С Т А Т Ь И

УДК 621.039.538

ЭВОЛЮЦИОННЫЙ ПОДХОД К ПОСТРОЕНИЮ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ВВЭР

Чебышов С.Б. (АО «Атомэнергомаш», г. Москва), Поликанин А.В. (АО «СНИИП», г. Москва), Подшибякин М.А. (АО «ОКБ Гидропресс», г. Подольск, Московская обл.).

Сложность и скорость протекания ядерно-физических и теплогидравлических процессов в реакторной установке, большое число факторов, влияющих на ее безопасность, определяют повышение требований к системам управления и безопасности. В этой связи их совершенствование с учетом новых требований, в том числе и международных определяют актуальность разработки новых решений системной архитектуры, улучшения измерительных и надежностных характеристик аппаратуры. Особенно следует выделить требования международных документов в части безопасной эксплуатации, высокой надежности, оптимальной информатизации контроля и управления документов, формулирующих общие требования к управляющим системам безопасности атомных станций [1—4].

Анализ показал, что одной из ключевых является концепция защиты в глубину на основе принципа разнообразия. Отечественная нормативная база и нормы МАГАТЭ не формулируют в явном виде требования к способу реализации принципа разнообразия для защиты от отказов по общей причине, в том числе связанных с ошибками в программном обеспечении технических средств управляющих систем безопасности (УСБ). Вместе с тем нормы МАГАТЭ [1, 2] и стандарт [3] включают следующие положения:

при построении УСБ на микропроцессорной технике должны быть учтены отказы по общей причине из-за программного обеспечения;

для определения способов защиты от отказов по общей причине следует применять детерминистические, вероятностные анализы или их комбинацию;

при наличии неопределенностей, трудностей в достижении требуемой надежности системы, например, при рассмотрении отказов из-за ошибок в программном обеспечении следует применять консервативный подход. Применительно к УСБ на микропроцессорной технике реализация принципа разнообразия является консервативным решением, компенсирующим трудность демонстрации достижения требуемого уровня надежности системы;

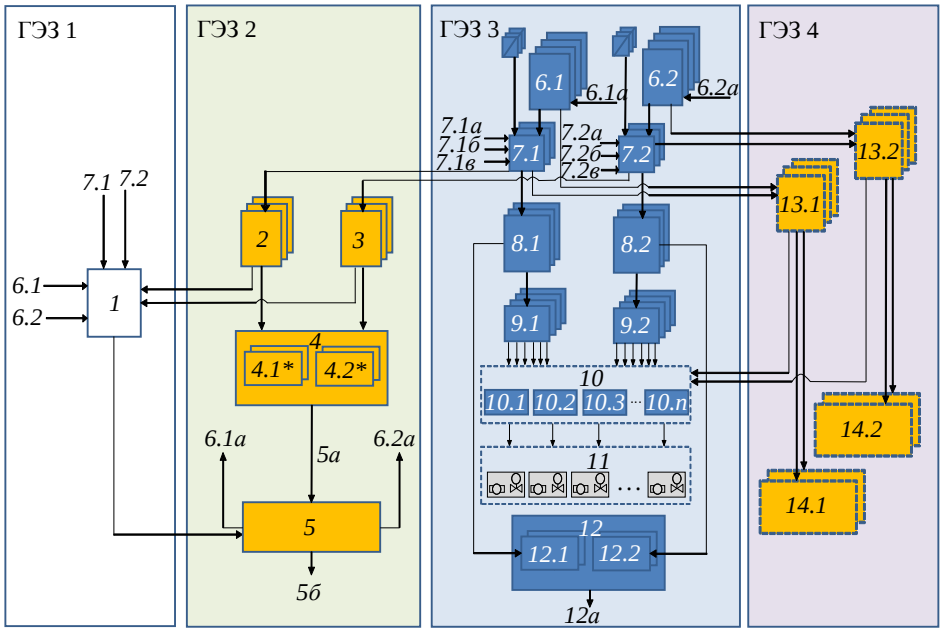
ошибки программного обеспечения являются систематическими, вызванными ошибками при проектировании и, следовательно, не могут быть описаны вероятностными методами, применяемыми в анализе надежности аппаратуры.

Эти положения с учетом неопределенности, связанной с отсутствием общепризнанных методик оценки надежности программного обеспечения, трудностью верификации и валидации, исключающих отказы по общей причине, тестированием всех возможных комбинаций изменений входных параметров свидетельствуют о необходимости применения средств на жесткой логике, исключающих отказы по общей причине. Под жесткой логикой понимаются технические средства, логические состояния которых полностью (на 100%) покрываются испытаниями и проверками для всех комбинаций входных сигналов. Так, число логических состояний программного обеспечения для модуля с одной входной и одной выходной переменной, с пятью ветвлениями и одним циклом составляет 10^{14} [5].

Поскольку микропроцессорная техника имеет существенные преимущества, связанные прежде всего с удобством эксплуатации, а ее применение соответствует современному уровню развития науки и техники, решение о ее полной замене на жесткую логику представляется

далеким от оптимального. В этой связи одним из примеров использования принципа разнообразия и реализации концепции глубокоэшелонированной защиты для исключения отказов управляющей системы безопасности по общей причине являются технические решения, принятые в проектах Нововоронежской АЭС-2 и Ленинградской АЭС-2. В обобщенном виде эти технические решения применительно к проекту Нововоронежской АЭС-2 показаны на рис. 1.

Новым решением в данном случае является дополнительная (диверсная) система защиты, построенная на технических средствах с жесткой логикой. В соответствии с техническим проектом она должна совместно с технологическими системами выполнять основные функции безопасности — управление реактивностью, теплоотвод, удержание радиоактивных продуктов и ограничение аварийных выбросов при проектных исходных событиях и одновременном отказе инициирующей части аварийной защиты и управляющей системы безопасности технологической (ИЧ АЗ-УСБТ), построенной на микропроцессорной технике. При этом в техническом проекте наложение отказа ИЧ АЗ-УСБТ на проектное исходное событие постулируется как запроектная авария, которая должна преодолеваться без тяжелого повреждения активной зоны. Алгоритмы дополнительной системы защиты сформированы на основе анализа безопасности. Общее число условий инициирования функций безопасности по ее сигналам составляет примерно 16 (ИЧ АЗ-УСБТ — около 50). Число шкафов 6 и 42 соответственно.



Р и с. 1. Структурная схема СУЗ реакторной установки В-392М Нововоронежской АЭС-2: ▭, ▭, ▭, ▭ — оборудование, выполненное на платформе *1*, отнесенное к классу безопасности 3, на платформе 2, отнесенное к классу безопасности 3 и 2, на платформе 3, отнесенное к классу безопасности 3 соответственно; *1* — автоматический регулятор мощности; *2*, *3* — 1-й и 2-й комплекты из трех независимых каналов формирования сигналов предупредительной защиты на оборудовании TELEPERM XS; *4* — исполнительная часть предварительной защиты из двух комплектов шкафов аварийных команд; *5* — система группового и индивидуального управления (СГИУ); *5а* — команды УПЗ, ПЗ1, ПЗ2; *5б* — сигналы на приводы органов регулирования (ОР) СУЗ; *6.1*, *6.2* — 1-й и 2-й комплекты из четырех независимых каналов аппаратуры контроля нейтронного потока (АКНП); *6.1а*, *6.2а* — сигналы положения ОР из СГИУ в АКНП; *7.1*, *7.2* — 1-й и 2-й комплекты из трех независимых каналов устройства гальванического разделения и размножения; *7.1а*, *7.2а* — сигналы от автоматизированной системы радиационного контроля; *7.1б*, *7.2б* — сигналы системы индустриальной антисейсмической защиты; *7.1в*, *7.2в* — сигналы от системы внутриреакторного контроля; *8.1*, *8.2* — 1-й и 2-й комплекты из трех независимых каналов аварийной защиты управляющей системы технологической безопасности на оборудовании TELEPERM XS; *9.1*, *9.2* — 1-й и 2-й комплекты из четырех независимых каналов мажоритарной обработки управляющей системы безопасности, инициирующей на оборудовании TELEPERM XS; *10* — модули приоритетного управления; *11* — исполнительные механизмы технологических систем; *12* — исполнительная часть аварийной защиты; *12а* — сигналы на приводы ОР СУЗ; *12.1* —1-й и 2-й шкаф аварийных команд; *12.2* — 3-й и 4-й шкаф аварийных команд; *13.1*, *13.2* — 1-й и 2-й комплекты из трех независимых каналов комплекса средств автоматизации дополнительной системы защиты; *14.1*, *14.2* — шкафы прерывателей питания приводов ОР СУЗ; *4.1**, *4.2** — оборудование для мажоритарной обработки команд ПЗ в шкафах аварийных команд, входящих в исполнительную часть

На рис. 1 показано распределение подсистем, входящих в систему управления и защиты (СУЗ), по уровням глубокоэшелонированной защиты следующим образом: 1-й уровень — режимы нормальной эксплуатации; 2-й уровень — отклонения от нормальной эксплуатации; 3-й уровень — проектные аварии; 4-й уровень — запроектные аварии. Чем выше категория режима, тем ниже частота его возникновения. Таким образом, режимы нормальной эксплуатации должны обеспечиваться за счет работы автоматического регулятора мощности реактора (АРМ), воздействующего на органы регулирования СУЗ, режимы категории 2 должны преодолеваться, как правило, за счет работы предупредительной защиты, проектные аварии — за счет работы управляющих систем безопасности (АЗ-УСБТ). Следует отметить, что инициирующая часть предупредительной защиты реализована в виде двух трехканальных комплектов. Команды поступают в систему управления приводами органов регулирования СУЗ, где в зависимости от вида защиты обеспечивается соответствующий алгоритм. Оборудование для мажоритарной обработки команд предупредительной защиты конструктивно выполнено в шкафах аварийных команд, входящих в исполнительную часть аварийной защиты. Инициирующая часть АЗ-УСБТ реализована также в виде двух трехканальных комплектов. Для контроля нейтронно-физических параметров в составе каждого комплекта аварийной защиты применяется четырехканальная аппаратура контроля нейтронного потока (АКНП). Оборудование дополнительной системы защиты представлено в виде двух комплектов, размещаемых в каналах УСБ. Каждый комплект подсистемы состоит из трех измерительных и логических каналов (три шкафа), осуществляющих сбор и логическую обработку сигналов, формирование команд. Для сброса органов регулирования СУЗ при действии дополнительной системы защиты предусматривается снятие электропитания переменного тока и постоянного тока 110 В дополнительными коммутационными аппаратами.

Приведем классификацию по безопасности и соответствие ее уровням глубокоэшелонированной защиты оборудования СУЗ согласно НП-001—15 на примере Нововоронежской АЭС-2:

	Классификация	Уровень
Инициирующая часть:		
АЗ-УСБТ . . .	2НУ	3
предупредительной защиты . . .	3Н	2
Исполнительная часть:		
аварийной защиты . . .	2НУ	3
предупредительной защиты . . .	3Н	2
Дополнительная система защиты . . .	3У	4
Аппаратура контрольного нейтронного потока . . .	2НУ	1, 2, 3, 4
Автоматический регулятор мощности . . .	3Н	1
Система группового и индивидуального управления органами регулирования СУЗ . . .	3Н	1, 2

В дальнейшем архитектура СУЗ в зависимости от требований конкретного проекта может уточняться и совершенствоваться с учетом достигнутого технического уровня программно-технических средств, построенных на различных платформах, но применение дополнительной системы защиты на жесткой логике в качестве средства для управления запроектными авариями является базовым решением технических проектов реакторной установки АЭС-2006, ВВЭР-ТОИ и новых проектов. Одним из ключевых факторов, обусловливающих актуальность развития систем контроля и управления, является сооружение новых АЭС и модернизация действующих как на территории нашей страны, так и за рубежом. Поэтому представляется целесообразной интеграция оборудования реакторной установки и ее системы контроля и управления. Эволюционный шаг в развитии комплекса систем, обеспечивающих управление и безопасность реакторной установки, видится в создании интегрированного компонента АСУ ТП энергоблока — системы контроля и управления реакторной установкой. Дополнительным фактором в пользу интеграции оборудования являются требования НП-082—07 [6].

Необходимо отметить, что в состав технических проектов ВВЭР входят системы управления и защиты и система контроля управления и диагностики, включая систему внутриреакторного контроля. Все это в совокупности и позволило предложить вариант реализации СУЗ, системы контроля, управления и диагностики (СКУД) и еще несколько систем как интегрированную системную составляющую АСУ ТП с общим названием система контроля и управле-

ния реакторной установкой (СКУ РУ). В составе и совместно с АСУ ТП энергоблока, технологическими системами и оборудованием реакторной установки она обеспечивает:

безопасность, надежность и устойчивость работы в режимах нормальной эксплуатации и с нарушениями нормальной эксплуатации;

контроль, отображение и регистрацию параметров технологического процесса и состояния безопасности реакторной установки, включая контроль необходимых параметров для управления при запроектных авариях;

контроль пределов безопасной эксплуатации реакторной установки во всех ее состояниях;

информационную поддержку персонала;

диагностику состояния технологического оборудования реакторной установки и оборудования СКУ РУ.

При нарушениях нормальной эксплуатации СКУ РУ регистрирует и предоставляет оператору обобщенную информацию о развитии аварийной ситуации на основе симптомно-ориентированного подхода для упрощения принятия им нужных решений при ограниченном времени и максимального снижения последствий аварии.

Функциями СКУ РУ являются:

контроль нейтронно-физических и теплогидравлических характеристик активной зоны реактора и режимов его эксплуатации;

аварийная защита реактора, обеспечивающая его быстрый автоматический останов при возникновении на энергоблоке условий для формирования аварийной защиты;

предупредительная защита реактора до заданного уровня с заданной скоростью при возникновении нарушений нормальных условий эксплуатации;

сигнализация оператору о понижении уровня теплоносителя в реакторе при нарушениях условий нормальной эксплуатации;

диагностирование основного технологического оборудования реакторной установки;

создание архива эксплуатации активной зоны и основного технологического оборудования;

диагностирование собственных технических и программных средств;

информационная поддержка оператора;

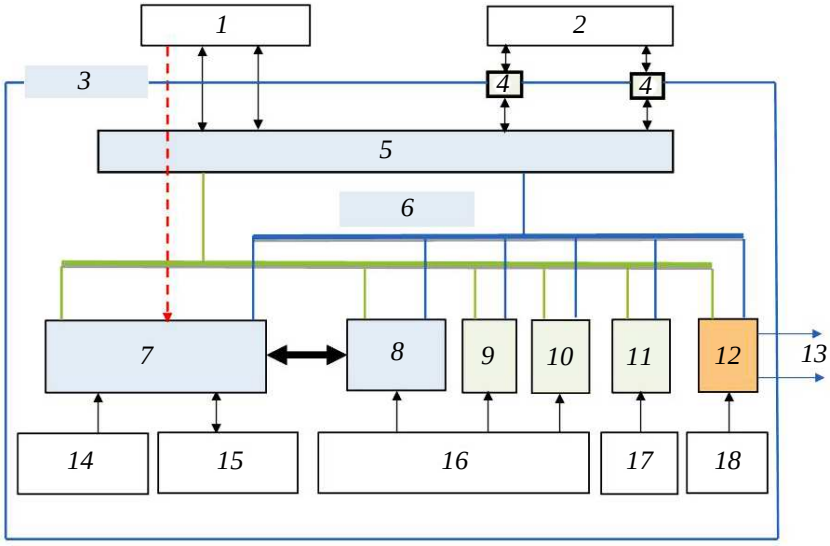
операторское дистанционное управление оборудованием.

Централизованные контроль и управление основными технологическими процессами реакторной установки осуществляются с блочного пульта управления (БПУ) во всех режимах работы и состояниях энергоблока. Информация, необходимая для управления, выводится на средства отображения, размещаемые на панелях и пультах БПУ и резервного пульта управления (РПУ). В случае нарушения работоспособного состояния блочного пульта управления аварийный останов и аварийное расхолаживание реакторной установки осуществляются с резервного пульта управления, расположенного отдельно от него, который не может быть выведен из строя при проектных исходных событиях одновременно с ним.

Параметры, контролируемые на блочном и резервном пультах управления, исполнительные механизмы в части СКУ РУ определены с учетом необходимости снижения нагрузки на оператора за счет повышения автоматизации процессов, оптимизации распределения функций между автоматикой и человеком, информационной поддержки оператора.

Архитектура СКУ РУ разрабатывается на основе концепции глубокоэшелонированной защиты, принципов резервирования (избыточности), независимости и разнообразия, требований со стороны проекта АЭС, НТД по безопасности и киберзащите как распределенная иерархическая, которая базируется на платформе программируемых технических средств на основе решений, апробированных на действующих АЭС. Номенклатура и число технических и программно-технических средств, объединенных в платформу, минимизированы, но вместе с тем достаточны для проектирования систем, выполняющих функции управления и защиты, информационные и диагностические функции.

В базовый состав СКУ РУ, показанной на рис. 2, целесообразно, основываясь на проектных решениях АЭС-2006, включать СУЗ с дополнительной системой защиты, СКУД, включая систему автоматического контроля остаточного ресурса (САКОР), систему контроля уровня теплоносителя в корпусе реактора, аппаратуру контроля гидроамортизаторов. Дополнительно, исходя из границ реакторной установки, в состав СКУ РУ могут быть введены оборудование автоматизированной системы радиацион-



Р и с. 2. Базовая структура СКУ РУ: *1* — блочный и резервный пункты управления; *2* — система верхнего блочного уровня АСУ ТП; *3* — система контроля и управления реакторной установкой; *4* — сетевые шлюзы связи; *5* — система верхнего уровня СКУ РУ; *6* — локальная сеть СКУ РУ; *7* — система управления и защиты; *8* — система контроля, управления и диагностики; *9* — система контроля уровня теплоносителя; *10* — аппаратура контроля гидроамортизаторов; *11* — оборудование радиационного контроля реакторного отделения; *12* — система послеаварийного мониторинга; *13* — защищенный пункт управления противоаварийными действиями; *14, 16* — первичные преобразователи; *15* — исполнительные механизмы; *17* — блоки детектирования ионизирующего излучения реакторного отделения; *18* — датчики физической информации комплекта аварийного КИП; – → — сигналы ручного управления

ного контроля в части контроля радиационных параметров в помещениях реакторного отделения, системы послеаварийного мониторинга.

Помимо уже упомянутых, новым элементом структуры является система верхнего уровня. Ее включение связано со следующими соображениями. В настоящее время информационный обмен между компонентами АСУ ТП АЭС строится, как правило, на основе единой вычислительной сети, причем информационный обмен между системами происходит через систему верхнего блочного уровня (СВБУ). В результате при возникновении пиковых нагрузок, характерных для переходных режимов работы или аварийных ситуаций, объем передаваемой информации резко возрастает. В таких ситуациях вероятность отказа вычислительной техники и/или программного обеспечения межсистемного обмена сети из-за перегрузки пропускной способности резко повышается, что, в свою очередь, может привести к отказу АСУ ТП по общей причине. Решение данной проблемы усложнением программного обеспечения и наращиванием вычислительных мощностей АСУ ТП не даст ощутимых результатов из-за отсутствия детерминированных методов оценки надежности программного обеспечения и инструментария для однозначного подтверждения работоспособности сетевого обмена АСУ ТП. Кроме того, как показывает практика, отказ или сбой в работе сетевого программного обеспечения приводит к потере оперативным персоналом необходимой информации. В этой связи при разработке общей архитектуры СКУ РУ было решено развязать контуры вычислительной сети СКУ РУ и АСУ ТП путем организации системы верхнего уровня СКУ РУ. Такое решение имеет несколько существенных преимуществ:

повышается скорость обмена информацией между системами СКУ РУ, поскольку передача информации происходит без участия СВБУ;

в СВБУ передается только полностью обработанный компактный объем информации, что существенно снижает загрузку сети АСУ ТП;

в случае отказа сети АСУ ТП работа СКУ РУ в объеме, необходимом для выполнения функций защиты реакторной установки, полностью обеспечена;

системы, наиболее важные для безопасности, электрически и информационно развязаны от всего остального оборудования АСУ ТП.

СВУ СКУ РУ включает в себя автоматизированные рабочие места, которые обеспечивают информационную поддержку персонала, а также при необходимости ручное управление оборудованием с блочного и резервного пультов управления при проектных авариях и с защищенного пульта управления противоаварийными действиями при запроектных авариях. Локальная сеть СКУ РУ классифицируется в соответствии с требованиями МАГАТЭ и МЭК.

Исходя из рассмотренного подхода, в состав основных функций системы верхнего уровня СКУ РУ включены:

сбор измеряемых параметров нейтронно-физических, теплогидравлических и технологических процессов от собственных датчиков;

необходимые для контроля состояния активной зоны расчеты;

формирование базы данных по измеренным и рассчитанным параметрам;

создание архива протекания технологических процессов и действий оперативного персонала в ходе эксплуатации энергоблока;

развязка локальных сетей СКУ РУ и СВБУ через шлюз, исключение их взаимного влияния;

представление информации о состоянии реакторной установки на автоматизированных рабочих местах блочного и резервного пультов управления, позволяющих оперативному персоналу поддерживать безопасное управление.

СКУ РУ проектируется из функционально законченных систем, которые разработаны на основе платформ программно-технических средств и комплексов аппаратуры, апробированных в условиях АЭС или других аналогичных объектов, с использованием принципа разнообразия оборудования и программного обеспечения. Использование цифровой программируемой техники в системах безопасности и системах, важных для безопасности, осуществляется в соответствии с требованиями МАГАТЭ и МЭК по процедурам испытаний программно-технических средств, верификации и валидации программного обеспечения, а также на основе принципов глубокоэшелонированной защиты и применения дополнительной системы защиты. В целом сочетание программно-технических средств на базе микропроцессоров с техническими средствами, построенными на жесткой логике, обосновывается с точки зрения как обеспечения необходимого уровня безопасности реакторной установки и энергоблока АЭС, так и эксплуатационных расходов. В СКУ РУ системы и подсистемы разных классов безопасности в такой мере разделены, чтобы нарушение или вывод из работы любого элемента или канала более низкого класса не влияли на способность системы более высокого класса выполнять свои функции. В частности, системы более низкого класса безопасности используют принятые по цифровым каналам показания датчиков систем более высокого класса безопасности при безусловном обеспечении отсутствия влияния системы более низкого класса на функционирование системы более высокого класса.

Как уже отмечалось, оборудование, включенное в СКУ РУ, дифференцировано по классам безопасности и обеспечивает реализацию следующих требований:

независимость подсистем/программно-технических/технических средств различных уровней глубокоэшелонированной защиты и разных классов безопасности, а также резервированных каналов посредством соответствующих технических решений;

принцип единичного отказа — системы должны выполнять заданные функции при любом исходном событии и независимом от исходного события отказе одного любого элемента;

предупреждение или защита от отказов по общей причине с применением принципов независимости, резервирования и разнообразия применительно к системам безопасности и системам, важным для безопасности.

При проектировании СКУ РУ должны быть рассмотрены отказы по общей причине, в том числе из-за ошибок в программном обеспечении. Помимо изложенных требований, СКУ РУ предусматривает возможность непрерывного, периодического контроля исправности программно-технических и технических средств, включая исполнительные механизмы. В СКУ РУ предусмотрены возможности изменения (усовершенствования) программного обеспечения и настройки в процессе пусконаладочных работ, а также инструментальные средства для оперативного редактирования алгоритмов и настройки пороговых величин с соблюдением требований верификации и валидации. По числу входных/выходных сигналов оборудование СКУ РУ должно иметь запас не менее 10% общего числа сигналов для расширения функциональных возможностей.

В соответствии с принятыми подходами СКУ РУ реализует следующие действия команд управления:

инициирование действий систем безопасности;

технологические защиты и блокировки;

дистанционное управление, включая дистанционное управление от оператора исполнительными механизмами по цепям жесткой логики для перевода энергоблока в безопасное со-

стояние при отказе всей микропроцессорной техники, включая систему верхнего уровня СКУ РУ;

автоматическое регулирование.

Приоритет команд при дистанционном управлении с разных постов управления определяется конкретным проектом реакторной установки и АЭС.

В СКУ РУ установлена классификация подсистем по защите от несанкционированного доступа к информации и определены требования по защите информации в соответствии с присвоенным классом.

Рассматривается вариант структуры, при котором в состав СКУ РУ включается оборудование, обеспечивающее сбор, обработку, документирование и хранение информации, достаточной для установления исходных событий возникновения нарушений нормальной эксплуатации и аварий, их развития, установления фактического алгоритма работы систем безопасности и элементов, важных для безопасности, отклонений от штатных алгоритмов, действий персонала.

Разработаны конструкторские решения обеспечения устойчивости оборудования СКУ РУ к внешним воздействиям. Конкретный комплекс мер определяется в зависимости от климатических и сейсмических условий в месте строительства АЭС. В техническом задании на создание СКУ РУ должны быть предусмотрены возможные внешние воздействия с заданием показателей в соответствии с нормативными документами. Технические средства СКУ РУ, размещаемые под защитной оболочкой, должны иметь классификацию не ниже IP55, за пределами защитной оболочки — не ниже IP20 (ГОСТ 15150—69) и обеспечивать электромагнитную совместимость в соответствии с ГОСТом Р 50746—2013. Квалификация и сертификация технических средств должны проводиться с учетом международных нормативных требований и национальных стандартов стран. Размещаемые в зоне ограниченного доступа технические средства и линии связи должны выполнять свои функции и сохранять параметры в пределах, установленных для соответствующих аварийных режимов.

СПИСОК ЛИТЕРАТУРЫ

1. **Лидерство** и менеджмент для обеспечения безопасности. Общие требования безопасности. Серия норм МАГАТЭ по безопасности № GSR. Ч. 2. Вена: МАГАТЭ, 2017.
2. **Безопасность** атомных станций: проектирование. Конкретные требования безопасности. Серия норм по безопасности МАГАТЭ № SSR-2/1. Вена: МАГАТЭ, 2016.
3. **Design** of Instrumentation and Control Systems for Nuclear Power Plants. Specific Safety Guide № SSG-39. IAEA Safety Standards. Vienna: IAEA, 2016.
4. **Nuclear** Power Plants — Instrumentation and Control Important to Safety — General Requirements for Systems. IEC 61513:2011, Ed 2.0.
5. **Майерс Г.** Искусство тестирования программ. Пер. с англ. Под ред. Б.А. Позина. М.: Финансы и статистика, 1982.
6. **Правила** ядерной безопасности реакторных установок атомных станций НП-082—07. — Ядерная и радиационная безопасность, 2008, № 1.

УДК 621.039-78

СОЗДАНИЕ АППАРАТУРЫ КОНТРОЛЯ НЕЙТРОННОГО ПОТОКА ДЛЯ ПЕРСПЕКТИВНЫХ ПРОЕКТОВ ВВЭР

Сергеев И.А., Ермолаев П.А., Стриковский В.И. (ООО «СКУ-Атом», г. Москва), Терехов Д.В. (Нововоронежская АЭС, г. Нововоронеж)

Ключевой задачей при проектировании реакторных установок с точки зрения безопасности является разработка быстродействующих систем управления и защиты. Требования к быстродействию таких систем вытекают из свойств активных зон ВВЭР, относительной инертности контрольно-измерительной аппаратуры, основанной на принципах измерения температуры, давления и других параметров. В связи с этим в состав систем управления и защиты включалось оборудование, контролирующее их мощность и скорость ее увеличения посредст-