Анализ структуры программного кода Анализ соответствия правилам кодирования Метрическая оценка сложности
2006 г.	ПТК верхнего уровня СВРК блока №2 ЮУАЭС	ПО подсистемы общесистемной базы данных реального времени	НПФ «ИНИТ» (г. Киев)	Метрическая оценка сложности
2006 г.	ПТК АРКУЗ исследовательского реактора ВВР-М	ПО блока оптической связи БОС ПО блока выбора блокировок БВБ; ПО библиотеки нижнего уровня; программа «Информационный сервер» из состава ПО верхнего уровня	ЗАО «Радий» (г. Кировоград)	Анализ соответствия правилам кодирования Метрическая оценка сложности
2007 г.	ПТК СГИУ (головной образец)	ПО блока датчика положения БДП; ПО блока размножения сигналов БРС; ПО блока силового управления БСУ; ПО блока выбора блокировок БВБ	ЗАО «Радий» (г. Кировоград)	Анализ соответствия правилам кодирования Метрическая оценка сложности
2007 г.	ПТК АЗ-ПЗ блока №1 ХАЭС	ПО блока ввода аналоговых сигналов БВА; ПО блока ввода дискретных сигналов БВД	ЗАО «Радий» (г. Кировоград)	Анализ соответствия правилам кодирования Метрическая оценка сложности

Параметры, определяемые при выполнении САПК, зависят от набора применяемых методик. Среди наиболее важных параметров следует отметить:

– линейные участки программного кода;

– местоположение в программном коде нелинейных операторов (условных и безусловных переходов, циклов) и вызовов процедур;

– перечень используемых операндов, их типы и ха-

рактеристики использования, связи между различными операндами;

– различные количественные параметры, характеризующие объем и сложность программного кода (количество строк, операторов, операндов, ветвей, процедур, функций, классов и объектов объектно-ориентированного кода, а также дифференциация типов перечисленных характе-ристик);

– конструкции программного кода, запрещенные стандартами программирования;

– время выполнения различных фрагментов программного кода;

– данные об использовании памяти.

Выводы

Основными результатами выполнения экспертиз ЯРБ для ПО ИУС АЭС являются:

– сравнительный анализ регулирующих требований национальных и международных стандартов у ПО ИУС АЭС;

– выполнение экспертной оценки всех новых ИУС АЭС, включая оценку ПО;

– выполнение экспертной оценки ИУС АЭС, соответствующих требованиям к диверсности;

– выполнение экспертной оценки ИУС АЭС, разработанных на базе ПЛИС;

– освоение и применение методик и инструментальных средств статического анализа.

Литература

1. Ястребенецкий М.А., Васильченко В.Н., Виноградская С.В. и др. Безопасность атомных станций: Информационные и управляющие системы.– К.: Техніка, 2004. – 472 с.

2. Скляр В.В., Харченко В.С. Анализ и гармонизация регулирующих требований к программному обеспечению информационных и управляющих систем АЭС с учетом изменений международной нормативной базы // Ядерная и радиационная безопасность. - 2004. – Т. 7. – № 4. – С. 34-47.

3. Скляр В.В. Инструментальные средства для статического анализа программного обеспечения: принципы применения, оценки и выбора // Электронное моделирование. – 2006. – Т. 28. – № 2. – С. 29-41.

4. Скляр В.В. Результаты применения статического анализа для оценки безопасности программного обеспечения информационных и управляющих систем АЭС // Ядерная и радиационная безопасность. – 2007. – Т. 10. – № 2. – С. 36-49.

5. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. – Х.: Нац. аэрокосмический ун-т, 2004. – 159 с.

6. Харченко В.С., Скляр В.В., Гордеев А.А. Верификация программного обеспечения. – Х.: Нац. аэрокосмический ун-т , 2006. – 132 с.

7. Скляр В.В., Харченко В.С., Ястребенецкий М.А. Особенности и оценка безопасности программного обеспечения информационных и управляющих систем АЭС Украины // Ядерные измерительно-информационные технологии. – 2006. – № 1 (17). – С. 3-18.

8. Скляр В.В., Харченко В.С., Ушаков А.А. Анализ безопасности и выбор технологий реализации информационно-управляющих систем АЭС: риск-ориентированный подход // Екологія і ресурси: Зб. наук праць Інституту проблем національної безпеки. – К.: ІПНБ, 2006. – № 13. – С. 39-64.

9. Бахмач Е.С., Сиора А.А., Скляр В.В., Токарев В.И., Харченко В.С. Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС // Радіоелектронні і комп'ютерні системи. – 2007. – № 7 (26). – С. 75-82.

Поступила в редакцию 28.01.2008

Рецензент: д-р техн. наук, проф. Г.Ф. Кривуля, Харьковский национальный университет радиоэлектроники, Харьков.