Нормы безопасности МАГАТЭ

для защиты людей и охраны окружающей среды

Проектирование систем контроля и управления для атомных электростанций

Специальное руководство по безопасности

№ SSG-39

IAEA

Международное агентство по атомной энергии

НОРМЫ БЕЗОПАСНОСТИ МАГАТЭ И ДРУГИЕ ПУБЛИКАЦИИ ПО ДАННОЙ ТЕМЕ

НОРМЫ БЕЗОПАСНОСТИ МАГАТЭ

В соответствии со статьей III своего Устава МАГАТЭ уполномочено устанавливать или принимать нормы безопасности для защиты здоровья и сведения к минимуму опасностей для жизни и имущества и обеспечивать применение этих норм.

Публикации, посредством которых МАГАТЭ устанавливает нормы, выпускаются в Серии норм безопасности МАГАТЭ. В этой серии охватываются вопросы ядерной безопасности, радиационной безопасности, безопасности перевозки и безопасности отходов. **Категории публикаций в этой серии — это Основы безопасности, Требования безопасности и Руководства по безопасности.**

Информацию о программе по нормам безопасности МАГАТЭ можно получить на сайте МАГАТЭ в Интернете

http://www-ns.iaea.org/standards/

На этом сайте содержатся тексты опубликованных норм безопасности и проектов норм безопасности на английском языке. Тексты норм безопасности выпускаются на арабском, испанском, китайском, русском и французском языках, там также можно найти глоссарий МАГАТЭ по вопросам безопасности и доклад о ходе работы над еще не выпущенными нормами безопасности. Для получения дополнительной информации просьба обращаться в МАГАТЭ по адресу: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

Всем пользователям норм безопасности МАГАТЭ предлагается сообщать МАГАТЭ об опыте их использования (например, в качестве основы для национальных регулирующих положений, для составления обзоров безопасности и учебных курсов) в целях обеспечения того, чтобы они по-прежнему отвечали потребностям пользователей. Эта информация может быть направлена через сайт МАГАТЭ в Интернете или по почте (см. адрес выше), или по электронной почте по адресу Official.Mail@iaea.org.

ПУБЛИКАЦИИ ПО ДАННОЙ ТЕМЕ

МАГАТЭ обеспечивает применение норм и в соответствии со статьями III и VIII.C своего Устава предоставляет сведения и способствует обмену информацией, касающейся мирной деятельности в ядерной области, и служит в этом посредником между своими государствами-членами.

Доклады по вопросам безопасности в ядерной деятельности выпускаются в качестве **докладов по безопасности**, в которых приводятся практические примеры и подробные описания методов, которые могут использоваться в поддержку норм безопасности.

Другие публикации МАГАТЭ по вопросам безопасности выпускаются в качестве публикаций по **аварийной готовности и реагированию, докладов по радиологическим оценкам, докладов ИНСАГ** — Международной группы по ядерной безопасности, **технических докладов и документов серии TECDOC**. МАГАТЭ выпускает также доклады по радиологическим авариям, учебные пособия и практические руководства, а также другие специальные публикации по вопросам безопасности.

Публикации по вопросам физической безопасности выпускаются в **Серии изданий МАГАТЭ по физической ядерной безопасности**.

Серия изданий МАГАТЭ по ядерной энергии состоит из информационных публикаций, предназначенных способствовать и содействовать научно-исследовательской работе в области ядерной энергии, а также развитию ядерной энергии и ее практическому применению в мирных целях. В ней публикуются доклады и руководства о состоянии технологий и успехах в их совершенствовании, об опыте, образцовой практике и практических примерах в области ядерной энергетики, ядерного топливного цикла, обращения с радиоактивными отходами и снятия с эксплуатации.

ПРОЕКТИРОВАНИЕ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДЛЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

Членами Международного агентства по атомной энергии являются следующие государства:

АВСТРАЛИЯ
АВСТРИЯ
АЗЕРБАЙДЖАН
АЛБАНИЯ
АЛЖИР
АНГОЛА
АНТИГУА И БАРБУДА
АРГЕНТИНА
АРМЕНИЯ
АФГАНИСТАН
БАГАМСКИЕ ОСТРОВА
БАНГЛАДЕШ
БАРБАДОС
БАХРЕЙН
БЕЛАРУСЬ
БЕЛИЗ
БЕЛЬГИЯ
БЕНИН
БОЛГАРИЯ
БОЛИВИЯ, МНОГОНАЦИОНАЛЬНОЕ ГОСУДАРСТВО
БОСНИЯ И ГЕРЦЕГОВИНА
БОТСВАНА
БРАЗИЛИЯ
БРУНЕЙ-ДАРУССАЛАМ
БУРКИНА-ФАСО
БУРУНДИ
БЫВШАЯ ЮГОСЛ. РЕСП. МАКЕДОНИЯ
ВАНУАТУ
ВЕНГРИЯ
ВЕНЕСУЭЛА, БОЛИВАРИАНСКАЯ РЕСПУБЛИКА
ВЬЕТНАМ
ГАБОН
ГАИТИ
ГАЙАНА
ГАНА
ГВАТЕМАЛА
ГЕРМАНИЯ
ГОНДУРАС
ГРЕНАДА
ГРЕЦИЯ
ГРУЗИЯ
ДАНИЯ
ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА КОНГО
ДЖИБУТИ
ДОМИНИКА
ДОМИНИКАНСКАЯ РЕСПУБЛИКА
ЕГИПЕТ
ЗАМБИЯ
ЗИМБАБВЕ
ИЗРАИЛЬ
ИНДИЯ
ИНДОНЕЗИЯ
ИОРДАНИЯ
ИРАК
ИРАН, ИСЛАМСКАЯ РЕСПУБЛИКА
ИРЛАНДИЯ
ИСЛАНДИЯ
ИСПАНИЯ
ИТАЛИЯ
ЙЕМЕН
КАЗАХСТАН
КАМБОДЖА
КАМЕРУН
КАНАДА
КАТАР
КЕНИЯ
КИПР
КИТАЙ
КОЛУМБИЯ
КОНГО
КОРЕЯ, РЕСПУБЛИКА
КОСТА-РИКА
КОТ-Д'ИВУАР
КУБА
КУВЕЙТ
КЫРГЫЗСТАН
ЛАТВИЯ
ЛАОССКАЯ НАРОДНО-ДЕМОКРАТИЧЕСКАЯ РЕСПУБЛИКА
ЛЕСОТО
ЛИБЕРИЯ
ЛИВАН
ЛИВИЯ
ЛИТВА
ЛИХТЕНШТЕЙН
ЛЮКСЕМБУРГ
МАВРИКИЙ
МАВРИТАНИЯ
МАДАГАСКАР
МАЛАВИ
МАЛАЙЗИЯ
МАЛИ
МАЛЬТА
МАРОККО
МАРШАЛЛОВЫ ОСТРОВА
МЕКСИКА
МОЗАМБИК
МОНАКО
МОНГОЛИЯ
МЬЯНМА
НАМИБИЯ
НЕПАЛ
НИГЕР
НИГЕРИЯ
НИДЕРЛАНДЫ
НИКАРАГУА
НОВАЯ ЗЕЛАНДИЯ
НОРВЕГИЯ
ОБЪЕДИНЕННАЯ РЕСПУБЛИКА ТАНЗАНИЯ
ОБЪЕДИНЕННЫЕ АРАБСКИЕ ЭМИРАТЫ
ОМАН
ПАКИСТАН
ПАЛАУ
ПАНАМА
ПАРАГВАЙ
ПАПУА-НОВАЯ ГВИНЕЯ
ПЕРУ
ПОЛЬША
ПОРТУГАЛИЯ
РЕСПУБЛИКА МОЛДОВА
РОССИЙСКАЯ ФЕДЕРАЦИЯ
РУАНДА
РУМЫНИЯ
САЛЬВАДОР
САН-МАРИНО
САУДОВСКАЯ АРАВИЯ
СВЯТОЙ ПРЕСТОЛ
СЕЙШЕЛЬСКИЕ ОСТРОВА
СЕНЕГАЛ
СЕНТ-ВИНСЕНТ И ГРЕНАДИНЫ
СЕРБИЯ
СИНГАПУР
СИРИЙСКАЯ АРАБСКАЯ РЕСПУБЛИКА
СЛОВАКИЯ
СЛОВЕНИЯ
СОЕДИНЕННОЕ КОРОЛЕВСТВО ВЕЛИКОБРИТАНИИ И СЕВЕРНОЙ ИРЛАНДИИ
СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ
СУДАН
СЬЕРРА-ЛЕОНЕ
ТАДЖИКИСТАН
ТАИЛАНД
ТОГО
ТРИНИДАД И ТОБАГО
ТУНИС
ТУРКМЕНИСТАН
ТУРЦИЯ
УГАНДА
УЗБЕКИСТАН
УКРАИНА
УРУГВАЙ
ФИДЖИ
ФИЛИППИНЫ
ФИНЛЯНДИЯ
ФРАНЦИЯ
ХОРВАТИЯ
ЦЕНТРАЛЬНОАФРИКАНСКАЯ РЕСПУБЛИКА
ЧАД
ЧЕРНОГОРИЯ
ЧЕШСКАЯ РЕСПУБЛИКА
ЧИЛИ
ШВЕЙЦАРИЯ
ШВЕЦИЯ
ШРИ-ЛАНКА
ЭКВАДОР
ЭРИТРЕЯ
ЭСВАТИНИ
ЭСТОНИЯ
ЭФИОПИЯ
ЮЖНАЯ АФРИКА
ЯМАЙКА
ЯПОНИЯ

Устав Агентства был утвержден 23 октября 1956 года на Конференции по выработке Устава МАГАТЭ, которая состоялась в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке. Устав вступил в силу 29 июля 1957 года. Центральные учреждения Агентства находятся в Вене. Главной целью Агентства является достижение «более скорого и широкого использования атомной энергии для поддержания мира, здоровья и благосостояния во всем мире».

СЕРИЯ НОРМ МАГАТЭ ПО БЕЗОПАСНОСТИ, № SSG-39

ПРОЕКТИРОВАНИЕ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ ДЛЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ

СПЕЦИАЛЬНОЕ РУКОВОДСТВО ПО БЕЗОПАСНОСТИ

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА, 2018

УВЕДОМЛЕНИЕ ОБ АВТОРСКОМ ПРАВЕ

Группа сбыта и маркетинга
Издательская секция
Международное агентство по атомной энергии
Vienna International Centre
PO Box 100
1400 Vienna, Austria
факс: +43 1 26007 22529
тел.: +43 1 2600 22417
эл. почта: sales.publications@iaea.org
веб-сайт: www.iaea.org/books

Отпечатано МАГАТЭ в Австрии
Сентябрь 2018 года
STI/PUB/1694

ПРОЕКТИРОВАНИЕ СИСТЕМ
КОНТРОЛЯ И УПРАВЛЕНИЯ
ДЛЯ АТОМНЫХ ЭЛЕКТРОСТАНЦИЙ
МАГАТЭ, ВЕНА, 2018 ГОД
STI/PUB/1694
ISBN 978–92–0–406118–5
ISSN 1020–5845

ПРЕДИСЛОВИЕ

Юкия Амано
Генеральный директор

Устав МАГАТЭ уполномочивает Агентство «устанавливать или применять … нормы безопасности для охраны здоровья и сведения к минимуму опасности для жизни и имущества» — нормы, которые МАГАТЭ должно использовать в своей собственной работе и которые государства могут применять посредством их включения в свои регулирующие положения в области ядерной и радиационной безопасности. МАГАТЭ осуществляет это в консультации с компетентными органами Организации Объединенных Наций и с заинтересованными специализированными учреждениями. Всеобъемлющий свод высококачественных и регулярно пересматриваемых норм безопасности наряду с помощью МАГАТЭ в их применении является ключевым элементом стабильного и устойчивого глобального режима безопасности.

МАГАТЭ начало осуществлять свою программу по нормам безопасности в 1958 году. Значение, уделяемое качеству, соответствию поставленной цели и постоянному совершенствованию, лежит в основе широкого применения норм МАГАТЭ во всем мире. Серия норм безопасности теперь включает единообразные Основополагающие принципы безопасности, которые выработаны на основе международного консенсуса в отношении того, что должно пониматься под высоким уровнем защиты и безопасности. При твердой поддержке со стороны Комиссии по нормам безопасности МАГАТЭ проводит работу с целью содействия глобальному признанию и использованию своих норм.

Однако нормы эффективны лишь тогда, когда они надлежащим образом применяются на практике. Услуги МАГАТЭ в области безопасности охватывают вопросы проектирования, выбора площадки и инженерно-технической безопасности, эксплуатационной безопасности, радиационной безопасности, безопасной перевозки радиоактивных материалов и безопасного обращения с радиоактивными отходами, а также вопросы государственной основы, регулирования и культуры безопасности в организациях. Эти услуги в области безопасности содействуют государствам-членам в применении норм и позволяют обмениваться ценным опытом и данными.

Ответственность за деятельность по регулированию безопасности возлагается на страны, и многие государства принимают решения применять нормы МАГАТЭ по безопасности в своих национальных регулирующих положениях. Для сторон различных международных

конвенций по безопасности нормы МАГАТЭ являются согласованным и надежным средством обеспечения эффективного выполнения обязательств, вытекающих из этих конвенций. Эти нормы применяются также регулирующими органами и операторами во всем мире в целях повышения безопасности при производстве ядерной энергии и применении ядерных методов в медицине, промышленности, сельском хозяйстве и научных исследованиях.

Безопасность — это не самоцель, а необходимое условие защиты людей во всех государствах и охраны окружающей среды в настоящее время и в будущем. Риски, связанные с ионизирующими излучениями, должны оцениваться и контролироваться без неоправданного ограничения вклада ядерной энергии в справедливое и устойчивое развитие. Правительства, регулирующие органы и операторы во всем мире должны обеспечивать, чтобы ядерный материал и источники излучения использовались для всеобщего блага, в условиях безопасности и с учетом мнения общественности. Для содействия этому предназначены нормы МАГАТЭ по безопасности, которые я призываю применять все государства-члены.

НОРМЫ БЕЗОПАСНОСТИ МАГАТЭ

ОБЩИЕ СВЕДЕНИЯ

Радиоактивность — это естественное явление, и в окружающей среде присутствуют природные (естественные) источники излучения. Ионизирующие излучения и радиоактивные вещества с пользой применяются во многих сферах — от производства энергии до использования в медицине, промышленности и сельском хозяйстве. Радиационные риски, которым в результате этих применений могут подвергаться работники, население и окружающая среда, подлежат оценке и должны в случае необходимости контролироваться.

Поэтому такая деятельность, как медицинское использование радиации, эксплуатация ядерных установок, производство, перевозка и использование радиоактивных материалов и обращение с радиоактивными отходами, должна осуществляться в соответствии с нормами безопасности.

Регулированием вопросов безопасности занимаются государства. Однако радиационные риски могут выходить за пределы национальных границ, и в рамках международного сотрудничества принимаются меры по обеспечению и укреплению безопасности в глобальном масштабе посредством обмена опытом и расширения возможностей для контроля опасностей, предотвращения аварий, реагирования в случае аварийных ситуаций и смягчения любых вредных последствий.

Государства обязаны проявлять должную осмотрительность и соответствующую осторожность, и предполагается, что они будут выполнять свои национальные и международные обязательства.

Международные нормы безопасности содействуют выполнению государствами своих обязательств согласно общим принципам международного права, например, касающимся охраны окружающей среды. Кроме того, международные нормы безопасности укрепляют и обеспечивают уверенность в безопасности и способствуют международной торговле.

Глобальный режим ядерной безопасности постоянно совершенствуется. Нормы безопасности МАГАТЭ, которые поддерживают осуществление имеющих обязательную силу международных договорно-правовых документов и функционирование национальных инфраструктур безопасности, являются краеугольным камнем этого глобального режима. Нормы безопасности МАГАТЭ — это полезный инструмент, с помощью которого договаривающиеся стороны оценивают свою деятельность по выполнению этих конвенций.

НОРМЫ БЕЗОПАСНОСТИ МАГАТЭ

Статус норм безопасности МАГАТЭ вытекает из Устава МАГАТЭ, которым Агентство уполномочивается устанавливать и применять, в консультации и, в надлежащих случаях, в сотрудничестве с компетентными органами Организации Объединенных Наций и с заинтересованными специализированными учреждениями, нормы безопасности для охраны здоровья и сведения к минимуму опасности для жизни и имущества и обеспечивать применение этих норм.

В целях обеспечения защиты людей и охраны окружающей среды от вредного воздействия ионизирующего излучения нормы безопасности МАГАТЭ устанавливают основополагающие принципы безопасности, требования и меры для обеспечения контроля за радиационным облучением людей и выбросом радиоактивного материала в окружающую среду, ограничения вероятности событий, которые могут привести к утрате контроля за активной зоной ядерного реактора, ядерной цепной реакцией, радиоактивным источником или любым другим источником излучения, и смягчения последствий таких событий в случае, если они будут иметь место. Нормы касаются установок и деятельности, связанных с радиационными рисками, включая ядерные установки, использование радиационных и радиоактивных источников, перевозку радиоактивных материалов и обращение с радиоактивными отходами.

Меры по обеспечению безопасности и физической безопасности[1] преследуют общую цель защиты жизни и здоровья людей и охраны окружающей среды. Меры по обеспечению безопасности и физической безопасности должны разрабатываться и осуществляться комплексно, таким образом, чтобы меры по обеспечению физической безопасности не осуществлялись в ущерб безопасности, и наоборот, чтобы меры по обеспечению безопасности не осуществлялись в ущерб физической безопасности.

Нормы безопасности МАГАТЭ отражают международный консенсус в отношении того, что является основой высокого уровня безопасности для защиты людей и охраны окружающей среды от вредного воздействия ионизирующего излучения. Они выпускаются в Серии норм безопасности МАГАТЭ, которая состоит из документов трех категорий (см. рис. 1).

---

[1] См. также публикации в Серии изданий МАГАТЭ по физической ядерной безопасности.

РИС. 1. Долгосрочная структура Серии норм безопасности МАГАТЭ.

Основы безопасности

Основы безопасности содержат основополагающие цели и принципы защиты и безопасности и служат основой для требований безопасности.

Требования безопасности

Комплексный и согласованный набор требований безопасности устанавливает требования, которые должны выполняться с целью обеспечения защиты людей и охраны окружающей среды в настоящее время и в будущем. Требования регулируются целями и принципами основ безопасности. Если требования не выполняются, то должны приниматься меры для достижения или восстановления требуемого уровня безопасности. Формат и стиль требований облегчают их гармоничное использование для создания национальной основы регулирования. Требования, включая пронумерованные всеобъемлющие требования, выражаются формулировками «должен, должна, должно, должны». Многие требования конкретной стороне не адресуются, а это означает, что за их выполнение отвечают соответствующие стороны.

Руководства по безопасности

В руководствах по безопасности содержатся рекомендации и руководящие материалы, касающиеся выполнения требований безопасности, и в них выражается международный консенсус в отношении необходимости принятия рекомендуемых мер (или эквивалентных альтернативных мер). В руководствах по безопасности сообщается о международной положительной практике, и они во все большей степени отражают образцовую практику с целью помочь пользователям достичь высокого уровня безопасности. Рекомендации, содержащиеся в руководствах по безопасности, формулируются с применением глагола «следует».

ПРИМЕНЕНИЕ НОРМ БЕЗОПАСНОСТИ МАГАТЭ

Основные пользователи норм безопасности в государствах — членах МАГАТЭ — это регулирующие и другие соответствующие государственные органы. Кроме того, нормы безопасности МАГАТЭ используются другими организациями-спонсорами и многочисленными организациями, которые занимаются проектированием, сооружением и эксплуатацией ядерных установок, а также организациями, участвующими в использовании радиационных и радиоактивных источников.

Нормы безопасности МАГАТЭ применяются в соответствующих случаях на протяжении всего жизненного цикла всех имеющихся и новых установок, используемых в мирных целях, и на протяжении всей нынешней и новой деятельности в мирных целях, а также в отношении защитных мер для уменьшения существующих радиационных рисков. Они могут использоваться государствами в качестве базы для их национальных регулирующих положений в отношении установок и деятельности.

Согласно Уставу МАГАТЭ нормы безопасности являются обязательными для МАГАТЭ применительно к его собственной работе, а также для государств применительно к работе, выполняемой с помощью МАГАТЭ.

Кроме того, нормы безопасности МАГАТЭ закладывают основу для услуг МАГАТЭ по рассмотрению безопасности, и они используются МАГАТЭ в содействии повышению компетентности, в том числе, для разработки учебных планов и организации учебных курсов.

Международные конвенции содержат требования, аналогичные требованиям, которые изложены в нормах безопасности МАГАТЭ, и делают их обязательными для договаривающихся сторон. Нормы безопасности МАГАТЭ, подкрепляемые международными конвенциями,

отраслевыми стандартами и подробными национальными требованиями, создают прочную основу для защиты людей и охраны окружающей среды. Существуют также некоторые особые вопросы безопасности, требующие оценки на национальном уровне. Например, многие нормы безопасности МАГАТЭ, особенно те из них, которые посвящены вопросам планирования или разработки мер по обеспечению безопасности, предназначаются, прежде всего, для применения к новым установкам и видам деятельности. На некоторых существующих установках, сооруженных в соответствии с нормами, принятыми ранее, требования, установленные в нормах безопасности МАГАТЭ, в полном объеме соблюдаться не могут. Вопрос о том, как нормы безопасности МАГАТЭ должны применяться на таких установках, решают сами государства.

Научные соображения, лежащие в основе норм безопасности МАГАТЭ, обеспечивают объективную основу для принятия решений по вопросам безопасности; однако лица, отвечающие за принятие решений, должны также выносить обоснованные суждения и должны определять, как лучше всего сбалансировать выгоды принимаемых мер или осуществляемой деятельности с учетом соответствующих радиационных рисков и любых иных вредных последствий этих мер или деятельности.

ПРОЦЕСС РАЗРАБОТКИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ

Подготовкой и рассмотрением норм безопасности занимаются Секретариат МАГАТЭ и пять комитетов по нормам безопасности, охватывающих аварийную готовность и реагирование (ЭПРеСК) (с 2016 года), ядерную безопасность (НУССК), радиационную безопасность (РАССК), безопасность радиоактивных отходов (ВАССК) и безопасную перевозку радиоактивных материалов (ТРАНССК), а также Комиссия по нормам безопасности (КНБ), которая осуществляет надзор за программой по нормам безопасности МАГАТЭ (см. рис. 2).

Все государства — члены МАГАТЭ могут назначать экспертов в комитеты по нормам безопасности и представлять замечания по проектам норм. Члены Комиссии по нормам безопасности назначаются Генеральным директором, и в ее состав входят старшие правительственные должностные лица, несущие ответственность за установление национальных норм.

Для осуществления процессов планирования, разработки, рассмотрения, пересмотра и установления норм безопасности МАГАТЭ создана система управления. Особое место в ней занимают мандат МАГАТЭ, видение будущего применения норм, политики и стратегий безопасности и соответствующие функции и обязанности.

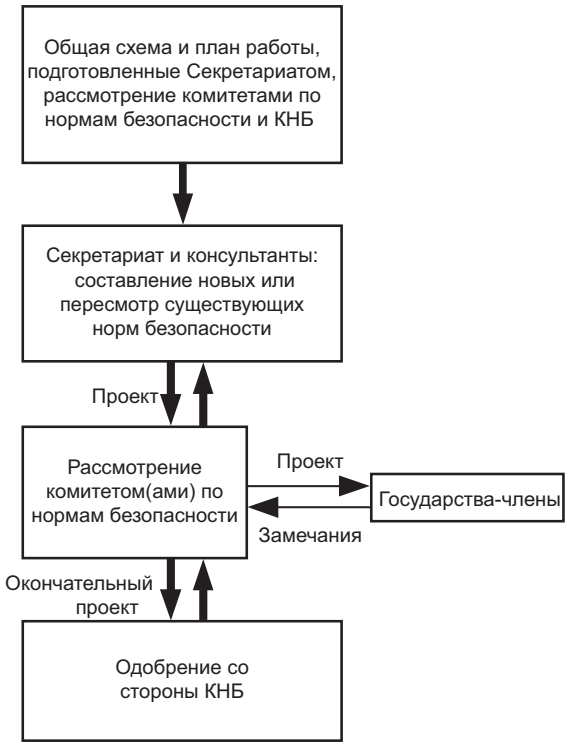

РИС. 2. Процесс разработки новых норм безопасности или пересмотр существующих норм.

ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ МЕЖДУНАРОДНЫМИ ОРГАНИЗАЦИЯМИ

При разработке норм безопасности МАГАТЭ принимаются во внимание выводы Научного комитета ООН по действию атомной радиации (НКДАР ООН) и рекомендации международных экспертных органов, в частности, Международной комиссии по радиологической защите (МКРЗ). Некоторые нормы безопасности разрабатываются в сотрудничестве с другими органами системы Организации Объединенных Наций или другими специализированными учреждениями, включая Продовольственную и сельскохозяйственную организацию Объединенных Наций, Программу Организации Объединенных Наций по окружающей среде, Международную организацию труда, Агентство по ядерной энергии ОЭСР, Панамериканскую организацию здравоохранения и Всемирную организацию здравоохранения.

ТОЛКОВАНИЕ ТЕКСТА

Относящиеся к безопасности термины должны толковаться в соответствии с определениями, данными в Глоссарии МАГАТЭ по вопросам безопасности (см. http://www-ns.iaea.org/standards/safety-glossary.htm). Для руководств по безопасности аутентичным текстом является английский вариант.

Общие сведения и соответствующий контекст норм в Серии норм безопасности МАГАТЭ, а также их цель, сфера применения и структура приводятся в разделе 1 «Введение» каждой публикации.

Материал, который нецелесообразно включать в основной текст (например, материал, который является вспомогательным или отдельным от основного текста, дополняет формулировки основного текста или описывает методы расчетов, процедуры или пределы и условия), может быть представлен в дополнениях или приложениях.

Дополнение, если оно включено, рассматривается в качестве неотъемлемой части норм безопасности. Материал в дополнении имеет тот же статус, что и основной текст, и МАГАТЭ берет на себя авторство в отношении такого материала. Приложения и сноски к основному тексту, если они включены, используются для предоставления практических примеров или дополнительной информации или пояснений. Приложения и сноски неотъемлемой частью основного текста не являются. Материал в приложениях, опубликованный МАГАТЭ, не обязательно выпускается в качестве его авторского материала; в приложениях к нормам безопасности может быть представлен материал, имеющий другое авторство. Содержащийся в приложениях посторонний материал, с тем чтобы в целом быть полезным, по мере необходимости публикуется в виде выдержек и адаптируется.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

ОБЩИЕ СВЕДЕНИЯ

1.1. Настоящее Руководство по безопасности содержит рекомендации по проектированию систем контроля и управления (СКУ), предназначенные для обеспечения соответствия требованиям, установленным в публикации Серии норм безопасности МАГАТЭ, № SSR-2/1 (Rev.1), «Безопасность атомных электростанций: проектирование» [1].

1.2. Настоящая публикация представляет собой пересмотр и объединение двух Руководств по безопасности: публикаций в Серии норм безопасности МАГАТЭ, № NS-G-1.1[1] и № NS-G-1.3[2], которые она заменяет. При пересмотре во внимание было принято развитие СКУ со времени выпуска этих более ранних Руководств по безопасности в 2000 и 2002 годах соответственно. Основные изменения обусловлены непрерывным развитием компьютерных приложений, а также эволюцией методов, необходимых для обеспечения их безопасности, физической безопасности (защищенности) и практического применения. Кроме того, были учтены достижения в учете человеческого фактора и необходимость обеспечения компьютерной безопасности. В настоящем Руководстве по безопасности также даются соответствующие ссылки и учитываются другие документы Серии норм безопасности МАГАТЭ и Серии изданий МАГАТЭ по физической ядерной безопасности, в которых представлены рекомендации по проектированию СКУ. Среди них особо следует отметить публикации Серии норм безопасности МАГАТЭ, № GS-R-3, «Система управления для установок и деятельности» [2]; № GS-G-3.1, «Применение системы управления для установок и деятельности» [3]; GS-G-3.5, «Система управления для ядерных установок» [4]; GSR Part 4 (Rev. 1), «Оценка безопасности установок и деятельности» [5].

---

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna (2000) (МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Программное обеспечение для компьютерных систем, важных для безопасности атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.1).

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Системы контрольно-измерительных приборов и управления, важные для безопасности атомных электростанций, Серии норм безопасности МАГАТЭ, № NS-G-1.3, МАГАТЭ, Вена (2008).

1.3. Ниже указаны основные темы, по которым в настоящем Руководстве по безопасности даны новые или актуализированные рекомендации:

— специфические для СКУ соображения в отношении обеспечения соблюдения требований, установленных в публикации GS-R-3 [2];
— исходные проектные данные, подлежащие рассмотрению при разработке проектной основы СКУ;
— взаимозависимый характер жизненных циклов проектирования и реализации СКУ, и, в частности, жизненного цикла всей структуры СКУ в рамках установки в целом, отдельных СКУ и программного обеспечения, а также необходимость интеграции входных данных учета человеческого фактора и входных данных по компьютерной безопасности в эти жизненные циклы;
— применение компьютерной техники, устройств, запрограммированных с помощью языков описания аппаратных средств, и промышленных устройств ограниченной функциональности, а также средств, обеспечивающих их корректное функционирование;
— общая архитектура СКУ, поддерживающая концепцию глубокоэшелонированной защиты, применяемой при проектировании систем станции и для формирования глубокоэшелонированной защиты для самой СКУ в качестве защиты от отказов по общей причине;
— передача данных между системами, важными для безопасности, с уделением особого внимания случаям, когда система, принимающая данные, имеет более высокий класс безопасности, чем система, отправляющая данные;
— средства обеспечения физической безопасности (защищенности) цифровых систем безопасности;
— деятельность, связанная с разработкой компьютерных программных средств, включая их проектирование, верификацию и валидацию, обусловленная принципами, приведенными в настоящем Руководстве по безопасности, либо вытекающими из предшествующего Руководства по безопасности, № NS-G-1.1[3].

1.4. В настоящем Руководстве по безопасности под термином «система контроля и управления» (СКУ) понимается любая СКУ (система контрольно-измерительных приборов и *система управления и защиты)*, важная для безопасности, в соответствии ее определением в Глоссарии МАГАТЭ по безопасности [6]. Термин-прилагательное «важный для безопасности» в дальнейшем использоваться не будет, за исключением его употребления

[3] См. сноску 1.

в целях акцентирования внимания. Когда рекомендации или пояснения применяются как в отношении СКУ, важных для безопасности, так и СКУ, не являющихся важными для безопасности, об этом прямо указывается в тексте настоящей публикации.

1.5. Настоящее Руководство по безопасности тесно коррелирует с публикацией Серии норм безопасности МАГАТЭ, № SSG-34, «Design of Electrical Power Systems for Nuclear Power Plants» («Проектирование систем электроснабжения атомных электростанций») [7], которая содержит рекомендации по системам электроснабжения, кабельным системам, защите от электромагнитных помех, заземлению корпуса оборудования и цепей передачи полезных сигналов, а также по другим темам, важным для удовлетворительного функционирования СКУ.

1.6. Дополнительные руководящие материалы по проектированию и разработке СКУ, оборудования и программного обеспечения издаются государствами и другими организациями, занимающимися разработкой стандартов. Такие публикации содержат значительно больший объем деталей по сравнению с нормами безопасности МАГАТЭ. Предполагается, что настоящее Руководство по безопасности будет применяться вместе с детализированными промышленными стандартами.

ЦЕЛЬ

1.7. Целью настоящего Руководства по безопасности является предоставление рекомендаций по архитектуре СКУ в целом, а также СКУ, важных для безопасности, на атомной электростанции, которые предназначены для достижения целей безопасности на станции.

1.8. В настоящем Руководстве по безопасности указана исходная информация, необходимая проектировщикам СКУ для определения проектной основы СКУ, исходя из механической, электротехнической, ядерной и строительной частей проекта станции, процесса компоновки станции, а также анализа безопасности. В проектную основу СКУ, например, включаются функциональные требования, которым должна соответствовать СКУ, предельные температуры окружающей среды, в интервале которых должно работать оборудования, внешние события, к которым оборудование СКУ должно быть устойчиво, а также условия, при которых будет требоваться автоматический останов.

СФЕРА ПРИМЕНЕНИЯ

1.9. Настоящее Руководство по безопасности содержит рекомендации по проектированию, реализации, квалификации и документированию СКУ, важных для безопасности, предусмотренных на АЭС, которые применяются в интересах обеспечения соответствия требованиям, изложенным в публикации SSR-2/1 (Rev. 1) [1]. Настоящее Руководство по безопасности также охватывает некоторые конкретные аспекты СКУ, касающиеся применения рекомендаций, содержащихся в некоторых других руководствах по безопасности, например в руководствах по вопросам системы менеджмента, ввода в эксплуатацию, установки, эксплуатации, а также эксплуатационных пределов и условий. В таких случаях в настоящем Руководстве по безопасности даются ссылки на соответствующие разделы этих других руководств по безопасности.

1.10. Настоящее руководство применяется к любому виду оборудования СКУ — от датчиков до исполнительных устройств и устройств управления механическим оборудованием. Оно охватывает, например:

— датчики;
— средства управления исполнительными устройствами;
— оборудование для автоматического и ручного управления оборудованием станции;
— операторский интерфейс.

1.11. Настоящее Руководство по безопасности также применяется к средствам реализации функций оборудования СКУ, таким как:

— компьютерные системы и связанные с ними системы коммуникации;
— программное обеспечение;
— устройства, запрограммированные с помощью языков описания аппаратных средств (например, программируемые пользователем вентильные матрицы);
— промышленные цифровые устройства ограниченной функциональности;

1.12. Настоящее Руководство по безопасности не содержит рекомендаций в отношении средств поддержки СКУ, таких как системы охлаждения, смазки и энергоснабжения. Рекомендации по системе электроснабжения представлены в публикации SSG-34 [7] [4].

1.13. Настоящее Руководство по безопасности охватывает некоторые аспекты учета человеческого фактора и компьютерной безопасности применительно к СКУ, однако оно не содержит всеобъемлющих рекомендаций по этим вопросам. Задача настоящего Руководства по безопасности сводится к определению основных взаимосвязей с человеческим фактором или мерами по обеспечению компьютерной безопасности и предоставлению рекомендаций по проектным решениям СКУ, которые могут оказывать влияние на эти аспекты. К вопросам, касающимся человеческого фактора или компьютерной безопасности, которые не охватываются настоящим Руководством, относятся компьютеризированные процедуры эксплуатации и безопасность информационных технологий. Более подробная информация по компьютерной безопасности приводится в публикации [8].

1.14. Настоящее Руководство применяется при проектировании СКУ для новых станций, при усовершенствовании уже имеющихся станций, а также при модернизации СКУ существующих станций. Вопросам модификации станции посвящена публикация Серии норм безопасности МАГАТЭ, № NS-G-2.3, «Модификации на атомных станциях» [9], и дублирование в настоящем Руководстве по безопасности материала публикации NS-G-2.3 [9] было сведено к минимуму.

1.15. В Глоссарии МАГАТЭ по вопросам безопасности [6] СКУ, важные для безопасности, определяются как СКУ, которые являются частью некоторой группы безопасности, а также как СКУ, неисправности или отказ которых могут привести к радиационному облучению персонала станции или лиц из населения. В разделе 5 настоящего Руководства по безопасности также используется термин-прилагательное «важный для безопасности» и другие термины применительно к классификации безопасности. Примеры СКУ, к которым может применяться настоящее Руководство по безопасности, включают:

— системы защиты реактора;

---

[4] Проект Руководства по безопасности по вспомогательным системам, в котором будут представлены рекомендации по другим средствам поддержки, находится в стадии разработки.

— системы контроля реактора и системы управления реактивностью и системы их мониторинга;
— системы мониторинга и контроля нормального охлаждения реактора;
— системы мониторинга и контроля аварийного энергоснабжения;
— системы мониторинга и контроля изоляции защитной оболочки;
— контрольно-измерительные приборы для мониторинга в ходе аварии;
— системы мониторинга сбросов;
— СКУ для обращения с топливом.

1.16. Настоящее Руководство по безопасности содержит рекомендации по разработке компьютерного программного обеспечения для использования в СКУ, важных для безопасности, а также для передачи цифровых данных. Настоящее Руководство по безопасности также указывает меры, осуществление которых необходимо для реализации функций СКУ, запрограммированных в интегральных схемах с использованием языка описания аппаратных средств.

1.17. В публикациях [10, 11] представлен обзор концепций, лежащих в основе настоящего Руководства по безопасности, и приводятся примеры рассматриваемых систем. Эти публикации могут служить полезным справочным материалом для некоторых пользователей, однако они не относятся к руководящим материалам МАГАТЭ.

СТРУКТУРА

1.18. Раздел 2 содержит руководящий материал по применению требований, изложенных в публикации GS-R-3 [2], и рекомендаций, изложенных в публикациях GS-G-3.1 [3] и GS-G-3.5 [4], поскольку они имеют конкретное отношение к разработке СКУ. Этот раздел также охватывает вопросы применения моделей жизненного цикла для описания процессов системы менеджмента применительно к разработке СКУ, и в нем приводятся рекомендации по общим процессам проектирования СКУ и изложен руководящий материал по осуществлению конкретных видов деятельности по разработке СКУ.

1.19. Раздел 3 посвящен исходным данным, необходимым для проектирования, и в нем предоставлены рекомендации по проектной основе СКУ.

1.20. Раздел 4 содержит рекомендации, касающиеся архитектуры СКУ в целом.

1.21. В разделе 5 описывается схема классификации безопасности, используемая для ранжирования применения рекомендаций, приведенных в настоящем Руководстве по безопасности, в соответствии с важностью для безопасности тех аспектов, к которым эти рекомендации применяются.

1.22. Раздел 6 содержит общие рекомендации, которые могут применяться к любым СКУ, важным для безопасности.

1.23. В разделе 7 приводятся рекомендации, предназначенные конкретно для некоторых систем, таких как система защиты реактора, для некоторых видов оборудования, например, датчиков, а также для некоторых технологий, например, цифровых систем и интегральных схем, конфигурированных с применением языков описания аппаратных средств. Рекомендации, изложенные в разделах 2–6 и разделах 8 и 9, применяются также и к конкретным системам, которым посвящен раздел 7.

1.24. Раздел 8 содержит рекомендации по человеко-машинному интерфейсу. Сюда включен руководящий материал по применению принципов человеческого фактора к СКУ, а также в нем приводятся характеристики, которым человеко-машинный интерфейс должен соответствовать.

1.25. В разделе 9 приводятся рекомендации по разработке программного обеспечения для компьютеризированных СКУ, важных для безопасности.

1.26. Настоящее Руководство по безопасности следует применять в целом, а не выборочно по отдельным разделам. Так, руководящий материал для программного обеспечения, представленный в разделе 9, следует применять вместе с рекомендациями по системе менеджмента и жизненным циклам, изложенным в разделе 2.

1.27. В качестве приложений включены: перечень промышленных стандартов, в которых приводятся более детальные рекомендации по основным разделам настоящего Руководства по безопасности; информация, отражающая корреляцию настоящего Руководства по безопасности с двумя Руководствами по безопасности (NS-G-1.1[5] и NS-G-1.3[6]), которые

---

[5] См. сноску 1.

[6] См. сноску 2.

оно заменяет; краткий перечень областей, в которых практика государств различается. Также прилагается список определений, конкретизированных для настоящего Руководства по безопасности.

2. СИСТЕМА МЕНЕДЖМЕНТА ДЛЯ ПРОЕКТИРОВАНИЯ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

ОБЩИЕ ПОЛОЖЕНИЯ

2.1. В требовании 6 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Проектирование АЭС должно обеспечивать, чтобы станция и узлы, важные для безопасности, обладали соответствующими характеристиками, обеспечивающими возможность выполнения функций безопасности с необходимой надежностью, возможность безопасной эксплуатации станции в рамках эксплуатационных пределов и условий в течение всего проектного срока службы станции и возможность безопасного снятия с эксплуатации, а также для сведения к минимуму воздействия на окружающую среду.»

2.2. В требовании 2 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Проектная организация должна создать и внедрить систему менеджмента для обеспечения того, чтобы все требования безопасности, установленные в отношении проекта станции, учитывались и осуществлялись на всех стадиях процесса проектирования, и чтобы окончательный проект отвечал этим требованиям».

2.3. В публикации GS-R-3 [2] устанавливаются требования, предъявляемые к системе менеджмента для установок и деятельности.

2.4. Пункт 2.1 публикации GS-R-3 [2] гласит:

> «Предусматривается создать систему управления (менеджмента), которая используется, оценивается и постоянно совершенствуется. Она приводится в соответствие с задачами организации и способствует их достижению. Основная цель системы управления состоит в достижении и повышении безопасности с помощью:
>
> — последовательного сведения воедино всех требований к управлению организацией;
> — описания планируемых и систематически осуществляемых действий, необходимых для обеспечения достаточной уверенности в том, что все эти требования выполняются;
> — обеспечения требований, связанных с вопросами здравоохранения, окружающей среды, физической безопасности, качества и экономики, без отрыва от требований безопасности, с тем чтобы исключить возможность их отрицательного воздействия на безопасность».

В пункте 4.2 публикации GS-R-3 [2] далее указано: «Информация и знания, имеющиеся у организации, управляются как один из видов ресурсов».

2.5. В интересах обеспечения безопасности в отношении документации по проектной основе, а также сопутствующей информации или записей, относящихся к СКУ, важным для безопасности, следует применять контроль, осуществляемый соответствующими методами, с целью обеспечения их полноты, ясности, лаконичности, точности и последовательности на протяжении всего жизненного цикла СКУ. Следует предусматривать систему менеджмента, обеспечивающую достаточность и адекватность документации по проектной основе и связанных с ней или вытекающих из нее данных или учетных записей, а также их ведение и сохранение на протяжении определенного периода времени с целью учета проектных изменений либо изменений условий эксплуатации станции. Сюда входят документы и информация, которые могут быть получены из документации по проектной основе и которые могут оказывать влияние на безопасность, такие как процедуры или инструкции по эксплуатации, обслуживанию или модификации таких систем.

2.6. Система менеджмента включает организационный план, организационную культуру, политику и процессы, в том числе те их них, которые применяются для определения и распределения ресурсов (например, кадров, оборудования, инфраструктуры и рабочей среды) в целях разработки СКУ, соответствующих требованиям безопасности.

2.7. Следует обеспечить, чтобы каждая организация, участвующая в деятельности по разработке СКУ, имела систему менеджмента, отвечающую ожидаемым результатам применения системы менеджмента эксплуатирующей организации.

2.8. Публикации GS-G-3.1 [3] и GS-G-3.5 [4] содержат руководящие материалы по применению требований, установленных в публикации GS-R-3 [2] для установок и деятельности, а также для ядерных установок.

2.9. Следует обеспечить, чтобы система менеджмента, применяемая для разработки СКУ, отвечала требованиям публикации GS-R-3 [2] и соответствовала рекомендациям, изложенными в публикациях GS-G-3.1 [3] и GS-G-3.5 [4], которые широко применяются при разработке конструкций, систем и элементов атомных электростанций. Настоящее Руководство по безопасности, касающееся конкретных процессов разработки СКУ, следует применять совместно с этими публикациями.

Применительно к процессу разработки СКУ особый интерес представляют следующие вопросы, нашедшие отражение в публикации GS-R-3 [2]:

— система менеджмента (управления);
— культура безопасности;
— приверженность руководства;
— соответствие законодательным и регулирующим требованиям;
— организационная политика;
— планирование;
— ответственность и полномочия;
— обеспечение ресурсами;
— людские ресурсы;
— разработка процессов системы менеджмента;
— менеджмент процессов;
— контроль документов, продукции (включая инструментальные средства) и учетных записей;
— закупки;
— коммуникация;

— менеджмент организационных изменений;
— мониторинг и измерения;
— самооценка;
— независимая оценка;
— несоответствия и корректирующие и профилактические меры;
— усовершенствования.

ПРИМЕНЕНИЕ МОДЕЛЕЙ ЖИЗНЕННОГО ЦИКЛА

2.10. Пункт 5.1 публикации GS-R-3 [2] гласит:

> «Определяются процессы системы управления (менеджмента), необходимые для осуществления задач, предоставления средств для соблюдения всех требований и выпуска продукции организации, а также планируется, осуществляется, оценивается и постоянно совершенствуется разработка этих процессов».

2.11. Современные СКУ атомных электростанций представляют собой сложную структуру элементов, к проектированию и квалификации которых необходимо применять различные подходы помимо тех, которые обычно применялись к старым системам. Часто функциональные и эксплуатационные показатели предыдущих поколений СКУ характеризовались моделями, основанными на законах физики и испытаниях, которые использовались для валидации этих моделей.

2.12. Современные СКУ, в частности цифровые системы, функциональность которых зависит от программного обеспечения и языка описания аппаратных средств, в корне отличаются от старых систем в том, что их поведение определяется логикой и не предопределяется внешними физическими законами. Вследствие этого незначительные ошибки в проектировании и реализации могут привести к неожиданному поведению цифровых систем.

2.13. В цифровых СКУ соответствие конечного продукта его целевому назначению главным образом, но не исключительно, обусловлено применением высококачественных процессов разработки, предусматривающих строгое регламентирование и применение проектных требований. Верификация и валидация необходимы для проверки пригодности конечного продукта к использованию. Однако вывод в отношении правильности функционирования цифровых СКУ в полном

диапазоне условий не может быть сделан на основе комбинации тестов и физических моделей так, как это может быть сделано в случае систем, функционирование которых зависит только от аппаратных (технических) средств. Поэтому уверенность в правильном функционировании современных систем в большей степени достигается за счет строгого осуществления процесса разработки в отличие от систем, построенных только с применением аппаратных средств.

2.14. В вязи с этим в атомной энергетике, а также в других областях с особыми требованиями к обеспечению безопасности, таких как аэрокосмическая промышленность, применяются процессы разработки, как правило, представляемые в виде моделей жизненного цикла, описывающих процессы разработки электронных систем и взаимосвязь между этими процессами. Эта общепринятая практика отражена в стандартах для атомной отрасли, содержащих подробные рекомендации по процессам разработки СКУ. Как правило, процессы, имеющие отношение к определенному этапу разработки, объединяются в группу одной стадии жизненного цикла.

2.15. Тщательно задокументированный процесс разработки также позволяет получить доказательства, на основании которых независимые эксперты и регулирующий орган могут удостовериться в пригодности конечного продукта к использованию по назначению.

2.16. Представленные в данном разделе рекомендации по процессам жизненного цикла также применимы к осуществляемым в течение жизненного цикла операциям, описанным в разделе 9. Рекомендации по процессам жизненного цикла, представленные в данном разделе, дополняют требования, изложенные в публикации GS-R-3 [2], и рекомендации, приведенные в публикациях GS-G-3.1 [3] и GS-G-3.5 [4], в той мере, в какой они применимы к процессу разработки СКУ.

2.17. Для описания разработки СКУ необходимо применять три базовых уровня жизненных циклов:

a) жизненный цикл общей архитектуры СКУ;
b) жизненные циклы одной или нескольких отдельных СКУ;
c) жизненные циклы одного или нескольких отдельных компонентов СКУ: управление жизненными циклами компонентов, как правило, осуществляется в рамках процесса разработки платформы, и эти циклы не зависят от уровня общей архитектуры, а также от жизненных

циклов на уровне отдельных систем. Жизненные циклы компонентов цифровых систем обычно подразделяются на отдельные жизненные циклы разработки программных и аппаратных (технических) средств.

2.18. Другие виды деятельности, выходящие за рамки разработки СКУ, будут в значительной мере влиять на требования к разработке СКУ, а также на сам процесс разработки СКУ. Учет человеческого фактора и обеспечение компьютерной безопасности являются примерами такой деятельности. Эти виды деятельности имеют более широкую цель, чем поддержка проектирования СКУ, но в будущем они будут оказывать значительное

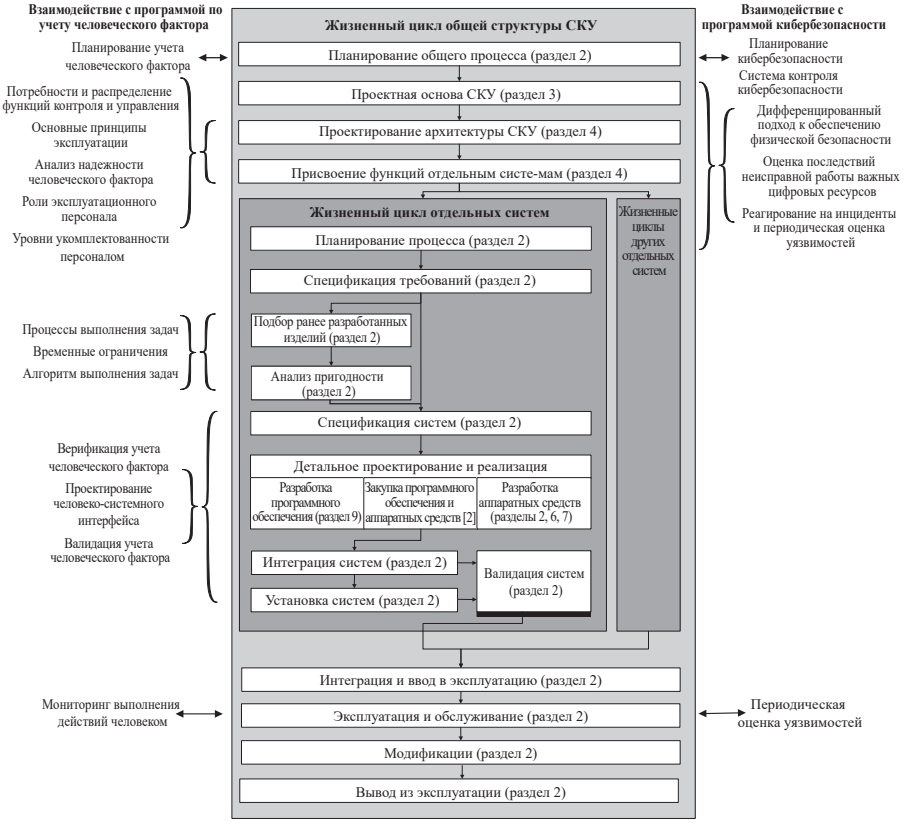

РИС 1. Типичные процессы, осуществляемые в течение жизненного цикла разработки СКУ, и взаимосвязь с программами учета человеческого фактора и обеспечения компьютерной безопасности.

влияние на разработку СКУ. Кроме того, проще и экономически выгоднее начинать работу по учету человеческого фактора и предусматривать средства обеспечения физической безопасности (защищенности) еще на стадии проектирования. По завершении стадии проектирования введение изменений может быть крайне сложным или даже невозможным.

2.19. На рис. 1 представлен пример жизненного цикла разработки СКУ и основные результаты, получаемые благодаря осуществлению программ учета человеческого фактора и обеспечения компьютерной безопасности.

2.20. V-образная модель, показанная на рис. 2, дает альтернативное представление о примере жизненного цикла разработки. Эта модель иллюстрирует взаимосвязь между спецификацией требований, проектированием, процессами интеграции и валидации системы, а также показывает, как работы по верификации и валидации связаны с

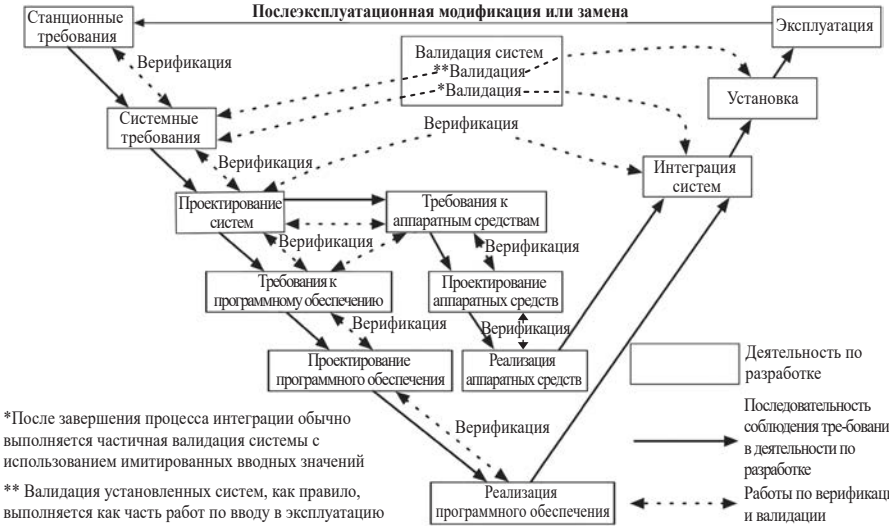

РИС 2. Типичные взаимосвязи между процессами жизненного цикла разработки СКУ и мерами по верификации и валидации.

деятельностью по разработке. Рис. 2 применим как для цифровых, так и для аналоговых систем. Разумеется, если программное обеспечение не применяется, его разработка не требуется.

2.21. В любой момент жизненного цикла в силу приобретенного опыта может возникнуть необходимость в пересмотре работы, проделанной на предыдущих стадиях. Такие изменения носят сквозной характер и могут влиять на работу, выполненную на промежуточных стадиях. В целях упрощения иллюстрации на рис. 1 и 2 такие итерационные пути не отображаются.

2.22. Все виды деятельности, связанные с разработкой, реализацией и эксплуатацией общей архитектуры СКУ, отдельных СКУ и элементов СКУ[7], следует осуществлять в рамках подтвержденного документацией жизненного цикла разработки.

2.23. Следует обеспечить, чтобы жизненный цикл каждой СКУ и каждого ее компонента охватывал период, который начинается с определения требований к ним и заканчивается, когда СКУ или ее компонент перестает быть необходимым для обеспечения безопасности станции.

Планирование процессов

2.24. Перед началом любой технической деятельности следует подготовить и утвердить, в соответствии с требованиями для системы менеджмента, план, определяющий необходимые исходные данные, продукты и процессы такой деятельности, а также взаимосвязи этой деятельности с другими видами деятельности.

2.25. Планы разработки СКУ включают вопросы, касающиеся конкретно СКУ, а также вопросы, в рамках которых может требоваться особый подход к разработке СКУ. Обычно в планы непосредственной разработки СКУ входят следующие вопросы:

— модели жизненного цикла;
— конфигурационное управление;
— идентификация, контроль и устранение несоответствий;
— анализ опасностей;
— верификация и валидация;
— использование результатов вероятностной оценки безопасности;
— анализ безопасности, предназначенный исключительно для СКУ;

---

[7] Элементы СКУ включают такие виды аппаратных средств и программного обеспечения, как, например, прикладное программное обеспечение и аппаратно-программное обеспечение (firmware), а также язык описания аппаратных средств.

— разработка технических требований;
— разработка архитектуры;
— подбор и приемка ранее разработанных изделий;
— проектирование;
— реализация (например, производство аппаратных средств и кодирование программного обеспечения или кодирование и синтез с использованием языка описания аппаратных средств);
— интеграция;
— валидация систем;
— установка (монтаж);
— ввод в эксплуатацию;
— квалификация оборудования;
— квалификация и использование инструментальных средств;
— ремонтопригодность;
— меры по смягчению последствий устаревания;
— эксплуатация;
— подготовка кадров;
— обслуживание программного обеспечения.

2.26. Планы по некоторым из этих отдельных пунктов могут быть объединены в один общий план.

2.27. Разработка СКУ также зависит от плана осуществления видов деятельности, не характерных для разработки СКУ, таких как:

— обеспечение качества;
— классификация узлов, важных для безопасности;
— закупки;
— изготовление;
— разработка и ведение документации.

2.28. Все виды деятельности по разработке СКУ следует осуществлять в соответствии с применимыми утвержденными планами.

Координация с деятельностью по проектированию с учетом человеческого фактора и деятельностью по обеспечению компьютерной безопасности

2.29. Модели жизненного цикла, связанные с учетом человеческого фактора при проектировании и обеспечением компьютерной безопасности, не входят в число тем настоящего Руководства по безопасности, однако

такие процессы позволяют получить информацию, требующуюся для разработки СКУ. На рис. 1 представлены взаимосвязи и интерфейсы между этими процессами. К ним относятся: разработка конкретных требований в отношении учета человеческого фактора; результаты верификации и валидации в связи с учетом человеческого фактора; технические меры по обеспечению физической безопасности; спецификация требований к компьютерной безопасности.

2.30. Разработку СКУ следует координировать с деятельностью по учету человеческого фактора и деятельностью по обеспечению компьютерной безопасности.

2.31. При разработке СКУ следует учитывать требования, определенные в результате осуществления программы по учету человеческого фактора, включая:

— описание функций и обязанностей эксплуатационного персонала и другие требования, касающиеся персонала;
— классификацию безопасности для конструкций, систем и элементов человеко-машинного интерфейса;
— спецификацию информационных потребностей, в том числе критерии определения набора элементов индикации и управления, требуемых для реагирования на аварийные условия и послеаварийные условия;
— спецификацию потребностей в управлении, функциональности автоматического и ручного управления, а также размещение средств контроля и управления в соответствующих местах;
— требования, касающиеся процессов выполнения задач, временных ограничений, также перемещения эксплуатационного персонала и потоков информации, полученной в результате проведения анализа (например, анализа задач; см. пункт 8.78);
— стратегии контекстно-ориентированное оповещения; контекстно-ориентированное оповещение исключает «избыточное» поступление сообщений, например, в процессе запуска и во время переходных процессов;
— требования к предоставлению информации о дефектах в СКУ;
— меры по обеспечению ремонтопригодности СКУ;
— сведения, полученные в результате учета потенциальных ошибок, обусловленных человеческим фактором, при анализе безопасности (т.е. анализа надежности человеческого фактора).

2.32. Следует обеспечить, чтобы меры по верификации и валидации, связанные с учетом человеческого фактора, позволили:

— проверить выполнение рекомендаций, касающихся учета человеческого фактора, и устранить недостатки, выявленные при проведении анализа проекта человеко-машинного интерфейса;
— удостовериться, что СКУ соответствуют применимым руководящим принципам проектирования с учетом человеческого фактора;
— удостовериться, что при проектировании были предусмотрены СКУ, другое оборудование и средства поддержки операторов, которые являются достаточными для оказания поддержки эксплуатационному персоналу в выполнения стоящих перед ним задач;
— удостовериться, что проектирование с учетом человеческого фактора способствует надлежащему реагированию операторов на сигналы оповещения, включая предоставление достаточного времени для выполнения оператором соответствующих действий;
— валидировать с использованием результатов, измеренных на основе показателей эффективности, способность эксплуатационного персонала осуществлять свои функции, применяя СКУ во всех условиях, в которых системы, как ожидается, будут функционировать, включая ситуации, когда некоторые элементы СКУ на основании санкционированного отключения будут находиться в нерабочем состоянии, например, для целей проведения обслуживания или тестирования.

2.33. Разработка требований к учету человеческого фактора и верификации и валидации учета человеческого фактора, как правило, осуществляется в рамках программы учета человеческого фактора. Настоящее Руководство по безопасности не содержит дополнительной информации о программе учета человеческого фактора, за исключением данных о взаимосвязях процессов жизненного цикла СКУ.

2.34. Следует обеспечить, чтобы общая структура СКУ станции обеспечивала реализацию мер безопасности, которые закреплены за ней в соответствии с планом обеспечения компьютерной безопасности.

2.35. Следует обеспечить, чтобы план по обеспечению компьютерной безопасности по мере необходимости обновлялся с учетом общей архитектуры СКУ, а также отдельных СКУ.

2.36. Разработку СКУ следует осуществлять посредством поддержания диалога между персоналом, ответственным за обеспечение безопасности, и персоналом, ответственным за обеспечение физической ядерной безопасностью, либо силами смешанной группы, состоящей из специалистов по безопасности и физической ядерной безопасности в обстановке, отвечающей техническим, процедурным и административным требованиям плана по обеспечению компьютерной безопасности.

2.37. Дополнительная информация по обеспечению компьютерной безопасности на ядерных установках приводится в публикации [8].

ДЕЯТЕЛЬНОСТЬ, СВОЙСТВЕННАЯ ВСЕМ СТАДИЯМ ЖИЗНЕННОГО ЦИКЛА

Конфигурационное управление

2.38. В пунктах 5.12, 5.13, 5.18 и 5.19 публикации GS-R-3 [2] указано:

> «5.12. Обеспечивается контроль документов.... Обеспечивается осведомленность всех пользователей документов о наличии надлежащих и правильных документов и использование ими таких документов.
>
> 5.13. Вносимые в документы изменения рассматриваются и регистрируются и подлежат утверждению на том же уровне, что и сами документы».
>
> …….
>
> «5.18. Устанавливается контроль, исключающий возможность непрохождения продукцией требуемой проверки.
>
> 5.19. Продукция идентифицируется в целях обеспечения ее надлежащего применения. В случае, когда возможность установить производителя (прослеживаемость) является обязательным условием, организация контролирует и регистрирует уникальную маркировку продукции».

2.39. В публикации GS-R-3 [2] эти темы освещены в пунктах с заголовками: контроль документов, контроль продукции, контроль учетных записей. Применительно к инженерно-техническим работам контроль документов и продуктов входят в общую рубрику, именуемую конфигурационным управлением. Требования публикации GS-R-3 [2] по контролю учетных записей также распространяются на документы, в отношении которых применяется конфигурационное управление, однако некоторые учетные записи могут контролироваться отдельно от систем конфигурационного управления (например, отдельной системой управления учетными записями). Публикации GS-G-3.1 [3] и GS-G-3.5 [4] содержат дополнительные рекомендации по четырем темам пункта 2.38.

2.40. Цели конфигурационного управления применительно к СКУ в течение их жизненного цикла включают:

— идентификацию всех единиц, в отношении которых применяется конфигурационное управление, а именно: документации, продуктов в составе СКУ и соответствующих учетных записей;
— обеспечение безопасного хранения и выборки конфигурационных единиц;
— определение зависимостей и связей между единицами, в отношении которых применяется конфигурационное управление;
— идентификацию всех изменений в единицах, в отношении которых применяется конфигурационное управление;
— предотвращение непреднамеренного и несанкционированного изменения единиц, в отношении которых применяется конфигурационное управление;
— обеспечение постоянного соответствия проектной основе;
— спецификацию базовых конфигурационных данных, т.е. по конфигурации взаимосовместимых и согласующихся компонентов для единицы каждого иерархического уровня конфигурации в рамках конфигурационного управления[8];
— обеспечение соответствия между физическим состоянием станции и технической документацией;

[8] Единицы, для которых устанавливается конфигурационный базис, могут включать отдельные элементы, системы или общую структуру СКУ. Базовые характеристики любой единицы охватывает все системы и элементы, входящие в данную единицу.

— спецификацию текущего состояния единиц, в отношении которых применяется конфигурационное управление (например, их рассмотрение или утверждение, или результаты валидации).

2.41. Следует обеспечить, чтобы в конфигурационное управление были включены методы и процедуры анализа последствий изменений, утверждения изменений, обеспечения корректного объединения версий, выпуска проектной документации и выдачи разрешения на использование программного обеспечения, а также составления и ведения записей в хронологическом порядке (например, отражающие, какие версии инструментальных средств должны применяться на определенном этапе проектирования).

2.42. Следует обеспечить, чтобы все единицы СКУ и связанная с ними документация имели соответствующие обозначения, были снабжены уникальным идентификатором и охвачены конфигурационным управлением.

2.43. В число единиц СКУ входят: поставленная СКУ, любые отдельно установленные единицы, предназначенные для поддержки системы или необходимые для функционирования системы, как это было предусмотрено, документация и файлы, характеризующие эти единицы, программные инструменты, влияющие на их качество.

2.44. Как правило, к единицам СКУ относятся, например:

— закупаемые единицы, повторно используемые единицы и вновь разработанные единицы;
— компоненты программного обеспечения, такие как исходный код и исполняемый код, язык описания аппаратных (технических) средств, конфигурационные данные программируемых пользователем вентильных матриц (также известные как битовые потоки) и программное обеспечение, установленное на оборудовании станции, включая прикладные программные средства, операционные системы и вспомогательные программные средства;
— компоненты аппаратного обеспечения и заменяемые элементы таких компонентов;
— аппаратно-программное обеспечение (firmware);

— разработанные документы, такие как спецификации, проектная документация, рабочие чертежи и инструкции, установочные чертежи и инструкции, язык описания программного обеспечения и аппаратных средств;
— конфигурационные данные оборудования и конфигурационные файлы (например, пределы безопасной эксплуатации, пределы срабатывания аварийного сигнала или сигнала предупреждения, заданные уставки и калибровочные параметры);
— физические инструментальные средства и программные инструменты, используемые для производства, контроля, конфигурирования, верификации или валидации компонентов СКУ, включая значения параметров, использовавшиеся при применении таких инструментальных средств.

2.45. Данные по конфигурационному управлению следует использовать для верификации того, что единицы СКУ правильно собраны и фактическое и топологическое место их установки выбрано правильно, и что надлежащая версия программного обеспечения установлена корректно.

2.46. Пункт 5.21 публикации GS-R-3 [2] гласит: «Учетные записи указываются в связанной с процессом документации и подлежат контролю. Все учетные записи должны быть читаемыми, полными, распознаваемыми и легко поддаваться поиску».

2.47. В отношении учетных записей в процессе жизненного цикла следует применять конфигурационное управления.

2.48. Программа конфигурационного управления в отношении учетных записей в течение жизненного цикла может отличаться от аналогичной программы, которая применяется в случае продуктов в составе СКУ.

2.49. Учетные записи в процессе жизненного цикла, в отношении которых применяется конфигурационный контроль, включают любую информацию, от которой зависит анализ безопасности системы или которая может повлиять на безопасность во время эксплуатации или осуществления мероприятий по техническому обслуживанию, например:

— планы и регламент процессов жизненного цикла;
— план подтверждения надлежащего обеспечения безопасности;
— документация по проведению анализа;

— результаты (артефакты) или записи, используемые для документирования демонстрации безопасности и используемых для ее подтверждения данных, например, артефакты или записи, свидетельствующие о достоверности, результаты верификации (включая анализ и тестирование), валидации (включая валидацию требований), оценки и аудита процессов, проверки аутентичности, интегральности и прослеживаемости;
— записи, касающиеся операций по верификации и валидации;
— спецификации, процедуры, планы и результаты проведения тестов;
— ограничительные уставки систем безопасности и методология введения ограничительных уставок систем безопасности;
— процедуры, планы и результаты интеграции систем;
— документация, содержащая данные о рассмотрении и аудите процессов;
— матрицы прослеживаемости требований;
— процедуры технического обслуживания и эксплуатационные процедуры;
— технические аспекты закупочных спецификаций для оборудования и запчастей;
— протоколы квалификации;
— документация систем и компонентов СКУ (см. пункт 2.90).

2.50. В идентификационные данные единиц, в отношении которых применяется конфигурационное управление, следует включать номер ревизии.

2.51. Конфигурационный контроль следует применять на начальном этапе разработки СКУ, при внесении изменений в процессе разработки и в случае реализации модификаций.

2.52. При осуществлении конфигурационного управления следует обеспечивать фиксирование и сохранение информации по каждой единице, к которой применяется конфигурационное управление.

2.53. Фиксируемая информация включает: время, когда формирование единицы было в первый раз признано завершенным; изменения, которые были внесены в разные версии, включая в соответствующих случаях сообщения об изменениях; данные о зависимостях от других единиц, к которым применяется конфигурационное управление; статус утверждения единицы; данные о лицах, ответственных за ее создание, ревизию и утверждение.

2.54. Следует обеспечить, чтобы идентификационные данные программного обеспечения, установленного в оборудовании СКУ, а также значения конфигурационных данных были указаны непосредственно на самом оборудовании СКУ.

2.55. Возможность считывания идентификационных данных и значений конфигурационных данных будет облегчать проведение верификации того, что устройства сконфигурированы должным образом. Установка средств автоматической проверки или программных инструментов может также помочь в проведении такой верификации.

Анализ опасностей для системы контроля и управления

2.56. Для выявления условий, которые могут поставить под угрозу глубокоэшелонированную защиту или концепцию неодинаковости (диверсности) в проекте, следует проводить анализ опасностей в рамках всей структуры СКУ.

2.57. Следует провести анализ опасностей для каждой системы безопасности с целью для определения условий, которые могут привести к ухудшению осуществления ее функции безопасности.

2.58. К опасностям, которые следует учитывать, относятся внутренние и внешние опасности, отказы оборудования станции и отказы в работе СКУ или их ложное срабатывания вследствие отказа аппаратных средств или ошибок в системе программного обеспечения. Также следует учитывать сопутствующие опасности, которые могут возникнуть вследствие нежелательного взаимодействия.

2.59. В анализе опасностей для СКУ следует рассматривать все состояния и в режимы эксплуатации станции, включая переходные фазы между режимами эксплуатации. В анализ следует также включать рассмотрение деградировавших состояний.

2.60. Следует обеспечить, чтобы начальные результаты анализа опасностей для СКУ были получены до завершения работы над проектной основой общей структуры СКУ.

2.61. Анализ опасностей следует обновлять на каждой стадии жизненного цикла процесса разработки, включая (но не ограничиваясь этим) проектирование общей архитектуры СКУ и разработку спецификации требований к системам безопасности и проектирование, реализацию, установку и модификацию этих систем.

2.62. Целью актуализации анализа опасностей является определение опасностей, которые могут быть обусловлены особыми характеристиками систем безопасности СКУ, взаимодействием между системами безопасности СКУ и станцией и взаимодействием систем безопасности СКУ с другими СКУ, независимо от присвоенного им класса безопасности.

2.63. Следует принять меры по устранению, предупреждению или смягчению последствий воздействия выявленных опасностей, которые могут привести к деградации функций систем.

2.64. Меры по устранению, предупреждению или смягчению последствий воздействия опасностей могут принимать форму внесения изменений в требования, процесс проектирования или реализацию СКУ, или же внесения изменений в проект станции.

2.65. Следует обеспечить, чтобы методы, выбранные для анализа опасностей, соответствовали анализируемой единице.

Верификация и валидация

2.66. На каждой стадии жизненного цикла СКУ используется информация, полученная на более ранних стадиях, а также формируются данные, которые будут применяться в более поздних стадиях.

2.67. Результаты, полученные на каждой стадии жизненного цикла, следует верифицировать на предмет соблюдения требований, установленных для предыдущих стадий.

2.68. Матрица прослеживаемости требований может использоваться для документального подтверждения того, что требования удовлетворительным образом соблюдаются для каждой стадии жизненного цикла или что надлежащие меры были приняты в случаях, когда требования соблюдены не были.

2.69. Следует обеспечить, чтобы общая структура СКУ, каждая отдельная СКУ и каждый компонент СКУ были верифицированы с целью подтверждения соответствия всем требованиям (как функциональным требованиям, так и нефункциональным требованиям), а также выявления наличия любых нежелательных алгоритмов поведения (см. пункты 2.128–2.142). Требования, установленные для общей структуры СКУ, каждой отдельной СКУ и каждого компонента СКУ, следует валидировать с целью подтверждения их выполнения, как это было предусмотрено в проекте.

2.70. Следует обеспечить, чтобы верификация и валидация проводились отдельными специалистами, группами специалистов или группами специализированной организации, не зависимыми от проектировщиков и разработчиков.

2.71. Обеспечение независимой верификации и валидации, как правило, предполагает чтобы, что отдельные специалисты, группы специалистов или группы специализированной организации, проводящие верификацию и валидацию:

— обладали соответствующей компетенцией и знаниями;
— были способны самостоятельно определять объем выполняемой работы;
— не находились под давлением со стороны разработчиков;
— не вынуждены были действовать в условиях бюджетных ограничений или жестких графиков проведения работ, могущих помешать им завершить проверку в полном объеме;
— могли представлять результаты проверки руководству без негативно воздействующего давления со стороны группы разработчиков.

2.72. Следует обеспечить, чтобы степень и характер независимости верификации и валидации соответствовал классу безопасности проверяемой системы или ее компонентов. Верификация и валидация могут осуществляться параллельно с разными уровнями независимости (например, это может быть верификация и валидация, проводимые специалистами по тестированию, независимыми от разработчиков, в первоначальной организации-разработчике, и дополнительная независимая верификация и валидация, проводимые отдельной организацией).

2.73. Работы по верификации и валидации, включая записи о выявленных отклонениях и их локализации, следует документально оформлять. Следует обеспечить, чтобы в случае обнаружения отклонений на этапе верификации и валидации в отношении последующих модификаций или изменений в проекте и их реализации применялся процесс верификации и валидации, аналогичный процессу, который использовался ранее.

2.74. Содержание сообщений при осуществлении коммуникации между группами по верификации и валидации, группами по интеграции систем, группами по вводу в эксплуатацию, проектировщиками и разработчиками систем следует документировать.

Использование результатов вероятностного анализа безопасности

2.75. Пункт 5.76 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «В проекте должны надлежащим образом учитываться результаты вероятностного анализа безопасности станции применительно ко всем режимам эксплуатации и всем состояниям станции, включая останов, с уделением особого внимания, в частности:
> a) установлению того, что сбалансированный проект разработан таким образом, что никакое конкретное устройство или постулируемое исходное событие не вносят непропорционально большой или в значительной степени неопределенный вклад в общий объем рисков, и что уровни глубокоэшелонированной защиты независимы в той мере, в какой это практически осуществимо;
> b) обеспечению гарантий того, что будут предотвращаться ситуации, в которых небольшие отклонения параметров станции могут привести к сильным изменениям условий на станции (пороговым эффектам) [сноска опущена];
> c) сравнению результатов анализа с критериями приемлемости риска, если таковые были установлены».

2.76. При проектировании СКУ следует учитывать выводы, полученные в результате вероятностной оценки безопасности.

2.77. Подробная информация по вероятностной оценке безопасности и использованию результатов вероятностной оценки безопасности при проектировании приводится в соответствующих Нормах безопасности МАГАТЭ [12, 13].

Оценка безопасности

2.78. Оценку безопасности СКУ следует проводить в соответствии с требованиями публикации GSR Part 4 (Rev. 1) [5] и рекомендациями публикации Серии норм безопасности МАГАТЭ, № SSG-3, «Разработка и применение вероятностной оценки безопасности уровня 1 для атомных электростанций» [12] и, № SSG-2, «Детерминистический анализ безопасности атомных электростанций» [14].

2.79. В целях подтверждения соблюдения всех требований проектной основы общей архитектуры СКУ и каждой отдельной СКУ следует провести анализ и верификацию и валидацию проекта.

2.80. Пункт 3.14 содержит рекомендацию в отношении вопросов, которые следует учитывать в требованиях проектной основы применительно к общей архитектуре СКУ и всем отдельным СКУ. В пункте 3.15 рекомендуются дополнительные вопросы, которые следует учитывать в требованиях проектной основы, предназначенных для систем безопасности.

2.81. К стандартным методам анализа, верификации и валидации проекта относятся:

— анализ прослеживаемости: анализ прослеживаемости обычно применяется для подтверждения реализации и валидации требований;
— анализ видов и последствий отказов: анализ видов и последствий отказов часто применяется для подтверждения соблюдения критерия единичного отказа, а также для подтверждения того, что все известные виды отказов могут обнаруживаться сами по себе, либо могут быть выявлены в ходе проведения планового тестирования;
— анализ глубокоэшелонированной защиты и неодинаковости (диверсности): анализ глубокоэшелонированной защиты и неодинаковости является одним из средств исследования подверженности систем безопасности отказам по общей причине (см. публикацию [11], в которой приводится дополнительная информация по этому вопросу);
— анализ надежности: при анализе надежности применяются статистические методы в целях оценки надежности систем или компонентов. Широко используемые методы анализа надежности включают анализ количества элементов, анализ напряжения на элемент, анализ данных о долговечности (например, анализ Вейбулла), блок-схемы расчета надежности и анализ дерева отказов;

— валидация: процесс валидационного тестирования включает детерминированные методы, а также может включать статистические методы;
— тестирование на физическую безопасность (защищенность): тестирование на физическую безопасность (защищенность), как правило, требует наличия результатов оценки уязвимостей, и оно используется для подтверждения применения надлежащей практики обеспечения физической безопасности (защищенности);
— анализ, подтверждающий проектирование единиц с обеспечением надежности: такой анализ используется для подтверждения того, что при проектировании были применены меры, которые, согласно известным данным, способствуют достижению высокой надежности, такие как резервирование, соблюдение критерия единичного отказа, тестопригодность, отказобезопасное проектирование и жесткие требования к квалификации[9];
— подтверждение функциональных требований для различных режимов эксплуатации СКУ: сюда входит анализ корректного поведения системы во время и после перерывов в снабжении электроэнергией, перезапуска или перезагрузки и других переходных состояний. Изменения в календарном времени (переход на летнее время и високосные годы) также являются переходными состояниями.

2.82. Следует обеспечить, чтобы каждое допущение, используемое в анализе, было зафиксировано, и применение допущения было обосновано.

2.83. Следует обеспечить, чтобы методология любого проводимого анализа была тщательно определена и задокументирована вместе с исходными данными для анализа, результатами анализа и структурой анализа.

2.84. С учетом использования передовых наработок для системы, которая разрабатывается и проектируется в соответствии с высочайшими критериями качества, показатель отказ/запрос порядка 10^{-4}–10^{-5} может быть принят в качестве общего предела надежности, заявляемого в вероятностном анализе безопасности, при условии, что будут учтены все потенциальные источники отказов (исключая источники отказов, имеющие отношение к кибербезопасности) в связи с разработкой спецификации, проектированием, производством, монтажом, условиями

[9] Для проверки соответствия систем СКУ требованиям к надежности обычно необходимо использовать комбинацию количественного анализа, качественного анализа и тестирования.

эксплуатации и методами технического обслуживания. В этом показателе при необходимости может быть отражен риск отказов по общей причине в резервированных каналах системы, и он применяется ко всем элементам системы, от датчиков и устройств обработки выходных сигналов до исполнительного оборудования. Выбор более высокого заявленного уровня надежности, чем показатель, который указан выше, не исключаются, однако для этого потребуется должное обоснование с учетом всех упомянутых факторов.

2.85. Любые заявленные показатели надежности СКУ следует обосновывать, и следует обеспечить, чтобы они были в рамках допустимых пределов (в Приложении III указаны пределы, принятые в некоторых государствах).

2.86. В процессе проектирования и реализации взаимодействие каждой СКУ со станцией следует регулярно проверять на соответствие рекомендациям безопасности и рекомендациям, изложенным в публикации SSR-2/1 (Rev. 1) [1].

2.87. При обнаружении расхождений с этими требованиями процесс проектирования и реализации следует должным образом корректировать.

Документация

2.88. Следует обеспечить, чтобы документация СКУ:

— предусматривала способы передачи информации между различными стадиями и различными сторонами процесса разработки;
— содержала записи, отражающие правильное понимание и соблюдение всех требований в установленной системе;
— включала существенно важную для процесса эксплуатации информацию и информацию относительно проектирования системы безопасности для эксплуатационного персонала станции;
— служила основой при проведении работ по техническому обслуживанию станции и СКУ, а также при внесении последующих поправок в проект;
— была прослеживаемой на всех стадиях жизненного цикла СКУ;
— контролировалась в рамках системы конфигурационного управления;
— была однозначно сформулированной, полной, последовательной, хорошо структурированной, легко читаемой, доступной для понимания целевыми группами пользователей (например, экспертами

в соответствующей области, инженерами по безопасности и разработчиками программного обеспечения), проверяемой и удобной в ведении.

2.89. Надлежащим образом составленная документация облегчит ведение процессов эксплуатации, надзора, поиска и устранения неисправностей, технического обслуживания, последующей модификации и модернизации системы, а также обучения персонала станции и специалистов технической поддержки.

2.90. Следует обеспечить, чтобы эксплуатирующая организация разработала или получила документацию для систем и элементов СКУ, которая, как минимум, включает:

— требования к проектированию;
— функции и функциональное проектирование;
— принципы эксплуатации;
— описание роли системы в общей концепции станции;
— проектные решения, включая описание решений, важных для безопасности;
— исполнительную документацию («как построено») и документацию по конфигурации;
— фактическую компоновку («как построено») систем и их основных элементов, включая датчики и исполнительные устройства;
— описание взаимодействия с другими системами станции и взаимозависимости от них;
— меры и требования по осуществлению надзора, проведению испытаний, диагностики, технического обслуживания и эксплуатации;
— процедуры испытаний и их результаты;
— меры по квалификации оборудования;
— процессы проектирования и разработки и требования к качеству, соблюдаемые при проектировании;
— стратегии для всех этапов испытаний, включая стадию ввода в эксплуатацию;
— проектирование и разработку методов верификации и валидации и результаты применения этих методов;
— эксплуатационные процедуры для всех нормальных эксплуатационных состояний и режимов;
— аварийные эксплуатационные процедуры и руководства по управлению тяжелыми авариями для сценариев с постулируемыми авариями и запроектными условиями;

— рекомендации и закупочные спецификации для поставки запасных частей и элементов;
— проектные решения по обеспечению физической безопасности (защищенности) и их применение[10].

2.91. Следует обеспечить, чтобы документация по процессам и требованиям, относящимся к приобретению и поставке, проектированию, изготовлению, программным кодам, верификации и валидации, была доступна для ее оценки эксплуатирующей организацией, регулирующим органом или независимыми третьими сторонами, действующими от имени этих организаций (см. пункты 9.100–9.103).

ДЕЯТЕЛЬНОСТЬ, ОСУЩЕСТВЛЯЕМАЯ В ТЕЧЕНИЕ ЖИЗНЕННОГО ЦИКЛА

Спецификация требований

2.92. Следует обеспечить, чтобы требования к общей структуре всех СКУ, каждой отдельной СКУ и элементам СКУ были задокументированы надлежащим образом.

2.93. Следует обеспечить, чтобы совокупность требований, применяемых ко всем СКУ и отдельным СКУ, отвечала проектной основе, предусмотренной для всей структуры СКУ.

2.94. Следует обеспечить, чтобы требования, действующие в отношении всей структуры СКУ и каждой отдельной СКУ, были определены на базе проектной основы СКУ.

2.95. В разделе 3 изложены рекомендации по расчету и содержанию проектной основы общей структуры СКУ.

---

[10] Если при проектировании используются допущения в отношении политики и практики по обеспечению физической безопасности (защищенности) при эксплуатации (включая политику и практику обеспечения компьютерной безопасности), следует обеспечить, чтобы пользователь был осведомлен о применении таких допущений. Целесообразным может быть размещение элементов такой информации в отдельном документе в целях ее более ограниченного распространения по сравнению с другой системной информацией.

2.96. Следует обеспечить, чтобы в требованиях к системам и элементам в соответствующих случаях были детально отражены:

— функции, которые должна выполнять каждая отдельная СКУ;
— связи между входами и выходами для каждой функции в каждом состояния станции и в каждом режиме эксплуатации станции;
— минимальные показатели точности и достоверности и максимальное время реакции для измерений, управляющих функций и индикации;
— интерфейсы систем (между системой и оператором и с другими системами);
— средства самоконтроля, включая требуемые показатели синхронизации (включая время обнаружения дефекта и время восстановления);
— действия, которые осуществляет СКУ при обнаружении дефектов посредством самоконтроля;
— средства обеспечения физической безопасности (такие как проверки валидности, специальные средства контроля компьютерной безопасности и средства, обеспечивающие наследование функций контроля физической безопасности в соответствующих средах, а также наследование привилегий доступа);
— уровень надежности и эксплуатационной готовности, который должен быть достигнут, и любые вспомогательные требования, необходимые для обеспечения достижения такого уровня[11];
— оборудование и средства, необходимые для технического обслуживания;
— проектные ограничения[12];
— безопасная реакция на определенные виды отказов;
— устойчивость к воздействию полного диапазона эксплуатационных сред, связанных с нормальными условиями и аварийными условиями на станции, а также с предполагаемыми внутренними и внешними опасностями.

2.97. Следует обеспечить, чтобы проектные ограничения, если они необходимы, были указаны, обоснованы и были прослеживаемыми.

---

[11] Уровень надежности и эксплуатационной готовности может быть определен количественно или качественно, например, применительно к вспомогательным требованиям, о которых говорится выше, таким как требования к реализации конкретных стратегий обеспечения надежности, требования к характеристикам процесса разработки или требования в отношении соответствия определенным нормам или стандартам.

[12] Примеры проектных ограничений включают ограничения, применяемые в поддержку требований по обеспечению независимости и неодинаковости (диверсности).

2.98. Проектные требования, касающиеся обеспечения физической безопасности (защищенности) цифровых систем, следует разрабатывать с учетом результатов оценки рисков, связанных с физической безопасностью, и следует обеспечить, чтобы эти требования соответствовали политике эксплуатационной организации в области обеспечения физической безопасности.

2.99. Для управления требованиями на протяжении жизненного цикла и для обеспечения соблюдения, верификации, валидации и реализации всех требований следует применять особые процессы.

2.100. Разработка требований — это особый процесс, направленный на обеспечение того, чтобы цели обеспечения безопасности, достигаемые с помощью СКУ, были учтены при проектировании.

2.101. Требования следует вводить в действие и документально оформлять с использованием заранее определенного набора методов, соответствующего важности системы для безопасности.

2.102. Методами разработки и документирования требований может предусматриваться применение в спецификации языка, предполагающего использование строго определенного синтаксиса и семантики, моделей, анализа и пересмотра.

2.103. Требования по мере возможности следует составлять с указанием того, что должно быть достигнуто, а не того, как эти требования должны разрабатываться и реализовываться.

2.104. Требования следует излагать так, чтобы они были понятны всем заинтересованным сторонам (например, лицензиатам, поставщикам и проектировщикам).

2.105. Следует обеспечить, чтобы документация требований содержала ссылки на дополнительную информацию, включала такую дополнительную информацию непосредственно или в виде дополнения, например, справочную информацию о конкретных требованиях, факторах риска, рекомендациях по проектированию функций или средств безопасности, в той мере, в какой это необходимо для обеспечения понимания этих требований целевыми группами пользователей.

2.106. Требования, потенциально способные оказывать влияние на безопасность, следует обозначать в качестве таковых.

2.107. В целях облегчения верификации, валидации, прослеживаемости к документации более высокого уровня и демонстрации того, что все соответствующие требования проектной основы были учтены, следует определить происхождение и обоснование каждого требования.

Подбор ранее разработанных изделий

2.108. Ранее разработанные изделия следует надлежащим образом квалифицировать (аттестовать) в соответствии с рекомендациями, изложенными в пунктах 6.78–6.134.

2.109. К ранее разработанным изделиям относятся аппаратные устройства (технические устройства), ранее разработанное программное обеспечение (программные средства), готовые коммерческие устройства, цифровые устройства, содержащие как аппаратные, так и программные средства, аппаратные устройства, конфигурированные с использованием языка описания аппаратных средств, или ранее разработанные функциональные блоки, используемые в языке описания аппаратных средств.

2.110. Публикация [11] содержит более детальную информацию об использовании готовых коммерческих устройств.

2.111. Следует показать, что любые функции ранее разработанного изделия, которые не участвуют в процессе реализации системы безопасности СКУ, не вступают в неприемлемое взаимодействие с функциями безопасности системы.

2.112. Ранее разработанные изделия по возможности следует конфигурировать так, чтобы неиспользуемые функции были деактивированы.

2.113. Выбираемые ранее разработанные изделия часто являются готовыми коммерческими изделиями. Применение готовых коммерческих изделий может способствовать снижению расходов и облегчению процесса ведения проектно-конструкторских работ. Кроме того, в случае, когда невозможно приобрести изделие, предназначенное специально для атомных

электростанций, использование проверенной готовой коммерческой продукции может оказаться более эффективным и надежным способом, чем разработка новой компонентной единицы.

2.114. Вместе с тем готовые коммерческие изделия нередко являются более сложными, могут содержать непредусмотренный функционал и часто быстро становятся устаревшими. Они часто могут иметь функции, в применении которых на АЭС нет необходимости. Проведение квалификационных проверок готовых коммерческих изделий может быть затруднено в виду того, что процессы разработки коммерческих изделий являются менее открытыми и хуже поддающимися контролю, чем процессы, описанные в настоящем Руководстве по безопасности. Нередко для проведения квалификационных проверок необходимо взаимодействие с поставщиком. Из-за отсутствия информации, подтверждающей качество и надежность продукции, часто могут возникать трудности, связанные с приемкой готового коммерческого изделия.

2.115. При принятии решения об использовании готовых коммерческих изделий лицензиату следует учитывать необходимость поддержания квалификационных характеристик этих изделий в течение срока службы станции.

2.116. Например, в линейке продукции могут предусматриваться частые конструктивные изменения, такие как замена субкомпонентов, новые версии аппаратно-программного обеспечения, новые технологии производства или новые версии программного обеспечения. У поставщика, также как и у работников станции, отвечающих за конфигурационное управление, могут возникать сложности, связанные с надлежащей идентификацией таких изменений, в особенности при проведении технического обслуживания СКУ и организации поставки запасных частей и работ по замене. В некоторых случаях эксплуатирующие организации закупают объем конкретной версии запасных частей для устройств на весь срок их службы во избежание того, что какая-нибудь деталь или версия станет недоступной для приобретения.

2.117. Следует обеспечивать, чтобы к ранее разработанным изделиям прилагалась документация, содержащая необходимую информацию по их применению в СКУ.

Проектирование и применение систем контроля и управления

2.118. Проектирование общей архитектуры СКУ и отдельных СКУ следует строить на системном и последовательном распределении необходимой функциональности, а также с учетом других требований.

2.119. Системные требования, которым должна соответствовать СКУ, следует применять к надлежащей комбинации аппаратных средств, устройств, конфигурированных с применением языка описания аппаратных средств, и программных средств (при их наличии).

2.120. Аппаратные средства могут включать интегральные схемы, предназначенных для определенных режимов использования. В число программных средств могут входить уже существующее программные средства и аппаратно-программное обеспечение, например, операционная система, программные средства, подлежащие разработке, или программное обеспечение, создаваемое путем конфигурирования ранее разработанных программных средств. В пересмотренных и доработанных требованиях могут быть также учтены проектные решения более низкого уровня, относящиеся к узлам, расположенным вне СКУ, например, в отношении типа и производительности исполнительных устройств.

2.121. Следует показать, что выполнение требований, не важных для безопасности, отрицательно не влияет на реализацию функций, важных для безопасности.

2.122. В правилах проектирования следует предусматривать обеспечение возможности проведения верификации и валидации внутренней логики каждой СКУ.

2.123. При проектировании следует учитывать параметры СКУ, подлежащие конфигурированию, верификации и валидации при эксплуатации, а также следует предусмотреть меры, обеспечивающие выполнение этих процессов (например, уставки на срабатывание системы аварийной защиты реактора, калибровочные постоянные и параметры конфигурации программных средств).

Интеграция систем

2.124. Следует обеспечить, чтобы при интеграции систем:

— охватывались все интерфейсы между интегрируемыми компонентами, например, между аппаратными (техническими) и программными средствами или между модулями программного обеспечения;
— подтверждалось соблюдение требований для интерфейсов между различными компонентами системы;
— подтверждалось функционирование компонентов, подузлов и подсистем в соответствии с проектом в интегрированной системе так, чтобы система соответствовала установленным требованиям, предъявляемым к системе, включая требования, охватывающие значения вне установленного диапазона, применение исключений и синхронизацию.

2.125. До начала процесса интеграции системы следует обеспечить наличие последовательной конфигурации верифицированных модулей (аппаратных и программных).

2.126. Для контроля передачи модулей для сборки в компоненты системы, а также для контроля версии программного обеспечения, применяемой для валидации системы, обычно используются программные инструменты. Программные инструменты также применяются на объекте во время эксплуатации для облегчения конфигурационного контроля и прослеживаемости между установленными компонентами и валидированными компонентами.

2.127. Следует обеспечить, чтобы задокументированный анализ прослеживаемости применялся для демонстрации завершения интеграции системы в соответствии с проектной спецификацией системы, а также для подтверждения достижения целей, изложенных в пункте 2.124.

Валидация систем

2.128. Валидацию следует проводить для каждой отдельной СКУ и для интегрированного комплекса нескольких СКУ.

2.129. Для целей настоящего Руководства по безопасности процесс валидации системы считается законченным с момента завершения установки системы на станции. В случае необходимости проведения

дополнительных мероприятий по валидации системы после ее установки на станции эти мероприятия могут быть включены в программу испытаний в период ввода в эксплуатацию при условии, что результаты будут отражены в протоколах валидационных испытаний и что группа проектировщиков и валидационная комиссия будут работать независимо друг от друга, как определено в пунктах 2.71 и 2.72.

2.130. Следует обеспечить, чтобы система, тестируемая для целей валидации, была репрезентативной применительно к окончательной конфигурации СКУ на объекте.

2.131. Следует обеспечить, чтобы программное обеспечение, подлежащее валидации, было идентично программным средствам, которые будут использоваться при эксплуатации.

2.132. Следует обеспечить, чтобы результаты валидации системы показывали, что система соответствует всем действующим требованиям в любых условиях взаимодействия и при любых режимах нагрузки.

2.133. Тестирование режимов эксплуатации и взаимодействия между СКУ и станцией, которые не удалось полностью протестировать во время валидации системы, следует выполнить в период ввода в эксплуатацию (проведения пуско-наладочных работ), либо следует провести их валидацию посредством выполнения дополнительного анализа.

2.134. Следует обеспечить, чтобы валидации системы охватывала:

— все элементы системы;
— полный спектр интерфейсных сигналов[13], включая сигналы, отражающие значения вне установленного диапазона;
— применение исключений;
— точность и гистерезис заданных уставок;
— все режимы эксплуатации станции и систем, включая переходы между режимами;
— восстановление после сбоя в подаче электроэнергии;
— синхронизацию;
— устойчивость к нежелательным воздействиям и переносимость дефектов.

---

[13] К интерфейсным сигналам относятся, например, входные и выходные сигналы других систем, датчиков, исполнительных устройств и операторских интерфейсов.

2.135. Следует обеспечить, чтобы валидационные испытания системы охватывали вариации всех входных параметров, т.е. следует использовать динамический метод проведения испытаний.

2.136. Динамические испытания следует строить на применении реалистичных сценариев, являющихся репрезентативными применительно к изменениям параметров станции, которые будут требовать использования СКУ и которые основаны на анализе возможных сценариев развития событий на станции.

2.137. Функциональные испытания следует строить так, чтобы они охватывали все алгоритмы поведения, допускаемые функциональными требованиями. Следует обеспечить, чтобы структурный охват, предусмотренный для функциональных испытаний, был обоснован с учетом функциональных требований.

2.138. Следует рассмотреть возможность проведения валидационных испытаний с использованием статистических методов.

2.139. Следует рассмотреть использование средств моделирования для валидации системы.

2.140. При валидации системы следует выполнить в максимально возможной степени валидацию руководств по эксплуатации системы и соответствующих разделов по техническому обслуживанию.

2.141. Следует обеспечить, чтобы задокументированный анализ прослеживаемости демонстрировал, что валидация системы завершена в соответствии со спецификацией требований, предъявляемых к системе, и что цели, изложенные в пунктах 2.132 и 2.134, были достигнуты.

2.142. Следует обеспечить, чтобы полный комплект документации по испытаниям был достаточным для повторения тестирования с уверенностью, что последовательно будут получены удовлетворительные результаты при повторном проведении ранее успешных испытаний.

Установка, общая интеграция СКУ и ввод в эксплуатацию

2.143. Установку СКУ на станции следует выполнять в соответствии с утвержденным проектом.

2.144. Следует обеспечить, чтобы была проведена инспекционная проверка оборудования при его получении, либо проведены его приемо-сдаточные испытания с тем, чтобы убедиться в том, что системы и компоненты не пострадали в процессе транспортировки.

2.145. В нижеследующих пунктах описываются факторы, которые необходимо учитывать при применении рекомендаций, изложенных в публикации Серии норм безопасности МАГАТЭ, № SSG-28, «Ввод в эксплуатацию атомных электростанций» [15] в отношении СКУ.

2.146. Следует обеспечить, чтобы ввод в эксплуатацию предусматривал постепенную интеграцию СКУ с другими компонентами и другими узлами станции, а также верификацию того, что они соответствуют принятым в проекте допущениям и удовлетворяют критериям функциональности и работоспособности.

2.147. Испытания, проводимые в станционной среде, являются важной составной частью работ по вводу в эксплуатацию.

2.148. При вводе в эксплуатацию особое внимание следует уделять верификации интерфейсов с внешними системами и подтверждению корректности функционирования вместе с интерфейсными устройствами.

2.149. Следует обеспечить, чтобы на стадии ввода в эксплуатацию все СКУ проработали в течение продолжительного времени в условиях эксплуатации, проведения испытаний и обслуживания, которые в максимально возможной степени являются репрезентативными по отношению к реальным условиям эксплуатации.

2.150. До окончания процесса ввода в эксплуатацию следует провести валидацию руководств по эксплуатации и соответствующих частей руководства по техническому обслуживанию.

2.151. Прежде чем признать системы СКУ пригодными для эксплуатации, следует завершить соответствующие плановые операции жизненного цикла, обеспечить прослеживаемость применения требований до установленных систем, а также следует обеспечить, чтобы составление исполнительной и проектной документация, отражающей фактическую конфигурацию («как построено»), было завершено.

Эксплуатация и техническое обслуживание

2.152. Мероприятия по техническому обслуживанию и контролю применительно к СКУ следует проводить в соответствии с руководящим материалом публикации Серии норм безопасности МАГАТЭ, № NS-G-2.6, «Техническое обслуживание, надзор и инспекции при эксплуатации на атомных электростанциях» [16], в которой изложены рекомендации по планированию, организации и осуществлению мероприятий по техническому обслуживанию и надзору, включая калибровку, применительно к СКУ.

2.153. В нижеследующих пунктах (2.154–2.156) изложены рекомендации по применению руководства NS-G-2.6 [16] к системам СКУ.

2.154. Изменения в параметры СКУ следует вносить с использованием надлежащих средств.

2.155. Следует обеспечить мониторинг действий персонала при эксплуатации и проведении мероприятий по техническому обслуживанию СКУ с целью последующего документального фиксирования опыта эксплуатации, который может указывать на необходимость внесения модификаций для снижения вероятности ошибок человека.

2.156. Следует обеспечить, чтобы на протяжении предполагаемого срока службы в наличии было достаточное количество запасных частей для осуществления эксплуатации и проведения технического обслуживания (количество может быть определено, например, на основе проектных данных СКУ, надежности компонентов и доступности в будущем запасных частей и сервисных услуг поставщика).

Модификации

2.157. В нижеследующих пунктах изложены рекомендации по применению руководства по безопасности NS-G-2.3 [9] к СКУ.

2.158. При проектировании модернизации и модификации СКУ следует учитывать:

— ограничения, связанные с физическими характеристиками сооруженной станции, которые существенно ограничивают варианты проектирования систем СКУ;

— возможную необходимость обеспечения согласованности конструкции оборудования, предназначенного для использования в качестве замены, с установленным оборудованием СКУ в целях, например, снижения сложности общего операторского интерфейса и мероприятий по техническому обслуживанию станции;
— практические соображения в отношении применения коммерчески доступных технологий или оборудования, а также перспектив оказания поддержки производителями или третьими сторонами в применении таких технологий и оборудования в течение установленного срока эксплуатации оборудования;
— необходимость в актуализации существующей проектной документации[14].

2.159. В случае, если осуществляется модификация СКУ или если система является частью модернизируемого оборудования, уровень строгости, который применяется при обосновании и осуществлении изменений, следует устанавливать заранее.

2.160. Следует обеспечить, чтобы уровень строгости устанавливался с учетом роли и функции соответствующих систем в обеспечении безопасности атомной электростанции совместно с остающимися системами, которые будут эксплуатироваться по окончании работ. Эта рекомендация также применима и в отношении внесения изменений в программные инструменты.

2.161. Разработку модификации или модернизации СКУ следует проводить в соответствии с установленными требованиями в отношении процессов жизненного цикла.

2.162. Сложность процесса жизненного цикла, модификация которого необходима, обусловливается сложностью этой модификации и ее важностью для безопасности.

[14] Проектная документация старых систем может быть неполной или неточной. Вследствие этого для значительной модификации или замены таких систем может потребоваться применение «реверс-инжиниринга» с целью воссоздания оригинальных проектных основ и спецификаций.

2.163. Следует обеспечить, чтобы жизненный цикл даже самых простых изменений, как минимум, включал стадии жизненного цикла отдельной системы, как показано на рис. 2, включая верификацию и валидацию после осуществления каждой модификации СКУ.

2.164. Применительно к учету человеческого фактора может потребоваться проведение дальнейшего анализа временных конфигураций человеко-машинного интерфейса, отражающих переход между новыми и существующими СКУ, чтобы обеспечить возможность использования временного оборудования или временных процедур. Расширение возможностей интерфейса во взаимодействии с оператором может привести к увеличению числа ошибок эксплуатационного персонала и персонала, выполняющего работы по техническому обслуживанию, в течение некоторого времени после введения изменений. В некоторых случаях могут потребоваться изменения в учебной подготовке персонала.

2.165. При замене СКУ следует рассматривать возможность эксплуатации новой СКУ параллельно со старой системой в течение испытательного периода, а именно до тех пор, пока не появится достаточная уверенность в адекватности новой системы. Также параллельная эксплуатация возможна с одновременной установкой нового резервированного оборудования на одну линию.

2.166. При рассмотрении целесообразности параллельной эксплуатации СКУ следует оценить негативные факторы, связанные с эксплуатационными проблемами и сложностями, сопоставив их с повышением уверенности, а также провести оценку всех возможных рисков.

2.167. Последствия модернизации или внесения изменений в программные средства в период между начальным этапом разработки и модификацией могут быть значительными, и следует оценить их возможное воздействие (например, модернизация компилятора может привести к аннулированию полученных ранее результатов анализа или необходимости верификации адекватности компилятора).

3. ПРОЕКТНАЯ ОСНОВА ДЛЯ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

ОПРЕДЕЛЕНИЕ ФУНКЦИЙ КОНТРОЛЯ И УПРАВЛЕНИЯ

3.1. В требовании 4 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Во всех состояниях станции должно обеспечиваться выполнение следующих фундаментальных функций безопасности АЭС: i) управление реактивностью, ii) отвод тепла от реактора и бассейна выдержки топлива и iii) локализация радиоактивного материала, защита от излучения и контроль за плановыми радиоактивными выбросами, а также ограничение аварийных радиоактивных выбросов».

3.2. Пункт 4.1 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «При определении важных для безопасности узлов, необходимых для выполнения фундаментальных функций безопасности, и при выявлении естественных (внутренних) свойств, которые способствуют выполнению фундаментальных функций безопасности или влияют на эти функции во всех состояниях станции, должен использоваться системный подход».

3.3. Пункт 4.2 публикации SSR-2/1 (Rev. 1) [1] гласит: «Должны быть предусмотрены средства контроля состояния станции, обеспечивающие выполнение требуемых функций безопасности».

3.4. Требуемые функции безопасности определятся в процессе проектирования атомной электростанции (см. раздел 4 публикации SSR-2/1 (Rev. 1) [1]), и при распределении этих функций между конструкциями, системами и элементами станции следует использовать системный подход.

3.5. Следует определить необходимые функции (а также соответствующие нефункциональные требования к таким параметрам, как безопасность, физическая безопасность (защищенность) и ограничения синхронизации) для СКУ в рамках процесса проектирования атомной электростанции.

3.6. В число функций, предусматриваемых для СКУ, входят функции, обеспечивающие наличие информации и возможностей управления, важных для эксплуатации станции в различных эксплуатационных состояниях и в аварийных условиях. Согласно концепции глубокоэшелонированной защиты задачи этих функций сводятся к:

— предотвращению отклонений от нормальной эксплуатации;
— обнаружению сбоев и контролю нарушений нормальной эксплуатации;
— контролю аварий, учитываемых в проектной основе станции (проектных аварий);
— контролю последствий запроектных условий;
— смягчению радиологических последствий аварий.

СОДЕРЖАНИЕ ПРОЕКТНОЙ ОСНОВЫ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

3.7. В требовании 14 публикации SSR-2/1 (Rev. 1) [1] указано:

> «В проектных основах узлов, важных для безопасности, должны быть указаны требуемые возможности, надежность и функциональность в соответствующих эксплуатационных состояниях, аварийных условиях и условиях, возникающих вследствие внутренних и внешних опасностей, с тем чтобы обеспечить удовлетворение критериев приемлемости в течение срока службы АЭС».

3.8. Пункт 5.3 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Проектные основы каждого узла, важного для безопасности, должны систематически обосновываться и документироваться. В документации должна содержаться информация, необходимая эксплуатирующей организации для безопасной эксплуатации станции».

3.9. Для общей архитектуры СКУ и каждой отдельной СКУ следует иметь задокументированную проектную основу.

3.10. Общая архитектура СКУ представляет собой организационную структуру отдельных СКУ станции. Общая архитектура СКУ атомной электростанции включает многочисленные СКУ, для каждой из которых отводится своя конкретная роль.

3.11. Проектная основа определяет функции, состояния и требования общей структуры СКУ и каждой отдельной системы СКУ. Далее эта информация используется для классификации функций и присвоения системам определенного класса безопасности [17].

3.12. В ряде случаев требования к системе СКУ могут быть определены только после завершения разработки проекта и проектной основы атомной электростанции. Таким образом, полное содержание проектной основы СКУ может отсутствовать на момент начала осуществления проекта.

3.13. Следует обеспечить, чтобы разработка проектной основы СКУ регламентировалась документацией проектной основы безопасности станции и обеспечивалось предоставление информации, касающейся:

— концепций глубокоэшелонированной защиты станции;
— необходимых функции по обеспечению безопасности (см. пункт 3.11);
— категорий безопасности, функциональных требований и требований к эксплуатационным характеристикам, предъявляемых к функциям станции, важным для безопасности;
— принципов установления приоритета в выборе между автоматическим срабатыванием и действиями оператора и между автоматизированными действиями, когда запустить устройство или функцию способна более чем одна система;
— национальных требований к лицензированию СКУ;
— национальных требований к классификации безопасности для СКУ;
— национальных требований в отношении эксплуатационных требований;
— анализа и определения цифровых СКУ, важных для функций безопасности и физической безопасности на станции;
— оценки риска и анализа воздействий на компьютерную безопасность;
— потребностей и распределения информации и контроля;
— основной концепции эксплуатации станции;
— анализа надежности человеческого фактора;
— функций эксплуатационного персонала;
— уровней укомплектованности штатов;

3.14. Следует обеспечить, чтобы в проектной основе СКУ были определены требуемые уровни работоспособности, надежности и функциональности общей структуры СКУ и каждой системы СКУ, включая:

— все функциональные требования, например:
  - эксплуатационные состояния станции, в которых требуется функционирование СКУ;
  - различные конфигурации станции, при которых каждая СКУ должна быть работоспособной;
  - функциональные требования[15] для каждого состояния станции, каждого режима эксплуатации станции и длительного останова;
  - значимость для безопасности каждой требуемой функции СКУ;
  - постулированные исходные события, на которые система должна реагировать;
  - роль каждой отдельной СКУ в реализации концепции глубокоэшелонированной защиты в общей структуре СКУ;
  - параметры или сочетания параметров, мониторинг которых должен осуществляться;
  - необходимые функции управления и защиты, включая спецификацию действий, которые должны выполняться автоматически, вручную или обоими способами, а также расположение средств управления;
  - требуемые пределы, скорость изменения, корректность, квантизация цифрового представления, точность вычислений и скорость реакции для каждой функции безопасности СКУ;
— все требования, устанавливаемые для достижения необходимого уровня надежности и эксплуатационной готовности, например:
  - требования, касающиеся независимости функций безопасности;
  - требования по проведению периодических испытаний, самодиагностики и обслуживания;
  - требуемые качественные и количественные показатели надежности и эксплуатационной готовности [16];
  - требования, касающиеся поведения при возникновении сбоя в процессе;

---

[15] Функциональные требования определяют, например, преобразования входов в выходы, а также меры, которые должны быть приняты;

[16] Пределы надежности и эксплуатационной готовности систем и компонентов могут быть определены с использованием детерминистических критериев, вероятностных критериев (например, соблюдения критерия единичного отказа или специальных процедур и методов верификации программного обеспечения) или обоих критериев одновременно.

— все требования, устанавливаемые для достижения необходимого уровня физической безопасности (защищенности), например:
  • ограничения, связанные с обеспечением физической безопасности, или эксплуатационные ограничения, которые должны быть учтены при проектировании;
  • меры физической безопасности, которые должны быть реализованы;
— все требования, необходимые для обеспечения надлежащей квалификации оборудования, например:
  • проектные критерии, включая спецификацию норм, которым СКУ должны соответствовать;
  • условия на станции, способные привести к деградации функционирования систем при выполнении ими своих функций, и меры, которые должны быть приняты для поддержания необходимой работоспособности;
  • спектр внутренних и внешних опасностей (включая природные явления), при которых система должна выполнять функции, важные для безопасности;
  • спектр условий окружающей среды на станции[17], при которых система должна выполнять функции, важные для безопасности;
  • ограничения, действующие в отношении используемых материалов;
  • ограничения, обусловленные физической конструкцией и компоновкой станции, включая ограничения, касающиеся размещения оборудования, прокладки кабелей и источников питания;
  • физическое расположение оборудования и интерфейсы между единицами оборудования.

3.15. В дополнение к рекомендациям, изложенным в пункте 3.14, в проектную основу систем безопасности следует включить:

— предельные значения параметров, необходимые для активации систем безопасности (аналитические пределы; см. пункт 6.209 и рис. 3 на стр. 103);

---

[17] К условиям окружающей среды на станции, о которых идет речь, относятся нормальные условия, внештатные условия и экстремальные условия, воздействию которых оборудование СКУ может подвергнуться при проектных авариях, внутренних событиях или внешних событиях. Любые взаимодействия различных СКУ, в особенности между компонентами, квалифицированными на разном уровне, могут поставить под угрозу соблюдение требований по обеспечению глубокоэшелонированной защиты, если они не будут в полной мере учтены.

— переменные величины и состояния, которые должны отображаться, чтобы операторы могли удостовериться в работе защитных функций системы;
— обоснование любых действий по обеспечению безопасности, не автоматически инициированных, включая:
  • происшествия, инцидентны, временные интервалы и условия на станции, для которых допускается ручное управление;
  • обоснование для разрешения на инициирование или управление после инициирования исключительно ручными методами;
  • диапазон окружающих условий работы операторов, при которых предполагается принятие мер операторами вручную при эксплуатационных состояниях и в аварийных условиях;
  • подтверждение того, что информация, которую операторы должны учитывать при выполнении действий вручную, будет отображаться в соответствующих местах и будет отражать эксплуатационные характеристики, необходимые для обоснования действий оператора;
— условия, при которых разрешен байпас функций СКУ по обеспечению безопасности;
— условия, которые должны быть выполнены до того, как запущенная защитная система может быть возвращена в исходное состояние;
— требования к различным функциям, обеспечивающих смягчение последствий отказа по общей причине.

3.16. Вышеупомянутые элементы могут быть включены в проектную основу общей структуры СКУ, либо в проектную основу отдельных систем. В случае некоторых элементов может требоваться дополнительное нормирование общих требований в проектной основе общей структуры СКУ и включение более подробных сведений в проектную основу отдельных систем. Следует обеспечить, чтобы проектные основы общей структуры СКУ и отдельных систем в любом случае соответствовали друг другу и взаимосвязь и взаимодействие между разными проектными основами были легко понятными.

4. АРХИТЕКТУРА КОНТРОЛЯ И УПРАВЛЕНИЯ

ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ

4.1. При проектировании архитектуры всей совокупности СКУ предусматривается:

— определение состава СКУ, образующих общую архитектуру;
— организация этих систем;
— распределение функций контроля и управления среди этих систем;
— взаимосвязь между СКУ и наличие соответствующих допустимых и запрещенных взаимодействий;
— введение проектных ограничений (включая недопустимые взаимодействия и алгоритмы поведения) для общей архитектуры;
— определение границ между различными СКУ.

4.2. При проектировании архитектуры отдельных СКУ предусматривается:

— установление отношений «композиция–декомпозиция» на всех уровнях интеграции до неделимой, отдельной единицы;
— распределение функций контроля и управления, алгоритмов поведения, ограничений и (производных) требований по качеству для каждой единицы на каждом уровне интеграции;
— наличие правил компонуемости и композиции для обеспечения того, чтобы композиционный состав алгоритмов поведения на одном уровне интеграции согласовывался с алгоритмами поведения, требуемыми на следующем более высоком уровне интеграции, и не добавлял других алгоритмов поведения;
— взаимосвязь между единицами на каждом уровне интеграции и между уровнями интеграции и наличие соответствующих предусмотренных и недопустимых взаимодействий;
— введение проектных ограничений (включая недопустимые взаимодействия и алгоритмы поведения) для каждой отдельной СКУ.

4.3. Современные системы СКУ являются более взаимосвязанными и труднее поддаются анализу (и, таким образом, обеспечение безопасности усложнилось по сравнению с предыдущими поколениями СКУ). Качественно разработанная архитектура СКУ обеспечивает глубокоэшелонированную защиту и неодинаковость (диверсность), а также

локализацию и концентрацию сложных для анализа средств в системе таким образом, чтобы эти средства не приводили к чрезмерному усложнению процесса обеспечения безопасности станции.

4.4. Следует обеспечить, чтобы общая архитектура СКУ и архитектура отдельных СКУ удовлетворяли требованиям станции, включая требования к системным интерфейсам и требования к таким характеристикам, как безопасность, физическая безопасность, верифицируемость, анализируемость и ограничения синхронизации.

4.5. Требование 7 публикации SSR-2/1 (Rev. 1) [1] гласит: «В проекте АЭС должна быть предусмотрена глубокоэшелонированная защита. Уровни глубокоэшелонированной защиты должны быть настолько независимыми, насколько это практически возможно».

4.6. В публикациях [18, 19] приводится объяснение концепции глубокоэшелонированной защиты и описание уровней глубокоэшелонированной защиты.

4.7. Следует обеспечить, чтобы общая архитектура СКУ не создавала угрозы для концепции глубокоэшелонированной защиты и принципов обеспечения неодинаковости, применяемых в проекте станции.

4.8. В общей архитектуре СКУ следует определить концепцию глубокоэшелонированной защиты и принципы обеспечения неодинаковости, которые должны применяться в рамках общей структуры СКУ.

4.9. При проектировании общей архитектуры СКУ также устанавливается уровень независимости между СКУ, поддерживающими различные уровни реализации концепции глубокоэшелонированной защиты и принципов обеспечения неодинаковости на станции.

4.10. Глубокоэшелонированная защита в рамках общей архитектуры СКУ достигается посредством построения независимых линий защиты таким образом, чтобы отказ одной линии защиты компенсировался функционированием следующей линии.

СОДЕРЖАНИЕ ОБЩЕЙ АРХИТЕКТУРЫ КОНТРОЛЯ И УПРАВЛЕНИЯ

4.11. Следует обеспечить, чтобы общая архитектура СКУ:

— включала все функции СКУ, необходимые для реализации проектной основы станции;
— определяла вопросы, которые будут систематически затрагиваться при работе с СКУ[18];
— определяла отдельные СКУ, которые будут включены в общую архитектуру СКУ в целях:
  • поддержки концепций глубокоэшелонированной защиты и неодинаковости, применяемых на станции;
  • поддержки требований проектной основы к независимости общей системы СКУ;
  • надлежащего разделения систем разных классов безопасности и функций разных категорий безопасности;
— определяла связи и средства коммуникации между отдельными СКУ;
— определяла необходимые проектные стратегии, применяемые в целях соблюдения требований к надежности каждой функции обеспечения безопасности, относящейся к общей архитектуре СКУ[19];
— поддерживала соблюдение в группах безопасности критерия единичного отказа;
— обеспечивала получение информации, необходимой для главного щита управления, дополнительного щита управления и других пунктов, где может требоваться информация для целей эксплуатации или управления аварией;
— включала необходимые средства управления в помещении главного щита управления, дополнительного щита управления и других местах, где могут требоваться средства управления для целей эксплуатации или управления аварией;

---

[18] Вопросы для последовательного рассмотрения применительно к СКУ включают, например, применение эксплуатационной концепции для станции, применение проектных норм для человеко-машинного интерфейса, ограничения для путей прокладки кабелей, технологии заземления и основные принципы управления сигнализацией.

[19] Стратегии определения требований к надежности могут включать соблюдение критерия единичного отказа, резервирование, обеспечение независимости между функциями резервирования, отказобезопасное проектирование, обеспечение неодинаковости (диверсности) и верифицируемости (включая анализируемость и тестопригодность). В разделе 6 изложены соображения в отношении реализации стратегий достижения надежности.

— включала автоматические средства управления, необходимые для поддержания и установления ограничений для параметров процессов в рамках определенного рабочего диапазона, а также для ограничения последствий отказов и отклонений от нормального режима эксплуатации так, чтобы они не выходили за рамки возможностей систем безопасности.

4.12. Характеристики платформ СКУ, используемых для реализации различных СКУ, могут влиять на проектирование общей архитектуры СКУ, а общая архитектура СКУ, в свою очередь, определяет функциональные и квалификационные требования, предъявляемые к платформам СКУ. В связи с этим обычно рекомендуется подбирать платформы СКУ в соответствии со спецификацией характеристик общей архитектуры СКУ. Функциональные и квалификационные требования, применяемые в случае систем безопасности, как правило, отличаются от функциональных и квалификационных требований, действующих в отношении систем управления. В силу этого, а также по соображениям обеспечения неодинаковости в общей структуре СКУ обычно используется две или более платформ.

СОДЕРЖАНИЕ АРХИТЕКТУРЫ ОТДЕЛЬНЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

4.13. Следует обеспечить, чтобы при проектировании архитектуры каждой СКУ:

— предусматривались все функции СКУ, необходимые для выполнения задачи, определенной для этой системы в рамках общего архитектурного проекта СКУ;
— при необходимости система разделялась на резервированные отдельные группы и определялась требуемая степень независимости между такими группами[20];
— определялись единицы СКУ, подлежащие включению в каждую из резервированных отдельных групп;

[20] Как правило, системы безопасности организуются в резервированные отдельные группы с целью обеспечения соблюдения критерия единичного отказа. Для систем с более низким классом безопасности резервирование элементов для обеспечения безопасности может не требоваться, однако такое резервирование может быть предусмотрено для повышения уровня надежности этих элементов в условиях нормальной эксплуатации.

— указывалось распределение функций СКУ и других системных требований применительно к каждой компонентной единице СКУ;
— определяло интерфейсы и средства коммуникации между единицами СКУ в рамках системы;
— определялись основные проектные решения, относящиеся к основным компонентным единицам и каналам передачи данных.

НЕЗАВИСИМОСТЬ

4.14. Обеспечение независимости в рамках общей архитектуры СКУ преследует цель предотвращения распространения отказов между системами и предупреждения, когда это практически возможно, воздействия одного и того же источника отказа по общей причине на многие системы. Примеры таких источников отказа по общей причине включают внутренние события, внешние события и отказ общих сервисных систем поддержки.

4.15. Следует обеспечить, чтобы общая архитектура СКУ негативно не влияла на независимость групп систем безопасности, а также на независимость различных уровней глубокоэшелонированной защиты, применяемой на станции.

4.16. Функции СКУ, которые должны быть полностью независимы, следует закрепить за независимыми системами аппаратного обеспечения или независимыми компонентными единицами.

4.17. Следует обеспечить, чтобы системы безопасности были независимы от систем более низкого класса безопасности.

4.18. Следует обеспечить, чтобы резервированные отдельные группы в составе систем безопасности были независимы друг от друга в той степени, в какой это необходимо для обеспечения того, чтобы все функции безопасности могли выполняться, когда это требуется. При необходимости коммуникации между резервированными отдельными группами, например, для выполнения голосования или активации частичного останова, следует предусматривать достаточные меры для обеспечения электрического или физического разделения, а также независимости коммуникации. Коммуникация для голосования способна ограничить ложное срабатывание из-за случайного отказа, которое может поставить безопасность под угрозу.

4.19. Следует обеспечить, чтобы операторские интерфейсы не блокировали одновременно функцию безопасности более чем одной резервированной отдельной группы.

4.20. Рабочая станция управления безопасностью позволяет контролировать работу единицы оборудования системы безопасности, находящейся за пределами своей отдельной группы, посредством использования приоритетной функции, соответствующей рекомендациям пункта 6.55.

4.21. Управление системами безопасности или ее компонентами также можно осуществлять с помощью операторских средств управления, относящихся к более низкому классу безопасности, только если требования системы безопасности имеют приоритет в управлении работой устройства.

4.22. Информация от систем безопасности может быть представлена на рабочих станциях управления, относящихся к более низкому классу безопасности, при соблюдении требований, изложенных в пунктах 6.25–6.56.

4.23. Следует обеспечить, чтобы системы безопасности и ее компоненты были способны выполнять свои функции безопасности при воздействии на них аварийных условий или возникающих в случае внутренних и внешних опасностей условий, при которых необходимо их реагирование.

4.24. Следует обеспечить, чтобы отказ или ложное срабатывание средств поддержки системы безопасности СКУ не ставило под угрозу независимость друг от друга резервированных частей систем безопасности, целых систем безопасности и систем более низкого класса безопасности или независимость различных уровней применяемой на станции концепции глубокоэшелонированной защиты.

УЧЕТ ОТКАЗОВ ПО ОБЩЕЙ ПРИЧИНЕ

4.25. В требовании 24 публикации SSR-2/1 (Rev. 1) [1] указано:

> «При проектировании оборудования должна надлежащим образом учитываться потенциальная возможность отказов по общей причине узлов, важных для безопасности, с тем чтобы определить, каким образом следует применять принципы неодинаковости, резервирования, физического разделения и функциональной независимости для достижения требующейся надежности».

4.26. Глоссарий МАГАТЭ по вопросам безопасности [6] определяет «отказ по общей причине» как «Отказ двух или более конструкций, систем и элементов вследствие единичного события или единичной причины».

4.27. Отказ по общей причине может произойти вследствие человеческих ошибок, ошибок в разработке или изготовлении, ошибок в обслуживании, ошибок в программных инструментах, используемых в процессе разработки, из-за распространения отказов между системами или компонентами или вследствие ненадлежащей спецификации, квалификации внутренних или внешних опасностей либо защиты от них.

4.28. В общей архитектуре СКУ следует определить архитектурные концепции, которые должны применяться в целях обеспечения максимально возможной степени независимости уровней глубокоэшелонированной защиты.

4.29. СКУ следует проектировать с защитой от отказа по общей причине в пределах одной системы и между системами в целях обеспечения независимости уровней глубокоэшелонированной защиты на станции. Для достижения этой цели следует тщательно разработать схему распределения функций между различными системами и системными элементами, обеспечить должные уровни независимости систем и определить методы обеспечения защиты от отказов по общей причине в рамках систем безопасности.

4.30. Следует оценить, насколько отказ по общей причине в общей структуре СКУ потенциально способен привести к нарушению одной или нескольких фундаментальных функций безопасности.

4.31. Для любых выявленных отказов по общей причине, не учтенных в данной оценке, следует представить соответствующее обоснование.

4.32. В рамках анализа безопасности следует провести анализ последствий каждого постулируемого исходного события, которое может произойти в сочетании с отказами по общей причине, приводящими к тому, что система защиты будет не способна выполнять требующиеся функции безопасности.

4.33. Анализ концепций глубокоэшелонированной защиты и неодинаковости является одним из методов проведения анализа, описываемого в пункте 4.32. См. пункт 2.81.

4.34. Если в результате анализа, описанного в пункте 4.32, будет определено, что постулируемое исходное событие в сочетании с отказом по общей причине защитной системы ведет к неприемлемым последствиям, в проект следует внести соответствующие изменения.

4.35. Полное устранение всех уязвимостей в СКУ и архитектуре этих систем к отказам по общей причине обеспечить невозможно, и поэтому следует подготовить обоснование принятия выявленных уязвимостей.

Неодинаковость

4.36. Глоссарий МАГАТЭ по вопросам безопасности [6] определяет «неодинаковость» как «Наличие двух или более резервных систем или элементов для выполнения одной определенной функции, при котором разные системы или элементы наделяются различными признаками таким образом, чтобы уменьшалась возможность отказа по общей причине, включая общий отказ».

4.37. Применение принципа неодинаковости (диверсности) — это способ снижения подверженности отказам по общей причине вследствие ошибок в требованиях, проектировании, изготовлении или обслуживании, а также проявления консерватизма в целях решения проблемы подтверждения нормированного уровня надежности.

4.38. Если признается, что применение принципа неодинаковости позволяет смягчить последствия отказа по общей причине защитной системы, следует подготовить обоснование, подтверждающее, что меры по обеспечению неодинаковости действительно смягчают последствия рассматриваемого отказа по общей причине.

4.39. При использовании неодинаковых СКУ следует обеспечить, чтобы эти неодинаковые (диверсные) системы не могли подвергаться воздействию одинаковых ошибок в спецификации, проектировании, изготовлении или обслуживании.

4.40. При проведении вероятностных исследований[21] важные для безопасности узлы СКУ не следует рассматривать как полностью независимые[22], если не достигнут требуемый уровень их неодинаковости и если они не приведены в соответствие с требованиями в отношении функциональной независимости, гальванической развязки, независимости средств коммуникации, квалификации по условиям окружающей среды, сейсмической квалификации, квалификации по электромагнитной совместимости, физического разделения и защиты от внутренних событий в соответствии с настоящим Руководством по безопасности.

5. КЛАССИФИКАЦИЯ БЕЗОПАСНОСТИ ДЛЯ ФУНКЦИЙ, СИСТЕМ И ОБОРУДОВАНИЯ КОНТРОЛЯ И УПРАВЛЕНИЯ

5.1. В требовании 18 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Инженерно-технические правила проектирования узлов АЭС, важных для безопасности, должны быть конкретно указаны и должны согласовываться с соответствующими национальными и международными сводами положений и нормами, а также апробированной инженерно-технической практикой при надлежащем учете их значимости для ядерно-энергетических технологий».

5.2. В требовании 22 публикации SSR-2/1 (Rev. 1) [1] указано: «Все узлы, важные для безопасности, должны быть определены и классифицированы на основе их функции и их значимости с точки зрения безопасности».

---

[21] Вероятностные исследования включают, например, анализ надежности и вероятностную оценку безопасности.

[22] Системы в вероятностных исследованиях признаются полностью независимыми на основании простого вычисления произведения отдельных вероятностей отказа.

5.3. Пункт 5.34 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Метод классификации узлов, важных для безопасности, на основе их значимости с точки зрения безопасности прежде всего должен быть основан на детерминистических методах, дополненных при необходимости вероятностными методами, с учетом таких факторов, как:
> a) функция(и) безопасности, которую(ые) выполняет данный узел;
> b) последствия отказа выполнять функцию безопасности;
> c) частота, с которой от данного узла потребуется выполнение функции безопасности;
> d) время после постулируемого исходного события или период, в течение которого от узла потребуется выполнение функции безопасности».

5.4. Пункт 5.36 публикации SSR-2/1 (Rev. 1) [1] гласит: «Оборудование, выполняющее несколько функций, должно быть отнесено к классу безопасности, который соответствует наиболее важной функции, выполняемой этим оборудованием».

5.5. В публикации Серии норм безопасности МАГАТЭ, № SSG-30, «Safety Classification of Structures, Systems and Components in Nulear Power Plants» («Классификация безопасности конструкций, систем и элементов атомной электростанции») [17] изложены рекомендации и приводится руководящий материал в отношении того, как обеспечить соответствие требованиям, установленным в публикациях SSG-2/1 (Rev. 1) [1] и GSR Part 4 (Rev. 1) [5], к определению конструкций, систем и элементов, важных для безопасности, и к их классификации на основании их функций и степени важности для безопасности.

5.6. Процесс классификации безопасности, рекомендуемый в публикации SSG-30 [17], соответствует концепции глубокоэшелонированной защиты, определенной в публикации SSR-2/1 (Rev. 1) [1]. В этом процессе рассматриваются функции, реализуемые на различных уровнях глубокоэшелонированной защиты.

5.7. Следует обеспечить, чтобы в процессе классификации для конкретной атомной электростанции были учтены:

— проектная основа станции и внутренне присущие ей характеристики безопасности;

— список постулированных исходных событий, согласно требованию 16 публикации SSR-2/1 (Rev. 1) [1]. Следует учитывать частоту возникновения постулированных исходных событий, предусмотренную в проектной основе станции.

5.8. При составлении перечня постулированных исходных событий следует учитывать вероятность того, что отказ или ложное срабатывание узла, важного для безопасности, может непосредственно привести к возникновению постулируемого исходного события, или вероятность того, что отказ при запросе на выполнение функции узла, важного для безопасности, может ухудшить последствия постулируемого исходного события.

5.9. Следует определить все функции СКУ и предусмотренные в проекте меры, необходимые для обеспечения выполнения основных функций безопасности, как указано в требовании 4 публикации SSR-2/1 (Rev. 1) [1], при различных состояниях станции, включая все режимы нормальной эксплуатации.

5.10. Все функции СКУ следует распределить по категориям на основании их важности для безопасности, с учетом следующих трех факторов:

a) последствий отказа выполнять свою функцию;
b) частоты возникновения постулируемого исходного события, при котором потребуется выполнение данной функции;
c) времени после возникновения постулируемого исходного события, по истечении или в течение которого данная функция должна быть выполнена.

5.11. Следует идентифицировать и классифицировать СКУ и их компоненты, выполняющие каждую функцию, отнесенную к категории безопасности. Классификацию следует проводить главным образом на основании категории, которая присваивается выполняемой ими функции.

5.12. При присвоении класса безопасности следует учитывать своевременность и надежность, с которой могут выполняться альтернативные действия, а также своевременность и надежность, с которой отказ в СКУ может быть обнаружен и устранен.

5.13. В публикации SSG-30 [17] на основе опыта государств-членов рекомендованы три категории безопасности для функций и три класса безопасности для конструкций, систем и элементов. Вместе с тем допустимо применение большего или меньшего числа категорий и классов при условии, что они согласуются с рекомендациями, изложенными в пунктах 2.12 и 2.15 публикации SSG-30 [17].

6. ОБЩИЕ РЕКОМЕНДАЦИИ ДЛЯ ВСЕХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ

ОБЩИЕ ПОЛОЖЕНИЯ

6.1. Следует обеспечить, чтобы системы СКУ в полной мере соответствовали требованиям их проектной основы.

6.2. При проектировании систем безопасности СКУ следует избегать излишней сложности.

6.3. Следует обеспечить, чтобы все средства, применяемые в системах безопасности СКУ, способствовали выполнению присвоенных им функций безопасности.

6.4. Следует обеспечить, чтобы усложнение конструкции систем безопасности СКУ не приводило к нарушению других принципов проектирования (например, принципов независимости, резервирования или неодинаковости).

6.5. Отказ от усложнения преследует цель добиться максимально возможной простоты конструкции СКУ, которая одновременно должна полностью соответствовать требованиями безопасности. Примерами усложнения, которого следует избегать, являются: включение функций, не содействующих выполнению функций безопасности СКУ или не способствующих повышению уровня надежности; применение проектных решений и средств реализации, которые не поддаются анализу и верификации в достаточной степени; применение платформ для реализации, которые являются слишком сложными и не способствуют надлежащему подтверждению уровня безопасности. Таким образом,

следует обеспечить, чтобы создаваемая архитектура имела простую схему взаимодействия и простые средства коммуникации. Одной из эффективных мер, помогающих избежать ненужного усложнения, является тщательное ведение документации и проведение пересмотра обоснования каждого требования.

ПРОЕКТИРОВАНИЕ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ

6.6. В требовании 23 публикации SSR-2/1 (Rev. 1) [1] указано: «Надежность узлов, важных для безопасности, должна соответствовать их значимости с точки зрения безопасности».

6.7. В требовании 62 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Системы контроля и управления для узлов АЭС, важных для безопасности, должны проектироваться с таким расчетом, чтобы они обеспечивали высокую функциональную надежность и возможность проведения периодических проверок и испытаний (тестопригодность) в соответствии с выполняемой(ыми) ими функцией(ями) безопасности».

6.8. Пункт 6.34 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Для предотвращения утраты функции безопасности должны использоваться в той мере, в какой это практически возможно, такие проектные решения, как обеспечение возможности проведения проверок и испытаний (тестопригодность), включая в соответствующих случаях самопроверку, отказобезопасные характеристики, функциональная неодинаковость и неодинаковость конструкции и принципов действия элементов».

6.9. При проектировании СКУ примеры мер, обеспечивающих функциональную надежность системы, включают: способность справляться с внезапным отказом системы, обеспечение независимости между оборудованием и системами, резервирование, неодинаковость (диверсность), переносимость отказов по общей причине, тестопригодность и ремонтопригодность, отказобезопасное проектирование и подбор высококачественного оборудования.

Критерий единичного отказа

6.10. В требовании 25 публикации SSR-2/1 (Rev. 1) [1] указано: «Критерий единичного отказа должен применяться к каждой группе безопасности, включаемой в проект станции».

6.11. Пункт 5.39 публикации SSR-2/1 (Rev. 1) [1] гласит: «При применении критерия единичного отказа [сноска опущена] к группе безопасности или системе безопасности ложное срабатывание должно рассматриваться как один из видов отказа».

6.12. Для достижения соблюдения критерия единичного отказа, как правило, применяются такие концепции, как резервирование, независимость, тестопригодность, постоянный мониторинг, квалификация по условиям окружающей среды и ремонтопригодность.

6.13. Следует обеспечить, чтобы каждая группа безопасности выполняла все действия, требуемые при реагировании на постулируемое исходное событие при появлении любого единичного обнаруживаемого отказа в системе безопасности в сочетании с:

— любыми не поддающимися обнаружению отказами, т.е. отказами, которые не могут быть выявлены при проведении периодических испытаний, поступлении предупредительного сигнала или появлении аномальной индикации;
— любыми отказами, вызванными единичным обнаруживаемым отказом и не поддающимися обнаружению отказами;
— любыми отказами и ложными срабатываниями системы, которые способны вызвать постулируемое исходное событие или вызваны постулируемым исходным событием, могущим повлиять на функционирование группы безопасности;
— выводом системы безопасности из эксплуатации или байпасированием части системы безопасности для проведения испытаний или работ по техническому обслуживанию в рамках допустимых эксплуатационных пределов и условий станции.

6.14. Отказы вследствие ошибок в проектировании, обслуживании, эксплуатации или изготовлении не включаются в анализ соблюдения критерия единичного отказа. Следует обеспечить, чтобы известные ошибки устранялись надлежащим образом посредством системы менеджмента. Последствия неизвестных ошибок прогнозировать невозможно, и поэтому

критерий единичного отказа оказывается бесполезным инструментом в выработке понимания последствий таких ошибок для группы безопасности. Анализ, проводимый с целью оценки потенциальных последствий отказа по общей причине вследствие таких ошибок, описан в разделе 4.

6.15. Следует обеспечить, чтобы несоблюдение критерия единичного отказа было допустимо только в исключительных случаях, определено в проектной документации и четко обосновано в анализе безопасности.

6.16. В ходе проведении анализа низкочастотных событий, таких как внешние опасности, необходимо соблюдать предельную осторожность при обосновании несоблюдения критерия единичного отказа. Особое внимание следует уделить обеспечению долгосрочной эксплуатационной готовности электрических систем и других систем поддержки, необходимых для эксплуатации и мониторинга систем безопасности.

6.17. Анализ надежности, вероятностная оценка, учет опыта эксплуатации, инженерная оценка или сочетание этих методов могут быть использованы для обоснования исключения конкретного отказа из рассмотрения при применении критерия единичного отказа.

6.18. Следует обеспечить, чтобы при проведении обслуживания, ремонта и испытаний соблюдались эксплуатационные пределы и условия на станции даже в ситуациях, когда критерий единичного отказа не соблюдается.

6.19. Если соблюдения критерия единичного отказа недостаточно для выполнения требований к надежности, то в целях обеспечения выполнения требований, предъявляемых к надежности, в рамках системы следует предусмотреть дополнительные проектные решения или внести изменения в проект.

Резервирование

6.20. Следует обеспечить резервирование СКУ в объеме, необходимом для обеспечения соответствия требованиям к надежности СКУ и соблюдения критерия единичного отказа.

6.21. Применительно к СКУ резервирование, как правило, применяется для достижение целей обеспечения надежности в системах, включая соблюдение критерия единичного отказа. Резервирование не может быть полностью эффективной мерой, если не обеспечена независимость

резервированных элементов. В целом резервирование повышает уровень надежности, однако оно также повышает вероятность возникновения ложного срабатывания. Для достижения баланса между надежностью и отсутствием ложного срабатывания обычно применяется схема совпадений сигналов резервирования («логика голосования») либо схема отклонения ложных сигналов.

Независимость

6.22. В требовании 21 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Должно предотвращаться взаимовлияние систем безопасности или резервных элементов системы такими средствами, как физическое разделение, электрическая изоляция (гальваническая развязка), функциональная независимость и независимость связи (передачи данных), по мере целесообразности».

6.23. Пункт 5.35 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Проектирование должно проводиться таким образом, чтобы предотвращалось любое взаимодействие между узлами, важными для безопасности, и, в частности, чтобы любой отказ узлов, важных для безопасности, в системе, относящейся к более низкому классу безопасности, не распространялся на систему, относящуюся к более высокому классу безопасности».

6.24. В Глоссарии МАГАТЭ по вопросам безопасности [6] независимое оборудование определяется как

> «Оборудование, которое обладает двумя следующими характеристиками:
> a) способность выполнять требующуюся функцию не зависит от работы или отказа другого оборудования;
> b) способность выполнять предназначенную функцию не зависит от эффектов, возникающих в результате постулируемого исходного события, при наступлении которого оно должно функционировать».

6.25. Независимость обеспечивается в целях предотвращения влияния отказа, внутренней опасности или внешней опасности на резервируемые элементы систем безопасности. Она также предусматривается

для предотвращения влияния отказа или опасности на системы, обеспечивающие разные уровни глубокоэшелонированной защиты. К процессам возникновения отказов, которые следует учитывать, относятся: отказы вследствие проектных аварий, воздействие одних и тех же опасностей, нарушение электрических соединений между системами или резервированными отдельными группами, обмена данными межу системами или резервированными отдельными группами, а также вследствие общих ошибок в проектировании, изготовлении, эксплуатации или обслуживании.

6.26. Средства обеспечения независимости включают: физическое разделение, гальваническую развязку, функциональную независимость и независимость от воздействия ошибок связи (см. раздел 7). Квалификация оборудования и неодинаковость могут также способствовать обеспечению независимости. Этим вопросам посвящен нижеследующие пункты данного раздела (пункты 6.77–6.134). Как правило, для обеспечения независимости следует применять сочетание указанных мер.

6.27. Следует обеспечить, чтобы изолирующие устройства, использующиеся между системами разных классов безопасности, были частью системы более высокого уровня безопасности.

6.28. Средства, обеспечивающие изоляцию от различных физических воздействий, повреждений в электрической цепи и ошибок связи, не должны обязательно быть встроены в защищаемое устройство. Средства изоляции систем от различного вида угроз не должны обязательно располагаться в одном и том же физическом устройстве или на одном и том же участке цепи. Функции изоляции от одного воздействия могут распространяться на несколько устройств. Например, изоляция от ошибок в передаче данных может обеспечиваться буферной памятью, предотвращающей прямую передачу записанных данных от одной группы к другой, проверкой валидности, осуществляемой процессором на другом устройстве, в целях недопустимости прочтения данных из буфера до тех пор, пока они не будут соответствовать критериям валидности, корректности и аутентичности.

6.29. Следует обосновывать адекватность проектных решений, обеспечивающих соответствие требованиям в отношении независимости.

Физическое разделение

6.30. Цели применения физического разделения состоят в следующем:

— физическое разделение защищает от отказа по общей причине, возникающего вследствие воздействия внутренних опасностей. К внутренним опасностям, подлежащим учету, относятся возгорание, летящие предметы, струи пара, биение трубопроводов, химические взрывы, затопления и отказ смежного оборудования;
— физическое разделение может служить способом защиты от отказа по общей причине в нормальных, нештатных или аварийных условиях, от воздействия аварий (включая все проектные аварии) или от воздействия внутренних или внешних опасностей[23];
— физическое разделение может снижать вероятность возникновения отказа по общей причине в результате воздействия внешних событий с локализованными последствиями (например, авиакатастрофы. торнадо, цунами);
— физическое разделение снижает вероятность неизбежных ошибок во время эксплуатации или обслуживания резервированного оборудования.

6.31. Следует обеспечить, чтобы компонентные единицы, являющиеся частью систем безопасности, были физически отделены от единиц систем более низкого класса безопасности.

6.32. Следует обеспечить, чтобы резервированные части групп безопасности были физически разделены.

6.33. Полное физическое разделение резервированных единиц может быть практически неосуществимым, если датчики или исполнительные устройства расположены близко друг к другу, как, например, в случае приводов регулирующих стержней или внутрикорпусных контрольно-измерительных приборов.

---

[23] Примеры включают обеспечение пространства для ослабления воздействия электромагнитных помех и разделения между системами и компонентами, квалифицированными на разном уровне. Квалификация по условиям окружающей среды, сейсмическая квалификация и квалификация по электромагнитной совместимости могут проводится как в своем качестве, так и в сочетании с физическим разделением в целях защиты от воздействия аварий, внутренних опасностей или внешних опасностей.

6.34. Некоторые места, которые могут создавать осложнения в силу сближения оборудования или проводов, включают:

— герметичные проходки в защитной оболочке;
— шкафы управления электродвигателями;
— зоны размещения распределительных устройств;
— помещения для разводки кабелей;
— аппаратные;
— помещение главного щита управления и другие пункты управления;
— компьютер для управления технологическими процессами на станции.

6.35. В случае невозможности обеспечения надлежащего полного физического разделения следует предусмотреть максимально возможное разделение и обосновать исключения (см. пункт 6.43).

6.36. Физическое разделение достигается за счет расстояния, применения барьеров или сочетания этих двух способов.

6.37. В публикациях Серии норм безопасности МАГАТЭ, № NS-G-1.7, «Защита от внутренних пожаров и взрывов при проектировании атомных электростанций» [20] и, № NS-G-1.11, «Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants» («Защита от внутренних опасностей за исключением пожаров и взрывов при проектировании атомных электростанций») [21] изложен дополнительный руководящий материал по защите от пожаров и других внутренних опасностей.

Гальваническая развязка

6.38. Гальваническая развязка (электрическая изоляция) используется для предотвращения воздействия электрических отказов в одной системе на связанные с ней системы или на резервированные элементы в рамках данной системы.

6.39. Следует обеспечить, чтобы системы безопасности и их компоненты были гальванически изолированы от систем и компонентов более низкого класса безопасности.

6.40. Следует обеспечить, чтобы резервируемые части групп безопасности были гальванически изолированы друг от друга.

6.41. Следует обеспечить, чтобы устройства для гальванической развязки предотвращали отрицательное воздействие максимально допустимого напряжения или нестационарных токов, заземления, разомкнутых цепей и цепей короткого замыкания на одной стороне устройства на функционирование присоединенных схем безопасности.

6.42. Примеры обеспечения гальванической развязки включают: исключение электронных соединений, применение электронных устройств, обеспечивающих развязку, устройств оптической развязки (включая оптоволокно), реле, пространственного разноса и внутренних механических структур, или сочетание этих мер.

Связанные контуры

6.43. Если обеспечение физического разделения или гальванической развязки между контуром безопасности и контуром более низкого класса безопасности не может быть практически реализовано, следует обеспечить, чтобы контур более низкого класса безопасности (именуемый здесь «связанным контуром»):

— подвергался анализу или испытаниям для демонстрации того, что данная связь отрицательно не влияет на контуры безопасности, с которыми он связан[24];
— был определен в качестве части отдельной группы безопасности, с которой он связан;
— был физически отделен от других компонентов в той же степени, в какой физически отделены контуры отдельной группы безопасности, с которой он связан.

Функциональная независимость

6.44. Функциональная независимость — это состояние, при котором успешное выполнение системой требуемы функций не зависит от разных алгоритмов поведения, включая отказы или нормальное функционирование, другой системы, или от получения сигналов, данных или информации от другой системы. Функциональная независимость является средством

[24] Например, анализ или испытания могут включать рассмотрение максимального напряжения в связанном контуре в сравнении с напряжениями, которые способен выдерживать контур безопасности.

обеспечения изоляции одной системы от другой. Функциональная независимость может также использоваться в качестве средства обеспечения изоляции между резервированными единицами оборудования.

6.45. Функциональная независимость дополнительно обеспечивается посредством проектирования архитектуры и тщательной обработки данных, являющихся общими для реализуемых функций. Вопросам архитектуры посвящен раздел 4. Рекомендации по совместно используемым данным приводятся ниже.

6.46. Следует обеспечить, чтобы вводы от СКУ, относящихся к более низкому классу безопасности, негативно не влияли на способность систем безопасности осуществлять предписанные им функции безопасности.

6.47. Системы безопасности, однако, могут зависеть от входных сигналов, поступающих от систем обслуживания, которые не относятся ни к одному из классов безопасности, например, систем для проведения технического обслуживания, обновления программного обеспечения, тестирования или установки конфигурационных данных. Такие вводы, как правило, осуществляются, когда соответствующая отдельная группа оборудования переведена в автономный режим (режим офлайн), при этом по окончании ввода данных проводится верификации.

6.48. Системы мониторинга более низкого класса безопасности могут быть соединены с системами безопасности, если установлено, что системы мониторинга не мешают работе систем безопасности. При необходимости соединения систем безопасности с системами обслуживания более низкого класса безопасности — это соединение следует выполнять только в условиях, когда соответствующая отдельная группа или канал находится в автономном режиме (режиме офлайн), использование данных, полученных от системы обслуживания, ограничено конкретной целью и соединение системы обслуживания выполнено в соответствии с программой обеспечения компьютерной безопасности.

6.49. В случаях, когда проведение обслуживания допускается на уровне канала, следует обеспечить достаточную изоляцию между каналами, которые являются общими для одной отдельной группа.

6.50. Следует определить режимы работы станции, при которых система обслуживания может быть подключена.

6.51. Следует обеспечить, чтобы передача данных между системами безопасности и системами более никого класса безопасности была организована так, чтобы никакие вероятные отказы в системах более низкого класса безопасности не могли помешать выполнению функций безопасности подключенной системой безопасности.

6.52. Передачу данных между резервированными элементами группы безопасности следует организовывать так, чтобы ни один их возможных отказов отправляющего элемента не мог негативно повлиять на соответствие присоединенных элементов предъявляемым к ним требованиям.

6.53. В компьютерных системах однонаправленная широковещательная коммуникация данных часто используется, когда компьютерные системы более высокого класса безопасности передают данные системам более низкого класса безопасности. Характеристики аппаратного обеспечения, определяющие действие средств однонаправленной передачи, следует рассматривать в качестве средства обеспечения такой однонаправленной передачи, например, это может быть использование канала, соединенного только с передающим устройством в системе более высокого класса безопасности и только с приемным устройством в системе более низкого класса безопасности.

6.54. В случаях, когда это обосновано, сигналы могут направляться от систем более низкого класса безопасности к системам более высокого класса безопасности по отдельным линиям аналоговых или двоичных сигналов при условии, что:

— соблюдаются рекомендации, изложенные в пункте 6.51;
— потенциальная вероятность отказов системы более низкого класса безопасности, способной вызвать ложное срабатывание классифицированных по безопасности компонентов, оценена и является приемлемой.

6.55. Следует обеспечить, чтобы в случае, если исполнительные устройства систем безопасности действуют на основании информации, полученной от других систем, включая системы более низкого класса безопасности, принимались меры для обеспечения того, чтобы некорректные данные, полученные от других систем, не препятствовали выполнению функций безопасности. Как правило, это достигается посредством использования логики приоритетности, которая расставляет данные и командные сигналы системы безопасности в порядке их приоритетности.

6.56. Пункты 7.52–7.59 содержат дополнительные рекомендации относительно случаев, когда для систем защиты и управления используются общие входные сигналы.

Неодинаковость (диверсность)

6.57. В связи с подтверждением надежности компьютерных систем или систем, в которых используются сложные аппаратные функции, сложная аппаратная логика или сложные электронные компоненты, могут возникнуть трудности. Если не представляется возможным обеспечить надлежащее подтверждение надежности функции, выполняемой СКУ, для повышения уверенности в выполнении фундаментальных функций безопасности в СКУ может быть применено неодинаковое оборудование. Типы предусматриваемой неодинаковости существенно различаются в разных государствах.

6.58. Следует обосновать решение об использовании или неиспользовании принципа неодинаковости применительно к выполнению фундаментальных функций безопасности в условиях проектной аварии.

6.59. Если неодинаковость используется для решения проблемы потенциального возникновения отказа по общей причине, следует рассмотреть применение более одного типа неодинаковости.

6.60. Примеры различных типов неодинаковости (диверсности) включают:

— неодинаковость проектных решений: достигается посредством использования различных проектных подходов к решению одной и той же проблемы или похожих проблем;
— неодинаковость сигналов: достигается посредством использования систем, в которых действия по обеспечению безопасности могут быть инициированы на основании значения различных параметров станции;
— неодинаковость оборудования: достигается посредством использования аппаратных средств, основанных на применении другой технологии (например, аналогового оборудования против цифрового оборудования, твердотельного оборудования против электромагнитного оборудования или компьютеризированного оборудование против оборудования, работающего на программируемых пользователем вентильных матрицах);

— функциональную неодинаковость: достигается системами, совершающими разные действия для достижения одинакового результата в обеспечении безопасности;
— неодинаковость в процессах разработки: достигается привлечением разных проектных организаций, разных управленческих групп и групп разработчиков, а также разных групп по реализации проекта и проведению испытаний;
— неодинаковость логики: достигается использованием разных языков описания программных или аппаратных средств, разных алгоритмов, разных характеристик синхронизации логических функций и разной последовательности осуществления логических функций.

6.61. При использовании принципа неодинаковости следует представить подтверждение, что выбор используемых типов неодинаковости обеспечивает достижение заявленного уровня смягчения последствий отказа по общей причине.

6.62. Не всегда необходимо применять принцип неодинаковости в разных системах. Например, функциональная неодинаковость и неодинаковость сигналов могут применяться в рамках одной системы.

6.63. Меры по обеспечению неодинаковости также включают предотвращение образования областей потенциальной общности в применении принципа неодинаковости, таких как аналогичные материалы, аналогичные компоненты, аналогичные процессы изготовления, одинаковая логика, тонкое сходство принципов эксплуатации или общие устройства поддержки. Например, разные производители могут использовать один и тот же тип процессора или одну и ту же лицензионную операционную систему, тем самым создавая потенциальную возможность возникновения отказа по общей причине. Недостаточным является обоснование реализации принципа неодинаковости, построенное на перечислении разных изготовителей или номеров модели, которые изготовитель присваивает изделиям, без учета такой возможности.

Виды отказов

6.64. В требовании 26 публикации SSR-2/1 (Rev. 1) [1] указано: «Принцип отказобезопасного проектирования в надлежащих случаях должен применяться при проектировании систем и элементов, важных для безопасности».

6.65. Следует обеспечить, чтобы сбой в питании любого из компонентов СКУ или отказ любого из компонентов СКУ при любом из известных и задокументированных видов отказа переводил систему в заданный режим, который был подтверждаемо признан приемлемым с точки зрения обеспечения безопасности.

6.66. Методы обеспечения перевода системы в безопасный режим в случае отказов включают такое проектное решение, при котором системы переходят в безопасный режим в условиях отключения питания, или использование контрольного («сторожевого») таймера, обеспечивающего выявление состояния, при котором оборудование прекратило выполнять свою проектную функцию, и перевод системы в безопасный режим.

6.67. В случае такой практики при применении рекомендаций, изложенных в пункте 6.65, следует учитывать возможность отказа самих средств обеспечения отказобезопасности, предусмотренных в проекте.

6.68. Следует выявлять и документировать несистемные виды отказов компонентов СКУ и самих систем.

6.69. Знание видов отказов компонентов важно при применении принципа отказобезопасности к системе. Это также важно при подтверждении того, что отказы системы контроля не приводят к возникновению событий, выходящих за границы анализа безопасности.

6.70. Отказы, которые могут возникнуть вследствие ошибок в программном обеспечении, прогнозировать сложно. С другой стороны, не обязательно знать как происходят отказы программного обеспечения для определения возможных состояний отказа, отображающихся на терминалах устройств. Одно из решений заключается в выявлении и группировании возможных видов отказов в управляемый набор вероятностей (например, неверные выходные данные, выходные данные с задержкой, «замороженные» выходные данные).

6.71. Виды отказов, которые с наибольшей вероятностью возникают в силу системных факторов в проектирования аппаратного или программного обеспечения, практически не предсказуемы. Вследствие этого принцип отказобезопасного проектирования неэффективен применительно к принятию мер в отношении отказов, возникающих по таким причинам. Строго организуемые процессы разработки (см. раздел 2), анализ опасностей (пункты 2.56–2.65), применение принципа глубокоэшелонированной

защиты (см. раздел 4) и применение принципа неодинаковости (см. пункты 6.57–6.63) являются наиболее действенными средствами сокращения числа таких факторов и предотвращения воздействия таких сохраняющихся факторов.

6.72. Следует обеспечить, чтобы отказы компонентов СКУ выявлялись посредством проведения периодических испытаний или самодиагностики или самообнаруживались с подачей предупредительного сигнала или индикацией отклонения.

6.73. Предпочтительно, чтобы отказы были самообнаруживаемыми. Следует обеспечить, чтобы действие механизма самообнаруживаемости не приводило систему к небезопасному состоянию или ложному срабатыванию систем безопасности.

6.74. Любые идентифицированные отказы, которые не могут быть выявлены посредством проведения периодических испытаний, в результате поступления предупредительного сигнала или индикации отклонения, следует считать как возникшие в сочетании с единичными отказами при оценке соблюдения критерия единичного отказа. Следует обеспечить, чтобы определялись и выявлялись отказы самих средств самотестирования, самодиагностики или самооповещения.

6.75. Следует обеспечить, чтобы отказ компонента, насколько это практически возможно, не приводил к ложному срабатывания любой из систем безопасности.

6.76. При перезапуске или восстановлении подачи питания к системам или компонентам СКУ следует обеспечить, чтобы выходные сигналы инициализировались в предопределенном безопасном состоянии, за исключением случаев реагирования на достоверные аварийные сигналы.

КВАЛИФИКАЦИЯ ОБОРУДОВАНИЯ

6.77. В требовании 30 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Должна осуществляться программа аттестации (квалификации) оборудования для подтверждения того, что узлы АЭС, важные для безопасности, будут способны выполнять предписанные им функции в случае необходимости и в преобладающих условиях окружающей

среды в течение всего проектного срока службы этих узлов, при этом надлежащим образом должно быть учтено состояние станции при проведении технического обслуживания и испытаний».

6.78. Системы и компоненты СКУ следует квалифицировать на выполнение предписанных им функций в период их срока службы.

6.79. Следует обеспечить, чтобы квалификация компонентов СКУ охватывала программное обеспечение, аппаратные (технические) средства, язык описания аппаратных средств и интерфейсы процессов при их наличии.

6.80. Следует обеспечить, чтобы квалификация обеспечивала степень уверенности, соразмерную важности системы или компонента для безопасности.

6.81. В программу квалификации следует включать все аспекты, влияющую на пригодность каждой системы или компонента к выполнению предписанных им функций, включая:

— пригодность и корректность функций и эксплуатационных характеристик;
— квалификацию по условиям окружающей среды;
— квалификацию по воздействию внутренних и внешних опасностей;
— квалификацию по электромагнитной совместимости.

6.82. Следует обеспечить, чтобы квалификация оборудования базировалась на выборе следующих методов:

— использовании производственно-технологических процессов, соответствующих признанным стандартам;
— подтверждении надежности;
— использовании прошлого опыта, связанного с аналогичными применениями;
— типовых испытаниях;
— тестировании поставленного оборудования;
— анализе используемых для экстраполяции результатов испытаний или опыта эксплуатации в соответствующих условиях;
— оценке производственных процессов изготовителя;
— инспекции компонентов во время изготовления.

6.83. Как правило, в одновременном применении всех этих методов необходимости нет. Выбор определенного сочетания методов зависит от подлежащих квалификации систем или компонентов. Например, при квалификация уже существующих единиц больше внимания может уделяться имеющимся данным об опыте эксплуатации и результатам анализа, чтобы компенсировать отсутствие полностью задокументированных данных по верификации и валидации, получаемых в процессе проектирования и изготовления.

6.84. Выбор метода или комбинации методов квалификации оборудования следует обосновать.

6.85. Если для квалификации оборудования используется информация об опыте эксплуатации, следует подтвердить актуальность этого опыта применительно к предполагаемому использованию оборудования и окружающим условиям его целевого применения.

6.86. Основанные на опыте эксплуатации данные для подтверждении квалификации являются недостаточными в случае систем безопасности, и поэтому их следует использовать в сочетании с типовыми испытаниями и тестированием поставленного оборудования, а также оценкой производственных процессов, применяемых изготовителями, или инспекцией компонентов в процессе изготовления.

6.87. В анализ, используемый для подтверждения квалификации оборудования, следует включать обоснование применяемых методов, теорий и допущений.

6.88. Например, валидность математических моделей, используемых для квалификации оборудования, может быть подкреплена экспериментальными данными, данными тестирования или эксплуатационным опытом.

6.89. Следует обеспечить, чтобы в отношении каждой установленной системы и компонентов, важных для безопасности, а также применительно к соответствующим подтверждающим данным, используемым для квалификации, была обеспечена прослеживаемость.

6.90. Это включает прослеживаемость не только до компонентов, но также и прослеживаемость между квалифицированной конфигурацией и установленной конфигурацией.

Пригодность и корректность

6.91. Следует обеспечить, чтобы программа квалификации оборудования подтверждала, что процесс проектирования систем и компонентов СКУ соответствует всем функциональным требованиям, требованиям к эксплуатационным характеристикам и требованиям к надежности, включенным в проектную основу и спецификации оборудования систем и компонентов СКУ.

6.92. Примеры функциональных требований включают функциональность, требующуюся для данного применения, функциональность, требующуюся для поддержки работоспособности систем или оборудования, требования к операторскому интерфейсу и требования к диапазонам входов/выходов.

6.93. Примеры требований к эксплуатационным характеристикам включают требования по точности, разрешению, диапазону, частоте дискретизации и скорости реакции.

6.94. Примеры требований к надежности включают требования к минимальном среднему времени между отказами и требования по отказобезопасному поведению, независимости, выявлению отказов, тестопригодности, ремонтопригодности и сроку службы.

6.95. Следует обеспечить, чтобы программа квалификации оборудования подтверждала, что фактическое проектирование и фактическое исполнение СКУ («как построено»), а также установленные компоненты корректно реализованы в прошедшем квалификацию проекте.

Квалификация по условиям окружающей среды

6.96. В настоящем Руководстве по безопасности под квалификацией по условиям окружающей среды подразумевается квалификация по температурному режиму, влажности, химическому воздействию, радиационному воздействию, затоплению, электромагнитному воздействию и механизмам старения, влияющим на надлежащее функционирование компонентов в этих условиях.

6.97. Системы и компоненты следует проектировать так, чтобы они были способны выдерживать воздействие условий окружающей среды или были совместимыми с этими условиями, связанными с нормальной эксплуатацией, ожидаемыми при эксплуатации событиями и постулированными авариями, в которых они должны функционировать.

6.98. Следует продемонстрировать, чтобы компоненты отвечают всем требованиям при воздействии на них полного спектра указанных условий окружающей среды.

6.99. Подробная информация о требованиях к квалификации оборудования, процессов и методов представлена в публикации [22].

Компоненты, предназначенные для функционирования только в мягких окружающих условиях

6.100. Квалификация компонентов СКУ по условиям окружающей эксплуатационной среды, которые во время аварий никогда не могут быть значительно более жесткими, чем условия во время нормальной эксплуатации (так называемые «мягкие окружающие условия»), может основываться на четкой спецификации функциональных требований для конкретных условий окружающей среды, связанных с эксплуатационными состояниями станции, наряду с представлением поставщиками сертификата соответствия или проведением отдельной оценки того, что компоненты будут выполнять требуемые функции в указанных условиях окружающей среды.

Компоненты, предназначенные для функционирования в жестких окружающих условиях

6.101. Следует обеспечить, чтобы квалификация компонентов, которые должны функционировать в условиях окружающей среды, которые в любой момент времени являются значительно более тяжелыми, чем условия во время нормальной эксплуатации (так называемые «жесткие условия»), подтверждала, что компоненты в конце своего квалифицированного срока службы (аттестованного ресурса) способны выполнять предписанные им функции по обеспечению безопасности при воздействии всего спектра указанных условий эксплуатации.

6.102. При демонстрации способности компонентов функционировать, как это требуется, в конце своего квалифицированного срока службы, учитывается воздействие значительных факторов старения (например, старения в результате радиационного облучения и термического старения) в целях подтверждения требующейся функциональности в конце квалифицированного срока службы. Как правило, этот процесс также включает применение при необходимости дополнительных консервативных мер в целях компенсации воздействия непредвиденных механизмов старения.

6.103. В спецификации программы квалификации оборудования следует учитывать наихудшие вероятные сочетания условий эксплуатационной среды, включая синергетическое воздействие нескольких факторов, обусловленных разными эксплуатационными условиями.

6.104. При необходимости проведения раздельных испытаний на воздействие разных условий окружающей среды (например, раздельных испытаний на воздействие радиации и температуры), порядок проведения этих испытаний следует обосновывать как последовательность, стимулирующую деградацию, вызываемую сочетанием разных сред.

6.105. Применение наиболее строгих методов квалификации по условиям окружающей среды может требоваться только для компонентов с присвоенным классом безопасности.

6.106. При квалификации по условиям окружающей среды компонентов с присвоенным классом безопасности, которые должны функционировать в жестких окружающих условиях, следует выполнять типовые испытания.

6.107. В случае применения защитных барьеров для изоляции оборудования от возможных воздействий окружающей среды барьеры следует включать в программу квалификации для подтверждения их соответствия требованиям.

Внутренние и внешние опасности

6.108. Проектная основа станции и анализ безопасности станции позволяют установить внутренние и внешние опасности, такие как пожар, затопление и сейсмические явления, которые станция должна выдерживать при эксплуатации и которым станция должна безопасно противостоять, а также по которым требуется квалификация защита или системы.

Проектная основа станции и анализ безопасности станции позволяют также установить опасности, которые обусловлены системными причинами, такими как инженерно-технические решения или дефектность, и которые могут приводить к деградации функции безопасности; следует определить соответствующие системные ограничения с целью предотвращения деградации функции безопасности.

6.109. Следует обеспечить, чтобы СКУ и их компоненты были защищены от воздействия пожара или взрыва в соответствии с руководящим материалом, изложенным в публикации NS-G-1.7 [20].

6.110. Следует обеспечить, чтобы СКУ и их компоненты были защищены от воздействия внутренних опасностей в соответствии с руководящим материалом, изложенным в публикации NS-G-1.11 [21].

6.111. Следует обеспечить, чтобы СКУ и их компоненты были спроектированы и квалифицированы так, чтобы они выдерживали воздействие сейсмических опасностей, в соответствии с руководящим материалом, изложенным в публикации Серии норм безопасности МАГАТЭ, № NS-G-1.6, «Проектирование и аттестация сейсмостойких конструкций для атомных электростанций» [23].

6.112. Следует обеспечить, чтобы СКУ и их компоненты были защищены или спроектированы и квалифицированы так, чтобы они выдерживали воздействие внешних опасностей, в соответствии с руководящим материалом, изложенным в публикации Серии норм безопасности МАГАТЭ, № NS-G-1.5, «Учет внешних событий, исключая землетрясения, при проектировании атомных электростанций» [24].

Квалификация по электромагнитной совместимости

6.113. Электромагнитная совместимость — это способность системы или компонента удовлетворительно функционировать в окружающей их электромагнитной обстановке без наводки неприемлемых электромагнитных помех в любых предметах в этой среде. Подверженность компонентной единицы (узла) воздействию электромагнитных помех и вклад электромагнитных помех в электромагнитную обстановку (электромагнитная эмиссия) также входят в определение понятия электромагнитной совместимости.

6.114. К электромагнитным помехам также относятся радиопомехи, и, как указано в настоящем Руководстве по безопасности, они включают колебания напряжения, например, импульсные скачки напряжения вследствие переходных процессов при переключении.

6.115. Бесперебойная работа электрических и электронных систем и компонентов зависит от электромагнитной совместимости компонентов со своей эксплуатационной средой, т.е. от способности компонента противостоять помехам, создаваемым смежными или связанными с ним компонентами.

6.116. В число источников значительных электромагнитных помех входят: защита от токов короткого замыкания при срабатывании коммутационных устройств, автоматических выключателей или предохранителей; электрические поля, создаваемые радиопередатчиками; природные источники, такие как удар молнии или солнечные бури; другие внутренние или внешние источники антропогенного воздействия на станцию.

6.117. Квалификация по электромагнитной совместимости СКУ и их компонентов зависит от выбранного сочетания мер по проектирования систем и компонентов, применяемых для минимизации связи электромагнитных помех с компонентами СКУ, от испытаний, проводимых для подтверждения того, что компоненты могут противостоять ожидаемым уровням электромагнитного излучения, а также от испытаний, проводимых с целью подтверждения того, что уровни электромагнитного излучения находятся в допустимых пределах.

6.118. Методы минимизации образования и распространения электромагнитных помех, включают:

— подавление электромагнитных помех в источнике;
— отделение и изоляцию сигнальных кабелей СКУ от силовых кабелей;
— экранирование оборудования и кабелей от внешних источников магнитного и электромагнитного излучения;
— фильтрацию электромагнитных помех до их взаимодействия с чувствительными электрическими цепями;
— нейтрализацию или изоляцию электронного оборудования от изменений электрического потенциала Земли;
— надлежащее заземление электрического оборудования и оборудования СКУ, каналов для прокладки кабелей, щитов, шкафов, компонентов и кабельных экранов.

6.119. Надлежащая практика ведения работ по монтажу и техническому обслуживанию является необходимым условием для обеспечения должного применения и эффективности этих мер.

6.120. Следует установить детальные требования по электромагнитной совместимости для систем безопасности и их компонентов и подтвердить, что они соответствуют этим требованиям.

6.121. Международные нормы по электромагнитной совместимости для промышленного оборудования могут служить основой для установления требований при условии, что при необходимости в них будут включены дополнения, учитывающие особенности в обеспечении электромагнитной совместимости применительно к конкретной станции, в случае которой требуется применять более жесткие требования. Определение требований к электромагнитной совместимости включает учет возможности того, что компоненты СКУ будут подвергаться многократному воздействию переходных процессов (например, при отключении индуктивных нагрузок и вибрации реле) и высокоэнергетических скачков (например, при сбое в питании или в случае грозовых разрядов).

6.122. Обеспечение должной электромагнитной обстановки для компонентов СКУ на каждом энергоблоке атомной электростанции, как правило, включает проведение анализа для каждого энергоблока. Результаты анализа используются для оценки адекватности электромагнитной совместимости каждого компонента СКУ.

6.123. Оборудование и системы, важные для безопасности, включая связанные с ними кабели, следует проектировать и устанавливать так, чтобы они были устойчивы к электромагнитной обстановке, в которой они находятся.

6.124. К факторам воздействия электромагнитных помех, которые необходимо учитывать при проектировании систем и элементов СКУ, относятся:

— излучение электромагнитных помех и устойчивость к ним;
— излучение и передача электромагнитных помех через кабели;
— электростатические разряды;
— коммутационные переходные процессы и перенапряжения;

— излучение от беспроводных систем и устройств[25], используемых на станции, а также устройств, применяемых при ремонте, обслуживании и измерениях.

6.125. Вблизи чувствительного к воздействию помех оборудования следует создать исключительные зоны, в которых запрещено применение беспроводных устройств и других переносных источников электромагнитных помех.

6.126. Следует обеспечить, чтобы программа квалификации оборудования подтверждала, что компоненты СКУ с присвоенным классом безопасности способны выполнять предписанные им функции безопасности в условиях воздействия в пределах, ограничиваемых огибающей рабочего спектра электромагнитных помех, и способностью противостоять скачкам напряжения.

6.127. Применительно ко всему оборудованию станции следует установить пределы для эмиссионного и кондуктивного электромагнитного излучения.

6.128. Любое электрическое и электронное оборудование станции влияет на электромагнитную обстановку. Поэтому требование в отношении ограничения электромагнитного излучения следует применять ко всему оборудованию станции, а не только к оборудованию, классифицируемому как важное для безопасности.

6.129. Следует обеспечить, чтобы ограничения излучения, установленные для отдельных компонентов были такими, чтобы результирующее излучение в рабочей среде находилось в безопасных пределах огибающей поля электромагнитных помех каждого компонента при любых режимах или состояниях системы и компонентов, включая переходные процессы между режимами или состояниями и деградировавшие условия.

6.130. Следует обеспечить, чтобы программа квалификации оборудования подтверждала, что электромагнитное излучение всего оборудования на станции находилось в установленных пределах.

---

[25] Примерами беспроводных систем и устройств являются мобильные телефоны, радиостанции и беспроводные сети передачи данных.

6.131. Оборудование и системы, включая связанные с ними кабели и источники питания, следует проектировать и устанавливать таким образом, чтобы должным образом ограничивалось распространение (эмиссионным или кондуктивным путем) электромагнитных помех в местах расположения оборудования станции.

6.132. При подсоединении нескольких СКУ к одному источнику питания в квалификацию по электромагнитной совместимости следует включать оценку путей передачи электромагнитных помех.

6.133. Кабели контрольно-измерительных приборов следует скручивать парами и экранировать в целях минимизации электромагнитного и электростатического воздействия.

6.134. Публикация SSG-34 [7] содержит рекомендации по заземлению, побору и прокладке кабелей для снижения образования и распространения электромагнитных помех.

ПРОЕКТИРОВАНИЕ С УЧЕТОМ ПРОБЛЕМ СТАРЕНИЯ И УСТАРЕВАНИЯ

6.135. В требовании 31 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Должен быть рассчитан и указан проектный срок службы узлов АЭС, важных для безопасности. В целях обеспечения способности узлов, важных для безопасности, выполнять в течение всего проектного срока службы предписанные им функции безопасности при проектировании должны предусматриваться надлежащие запасы надежности с таким расчетом, чтобы надлежащим образом учитывались соответствующие механизмы старения, охрупчивания при нейтронном воздействии и износа, а также потенциального ухудшения характеристик вследствие старения».

6.136. Пункт 5.51 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «При проектировании АЭС должны надлежащим образом учитываться эффекты старения и износа во всех эксплуатационных состояниях, для которых предназначен тот или иной элемент, включая испытания, техническое обслуживание, простои вследствие технического

обслуживания, состояния станции при возникновении постулируемого исходного события и состояния станции после постулируемого исходного события».

6.137. Пункт 5.52 публикации SSR-2/1 (Rev. 1) [1] гласит:

«Должны предусматриваться меры для осуществления контроля, испытаний, отбора проб и инспектирования в целях оценки механизмов старения, прогнозируемых на стадии проектирования, и содействия определению непредвиденного поведения станции или ухудшения характеристик, которые могут проявиться во время эксплуатации».

6.138. Квалифицированный (аттестованный) срок службы электрических и электронных систем и компонентов может быть значительно меньше срока службы станции.

6.139. Деградация вследствие старения, ухудшающая способность компонента функционировать в тяжелых окружающих условиях, может возникнуть прежде, чем функциональные способности компонента, работающего в нормальном режиме, подвергнутся воздействию.

6.140. В процессе проектирования следует определить механизмы старения, способные значительно повлиять на компоненты СКУ и средства отслеживания последствий воздействия этих механизмов.

6.141. Процесс определения потенциального воздействия старения включает, прежде всего, понимание механизма соответствующего явления старения применительно к различным компонентам СКУ.

6.142. Старение компонентов СКУ происходит преимущественно вследствие воздействия тепла или излучения. Вместе с тем при применении рекомендаций, изложенных в пункте 6.140, следует учитывать вероятность того, что на конкретный компонент будут оказывать влияние другие явления (например, электромиграция в микросхемах, образование «усов олова», механические вибрации или химическая деструкция).

6.143. В программу проведения работ по техническому обслуживанию следует включать меры по выявлению тенденций к деградации (старению), включая выявление предшествующих явлений, которые могли привести к неспособности оборудования выполнять предписанную ему функцию безопасности.

6.144. Примеры методов мониторинга включают:

— проведение испытаний репрезентативных элементов станции или репрезентативного блока, подверженных старению, на деградацию эксплуатационных показателей через определенные промежутки времени;
— визуальный контроль;
— анализ опыта эксплуатации.

6.145. Примеры мер, позволяющих решить проблему воздействия процессов старения, включают:

— замену компонентов до окончания их квалифицированного срока службы (аттестованного ресурса);
— корректировку функциональных характеристик (повторную калибровку) с учетом эффектов старения;
— переход на процедуры технического обслуживания или изменение условий окружающей среды на условия, способные замедлить процесс старения.

6.146. Следует определить квалифицированный срок службы компонентов с присвоенным им классом безопасности, которые должны выполнять функции безопасности в жестких окружающих условиях.

6.147. Замену классифицированных по безопасности компонентов следует проводить до истечения их квалифицированного срока службы.

6.148. Проводимая квалификация может показать, что квалифицированный срок службы компонента может быть валидирован или что он отличается от расчетного срока службы, который был определен при проведении испытаний, анализа или на основании опыта эксплуатации. Результаты проведенной квалификации могут быть использованы для продления или сокращения квалифицированного срока службы компонента.

6.149. Предполагаемый срок службы и предполагаемое устаревание СКУ или их компонентов следует определять на стадии проектирования, и данные об этом следует передать эксплуатирующей организации.

6.150. Оценка срока службы и предполагаемой даты устаревания систем и компонентов СКУ позволяет эксплуатирующей организации получить необходимую информацию для заключения долгосрочных соглашений с поставщиками, планирования приобретения дополнительных запасных частей, а также планирования своевременной замены устаревших единиц.

6.151. Предполагается, что процессы старения и устаревания могут значительно сократить срок службы СКУ в сравнении со сроком службы станции. Поэтому, вероятно, целесообразно предусмотреть меры, облегчающие монтаж и использование запасных частей. Такими мерами можно считать резервирование места для монтажа нового оборудования и соответствующего комплекта кабелей.

6.152. Публикация Серии норм безопасности МАГАТЭ, № NS-G-2.12, «Управление старением атомных электростанций» [25] содержит рекомендации по управлению старением и устареванием. Она содержит описание взаимосвязи между программой квалификации оборудования и программой управления старением.

КОНТРОЛЬ ДОСТУПА К СИСТЕМАМ, ВАЖНЫМ ДЛЯ БЕЗОПАСНОСТИ

6.153. В требовании 39 публикации SSR-2/1 (Rev. 1) [1] указано: «Должны приниматься меры для предотвращения несанкционированного доступа на АЭС или вмешательства в функционирование узлов, важных для безопасности, включая аппаратные средства и программное обеспечение компьютеров».

6.154. Публикации [26–28] содержат руководящий материал по физической безопасности АЭС и координации безопасности и физической ядерной безопасности.

6.155. Доступ к оборудованию СКУ следует ограничить в целях предотвращения несанкционированного доступа и снижения вероятности возникновения ошибки.

6.156. В число эффективных методов входит применение должного сочетания административных мер и мер по обеспечению физической безопасности (например, запираемые ограждения и запираемые помещения и сигнализация на дверях ограждения).

6.157. К зонам особого внимания относятся места доступ к регулировкам заданных уставок, регулировкам калибровки и к данным по конфигурации ввиду их важности для предотвращении деградации эксплуатационных характеристик систем вследствие ошибок в эксплуатации или техническом обслуживании.

6.158. В пунктах 7.103–7.130 изложены дополнительные рекомендации по контролю электронного доступа к цифровым системам.

ИСПЫТАНИЯ И ТЕСТОПРИГОДНОСТЬ В ПЕРИОД ЭКСПЛУАТАЦИИ

6.159. В требовании 29 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Узлы АЭС, важные для безопасности, должны проектироваться с расчетом на калибровку, испытания, техническое обслуживание, ремонт или замену, инспектирование и контроль, которые требуются для обеспечения возможности выполнения ими своих функций и сохранения их работоспособности во всех условиях, предусмотренных их проектными основами».

6.160. Пункт 6.35 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Системы безопасности должны проектироваться с таким расчетом, чтобы имелась возможность проведения периодических проверок их функциональности, когда станция находится в эксплуатации, в том числе возможность независимой проверки каналов для обнаружения отказов и утраты резервирования. Проект должен предусматривать возможность проверки всех аспектов функциональности датчика, входного сигнала, конечного исполнительного механизма и дисплея».

Меры для проведения испытаний

6.161. В СКУ следует предусматривать средства для проведения испытаний.

6.162. Средства для проведения испытаний, постоянно связанные с системами безопасности, фактически представляют собой системы безопасности за исключением случаев, когда они спроектированы в соответствии с рекомендациям по независимости, изложенным в пунктах 6.25–6.56.

6.163. Следует обеспечить, чтобы проведение испытаний и калибровки оборудования систем безопасности было возможно в любых режимах нормальной эксплуатации, включая работу на мощности, при сохранении способности систем безопасности выполнять предписанные им функции безопасности.

6.164. Проведение периодических испытаний во время эксплуатации станции, как правило, требуются для обеспечения требуемого уровня надежности систем безопасности; тем не менее иногда целесообразно не проводить испытания при работе на мощности, если испытания могут поставить под угрозу безопасность станции. Польза от проведения испытаний и калибровки во время эксплуатации на мощности следует взвешивать с учетом отрицательных последствий для безопасности станции, к которым может привести проведение таких испытаний.

6.165. В случае невозможности провести испытания системы безопасности или ее компонента в режиме эксплуатации на мощности следует обеспечить, чтобы было:

— продемонстрировано, что надежность соответствующих функций будет приемлемой в период между испытаниями;
— продемонстрировано, что требуемая точность и стабильность непроверенных компонентов будет соответствовать требованиям в период между испытаниями;
— предусмотрено возможное использование средств для сравнения результатов измерений на неиспытанных измерительных каналах с другими устройствами (например, для сравнения мощности нейтронного потока с тепловой мощностью);
— предусмотрено возможное проведение испытаний непроверенных систем или компонентов во время останова.

Автоматические испытания, самоконтроль и мониторинг

6.166. В СКУ следует предусматривать средства самоконтроля или мониторинга для регулярного подтверждения правильного функционирования.

6.167. В число таких средств входят средства проверки рациональности вводов.

6.168. В цифровые системы безопасности следует включить устройства контроля безопасного состояния, например, контрольные («сторожевые») таймеры.

6.169. Средством выполнения рекомендации, изложенной в пункте 6.166, является проектирование систем или ее компонентов таким образом, чтобы их отказы были самообнаруживаемыми.

6.170. В состав тестового оборудования включаются программные и аппаратные средства для выполнения испытаний с соответствующими тестовыми последовательностями независимо от режима их запуска — вручную или автоматически.

6.171. Следует предусматривать предупредительную сигнализацию для индикации потери резервирования в системах безопасности.

6.172. Следует обеспечить, чтобы при обнаружении дефекта в системе или оборудовании методом самоконтроля предпринимались заранее определенные действия.

Сохранение функций контроля и управления при проведении испытаний

6.173. Пункт 5.46 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Если планируется, что узлы, важные для безопасности, будут проходить калибровку, испытания или техническое обслуживание при работе под нагрузкой, должны быть спроектированы соответствующие системы для выполнения таких задач без значительного снижения надежности выполнения функций безопасности. В проект должны быть включены меры для проведения калибровки, испытаний, технического обслуживания, ремонта, замены или инспектирования

узлов, важных для безопасности, в период останова, с тем чтобы такие задачи можно было выполнять без значительного снижения надежности выполнения функций безопасности».

6.174. Следует обеспечить, чтобы средства для проведения испытаний СКУ (вручную и в автоматическом режиме) были разработаны таким образом, чтобы тестирование не оказывало негативного воздействия на способность СКУ выполнять предписанные им функции безопасности и минимизировать вероятность ложного инициирования действий по обеспечению безопасности и другие негативные воздействия испытаний на эксплуатационную готовность станции.

6.175. Следует обеспечить, чтобы предусмотренные меры для проведения испытаний не подвергали угрозе независимость систем безопасности, а также не приводили к потенциальному возникновения отказов по общей причине.

6.176. К средствам для проведения испытаний относятся процедуры, тестовые интерфейсы, установленная тестовая аппаратура и встроенный комплекс тестового оборудования.

Тестовые интерфейсы

6.177. Пункт 5.45 публикации SSR-2/1 (Rev. 1) [1] гласит:

«Станция должна быть спланирована с таким расчетом, чтобы способствовать деятельности по калибровке, испытаниям, техническому обслуживанию, ремонту или замене, инспектированию и контролю и обеспечивать возможность их выполнения с соблюдением соответствующих национальных и международных кодексов и норм. Такая деятельность должна соответствовать важности выполняемых функций безопасности и должна производиться без чрезмерного облучения работников».

6.178. Следует обеспечить, чтобы устройства, предусматриваемые для целей проведения испытаний СКУ и их компонентов, характеризовались следующим:

— имели соответствующие тестовые интерфейсы[26] и средства индикации состояния;
— функционировали так, чтобы дефекты в оборудовании можно было легко обнаружить;
— имели средства предотвращения несанкционированного доступа;
— были легкодоступными для персонала, проводящего испытания, и для тестового оборудования;
— имели необходимые коммуникационные средства для поддержки проведения испытаний;
— были размещены так, чтобы ни сами испытания, ни доступ к месту проведения испытаний не подвергали эксплуатационный персонал воздействию опасных условий[27].

6.179. В случае, если подлежащее испытаниям оборудование располагается в опасных зонах, следует предусмотреть средства управления испытаниями за пределами опасной зоны.

---

[26] Например, тестовые интерфейсы с возможностью ввода смоделированных условий процесса или электрических сигналов.

[27] Примерные вопросы, учитываемые при выборе местоположения средств, предназначенных для проведения испытаний, включают:

— расположение датчиков таким образом, чтобы тестирование и калибровка этих датчиков могли выполняться в месте их расположения;
— расположение тестовых устройств и тестовой аппаратуры в местах, удобных для тестирования оборудования;
— особенности станции или административного управления, могущие затруднить доставку тестовой аппаратуры к месту расположения тестируемых компонентов, например, при необходимости перемещения аппаратуры в узких проходах или ее доставки в зараженные зоны и удаления из них;
— удобство определения состояния компонентов или подключения тестовых схем.

Программа испытаний

6.180. При проектировании СКУ следует предусматривать спецификацию программы испытаний и калибровки, которая поддерживает применение рекомендаций, изложенных в соответствующих Руководствах по безопасности МАГАТЭ [16, 29–31].

6.181. Программа испытаний СКУ, как правило, включает:

— описание целей программы;
— спецификацию тестируемых систем и каналов;
— нормирование частоты и последовательности отдельных испытаний;
— изложение причин и обоснования проведения испытаний и нормирование интервалов проведения испытаний;
— описание требуемой документации и учетных записей;
— изложение критериев прохождения или непрохождения испытаний и процедур устранения несоответствия этим критериям;
— требования по периодическому рассмотрению эффективности программы испытаний;
— спецификацию отдельных тестовых процедур, которые будут использоваться для проведения испытаний.

6.182. Следует обеспечить, чтобы объем и частота проведения испытаний и калибровки были с соответствующим обоснованием признаны отвечающими функциональным требованиям и требованиям эксплуатационной готовности.

6.183. Следует обеспечить, чтобы программа испытаний подтверждала соответствие указанным ниже условиям во время и по завершении испытаний:

— общие функциональные возможности систем не снижены;
— системы безопасности СКУ продолжают соответствовать функциональным требованиям и требованиям к эксплуатационным характеристикам.

6.184. Следует обеспечить, чтобы в программе испытаний проводимые тесты были организованы в такой последовательности, чтобы общее состояние тестируемой системы или тестируемого компонента было немедленно оценено без необходимости дальнейшего тестирования других компонентов или систем.

6.185. Следует обеспечить, чтобы осуществление программы испытаний не приводило к ухудшению работы компонента станции сверх пределов, предусмотренных при проектировании.

6.186. При осуществлении программы испытаний и принятии решения о достижении данным компонентом квалифицированного срока службы может требоваться учет износа и старения вследствие тестирования.

6.187. Следует обеспечить, чтобы программа испытаний обеспечивала:

— получение объективной информации о состоянии системы или компонента;
— оценку деградации компонента;
— получение данных о тенденциях, помогающих выявить деградацию;
— индикацию начальной стадии отказа в системе;
— определение потребности в оценках, которые должны быть проведены прежде, чем результаты повторного теста в случае отрицательных итогов первоначального теста могут быть использованы для подтверждения работоспособности [28].

6.188. В программе испытаний следует указать процедуры проведения периодических испытаний и калибровки, которые:

— определяют общие проверки функций безопасности, начиная с датчиков и заканчивая исполнительными устройствами;
— могут проводиться на месте;
— подтверждают соблюдение функциональных требований и требований к эксплуатационным характеристикам, предъявляемых к оборудованию;

[28] Оценку и документирование предпосылок, коренных причин и действий, предпринятых после непрохождения испытания, как правило, необходимо проводить до того, как результаты повторного теста будут использованы для подтверждения работоспособности данной системы или данного компонента. Корректирующие действия могут включать техническое обслуживание или ремонт компонентов, а также внесение изменений в тестовые процедуры. Если признается, что применение корректирующих действий не требуется, должно быть документально зафиксировано соответствующее обоснование.

— используются для тестирования функций на входе и выходе, таких как предупредительная сигнализация, индикаторы, управляющие воздействия и срабатывание исполнительных устройств, в той мере, в какой это необходимо для соблюдения требований, предъявляемых к надежности системы, и функциональных требований;
— указывают ожидаемые результаты каждого испытания;
— обеспечивают безопасность станции в ходе испытаний;
— минимизируют вероятность ложного срабатывания любого из устройств системы безопасности и возникновения любого нежелательного воздействия испытаний на эксплуатационную готовность станции;
— запрещают использование самодельных тестовых схем, временных перемычек или введение временных изменений в компьютерные коды[29];
— запрещают изменение конфигурации параметров элементов станции до тех пор, пока эти параметры не будут определены как сервисные;
— минимизируют интервал времени, в течение которого оборудование выводится из эксплуатации;
— применяются для тестирования по отдельности каждого датчика в той мере, в какой это возможно.

6.189. В дополнение к рекомендациям, изложенным в пункте 6.188, следует обеспечить, чтобы процедуры, предназначенные для проведения периодических испытаний и калибровки систем безопасности:

— представляли собой единичный неавтономный тест (в режиме онлайн)[30];

---

[29] Тестовая аппаратура может быть временно подсоединена к оборудованию станции, если тестируемое оборудование имеет устройства, специально предназначенные для подсоединения такой тестовой аппаратуры. При необходимости выполнения временных подсоединений, предназначенных для проведения периодических испытаний или калибровки, в отношении таких подсоединений и использования такой аппаратуры применяются надлежащие меры административного контроля.

[30] Такой неавтономный тест (в режиме онлайн) позволяет выявить конкретные дефекты сразу после начала его проведения без необходимости использования тестовых подсоединений, вмешательства в эксплуатацию оборудования, действующего в неавтономном режиме (режиме онлайн), или нарушения его работы в течение времени, не превышающего установленные ограниченные сроки.

— независимо подтверждали функциональные требования и требования к эксплуатационным характеристикам, предъявляемые к каждому каналу функций датчиков, команд, исполнительных или вспомогательных функций;
— охватывали испытываемые функции настолько полно, насколько это практически возможно (включая датчики и исполнительные устройства), без ущерба для непрерывной нормальной эксплуатации станции;
— по возможности выполнялись в реальных или моделируемых эксплуатационных условиях, включая последовательность операций;
— позволяли проводить испытания и калибровку всех задействованных параметров, если для запуска определенных сигналов для системы безопасности используются комбинации параметров;
— позволяли выявлять дефекты в резервированном оборудовании[31].

6.190. Когда проведение единичного неавтономного тест (в режиме онлайн) не представляется практически возможным, в программе испытаний может быть предусмотрено проведение частично дублирующихся тестов для достижения целей испытаний. Если единичный неавтономный тест (в режиме онлайн) не проводится для канала системы безопасности, следует подготовить документированное обоснование применения частично дублирующихся тестов.

6.191. Как правило, в обосновании подтверждается, что частично дублирующиеся тесты обеспечивают полный охват целей, что уровень надежности оборудования признается приемлемым с учетом длительного интервала времени испытаний и что любые компоненты, не проверенные в режиме онлайн, будут протестированы во время останова станции.

РЕМОНТОПРИГОДНОСТЬ

6.192. При проектировании СКУ следует предусматривать планы проведения технического обслуживания для всех систем и элементов.

[31] Резервированное оборудование может представлять собой резервированные отдельные группы или резервированное оборудование одной отдельной группы.

6.193. Системы и элементы СКУ следует проектировать, размещать и монтировать так, чтобы минимизировались риски для эксплуатационного персонала и облегчалось проведение планово-предупредительного технического обслуживания, поиска и устранения неисправностей и своевременного ремонта.

6.194. Проектные меры, облегчающие техническое обслуживание, поиск и устранение неисправностей и ремонт, включают:

— исключение размещения оборудования в местах, в которых предполагается наличие условий с экстремальными значениями температур или влажности во время нормальной эксплуатации станции;
— исключение размещения оборудования в местах, в которых присутствует риск возникновения высокого уровня излучения (см. публикацию Серии норм безопасности МАГАТЭ, № NS-G-1.13, «Аспекты радиационной защиты при проектировании атомных электростанций» [32]);
— учет человеческих возможностей и ограничений при осуществлении мероприятий по техническому обслуживанию;
— отведение достаточного пространства вокруг оборудования для обеспечения того, чтобы обслуживающий персонал мог выполнять порученные ему задачи в нормальных рабочих условиях.

6.195. В случае размещения элементов в недоступных местах примерами других стратегий устранения неисправностей могут быть:

— установка запасных резервируемых устройств;
— обеспечение возможности дистанционного обслуживания;
— планирование эксплуатации станции на пониженном уровне мощности в случае отказа в работе оборудования и отсутствия возможности его быстро и легко отремонтировать или произвести замену.

6.196. Меры, предусмотренные для целей технического обслуживания СКУ, следует проектировать с таким расчетом, чтобы допускались любые воздействия на безопасность станции.

6.197. К типичным примерам таких мер относится отключение одной отдельной группы в системе с несколькими резервированными отдельными группами или меры, предусматривающие выполнение альтернативных действий вручную.

МЕРЫ ПО ВЫВОДУ ИЗ ЭКСПЛУАТАЦИИ ДЛЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ ИЛИ ОБСЛУЖИВАНИЯ

6.198. Если использование аппаратуры для проведения испытаний или технического обслуживания может привести к нарушению функции СКУ, в интерфейсах следует предусмотреть аппаратную блокировку для обеспечения того, чтобы взаимодействие с системой для проведения испытаний или технического обслуживания было невозможно без намеренного вмешательства в ручном режиме.

6.199. При проектировании следует обеспечить, чтобы системы не возможно было неосознанно оставить в конфигурации для проведения испытаний или технического обслуживания.

6.200. Следует обеспечить, чтобы вывод из эксплуатации любого отдельного компонента системы безопасности или любой резервированной отдельной группы не приводил к потере необходимого минимума резервирования, за исключением случаев, когда может быть продемонстрировано, что эксплуатация системы может осуществляться с приемлемым уровнем надежности.

6.201. Пункт 6.36 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «В случае необходимости вывода системы безопасности или части системы безопасности из эксплуатации для проведения проверки и испытаний должны быть предусмотрены достаточные меры, позволяющие четко указать любые байпасы системы защиты, которые необходимы на срок проведения мероприятий по проверке и испытаниям или техническому обслуживанию».

6.202. Следует обеспечить, чтобы в помещении щита управления отображалась информация о неработоспособности или байпасировании компонентов системы безопасности или групп безопасности.

6.203. Следует обеспечить, чтобы для единиц оборудования (узлов), которые часто байпасируются или находятся в нерабочем состоянии, такая индикации была автоматической.

6.204. В публикации NS-G-2.6 [16] изложены рекомендации, касающиеся возврата систем и оборудования в эксплуатацию по завершении испытаний и работ по техническому обслуживанию.

ЗАДАННЫЕ УСТАВКИ

6.205. Пункт 5.44 (b) публикации SSR-2/1 (Rev. 1) [1] гласит: «Требования и эксплуатационные пределы и условия, устанавливаемые при проектировании АЭС, должны включать... пределы установок системы безопасности...».

6.206. Эксплуатационные пределы и условия для безопасной эксплуатации включают заданные уставки СКУ для систем безопасности.

6.207. При определении заданных уставок СКУ для систем безопасности, как правило, учитываются:

— пределы безопасности: ограничения определенных эксплуатационных параметров, по которым можно сделать вывод о безопасной работе станции[32];
— аналитический предел (заданной уставки): пределы измеренных или подсчитанных переменных величин, установленных анализом безопасности в целях обеспечения того, чтобы предел безопасности не мог быть превышен[33];
— заданная уставка защиты: заранее установленное значение для запуска устройства задания конечной уставки для инициирования мер защиты;
— допустимое значение: предельное значение, которое может быть задано после проведения периодических испытаний, в случае превышения которого требуется принятие соответствующих мер. Обнаружение превышения допустимого значения уставки может означать, что канал не функционировал в пределах допущений, принятых в анализе заданных уставок. В этом случае необходимо определить, были ли нарушены эксплуатационные пределы и условия, и при обнаружении таких нарушений — какие меры должны быть приняты для восстановления работоспособности канала;

---

[32] Пределы безопасности иногда задаются посредством параметров, которые не могут быть измерены непосредственно системой СКУ.

[33] При установлении запаса между аналитическим пределом и пределом безопасности учитывается время реакции измерительного канала и спектр переходных процессов, возникающих вследствие рассматриваемой аварии.

— пределы установок системы безопасности: уровни, при которых в случае возникновения ожидаемых при эксплуатации событий или аварийных условий защитные устройства должны запускаться автоматически в целях предотвращения превышения пределов безопасности[34].

6.208. Заданные уставки, измеренные во время проведения периодических испытаний, следует оценить для подтверждения того, что отклонение значений от предыдущей настройки соответствует ожидаемым результатам анализа неопределённостей. Избыточное отклонение, которое не ведет к нарушению допустимого значения (например, отклонение в консервативном направлении), может быть показателем того, что поведение канала не соответствует ожиданиям и что требуется либо ремонт оборудования, либо пересмотр результатов анализа.

6.209. Рис. 3 иллюстрирует соответствие между применяемой терминологией и типами неопределённостей и систематическими погрешностями измерений, которые обычно учитываются при определении основы для заданных уставок защиты и допустимых значений.

6.210. Заданные уставки могут быть фиксированным либо переменным значением, что зависит от некоторых других параметров или условий станции.

6.211. Заданные уставки защиты, используемые для инициирования действий по обеспечению безопасности, следует устанавливать так, чтобы требуемые действия по смягчению последствий совершались до того, как контролируемая переменная величина достигает аналитического предела.

6.212. Пределы установок системы безопасности следует определять с использованием документально подтвержденной методологии, в которой предусматривается достаточный допуск между заданными уставками

---

[34] В некоторых государствах в качестве официальных терминов могут быть приняты термины «пределы установок системы безопасности», «установки системы безопасности», либо «пределы настройки системы безопасности». Для этих предельных значений могут использоваться такие выражения как заданные уставки защиты, допустимые значениями или то и другое. Публикация Серии норм безопасности МАГАТЭ, № NS-G-2.2, «Пределы и условия эксплуатации и эксплуатационные процедуры для атомных электростанций» [29] содержит дополнительный руководящий материал по выбору и применению настроек системы безопасности.

РИС 3. Терминология, используемая для заданных уставок, и ошибки, учитываемые при определении заданных уставок

защиты и аналитическим пределом с целью учета систематических погрешностей измерений, систематических погрешностей канала, неопределенностей и любых появляющихся со временем изменений этих значений.

МАРКИРОВКА И ИДЕНТИФИКАЦИЯ УЗЛОВ, ВАЖНЫХ ДЛЯ БЕЗОПАСНОСТИ

6.213. Следует определить и применять на этапах проектирования, монтажа и эксплуатации в течение жизненного цикла станции последовательную, согласованную и легко понятную систему терминов и идентификации всех компонентов СКУ, а также использовать эту систему для создания описательных названий для человеко-машинного интерфейса.

6.214. Следует обеспечить, чтобы признанная подходящей идентификационная схема не содержала большого количества ссылок на чертежи, инструкции, руководства или другие материалы.

6.215. Принятие последовательных и легких для понимания наименований и идентификационных знаков для систем и компонентов является важным условием для облегчения работы инженерно-технического персонала, персонала, осуществляющего техническое обслуживание, и персонала, осуществляющего строительно-монтажные работы, а также для использования в маркировке средств управления, средств отображения информации и индикаторов.

6.216. На компоненты СКУ станции следует, как правило, наносить маркировку, содержащую идентифицирующую их информацию. Для компонентов или модулей, встроенных в оборудование, или сборных изделий не требуется наличие идентифицирующей маркировки. Конфигурационное управление обычно является достаточным для обеспечения идентификации таких компонентов, модулей или компьютерного программного обеспечения.

6.217. Следует обеспечить, чтобы компоненты, относящиеся к разным отдельным группам безопасности, быть легко отличимыми друг от друга, а также от компонентов более низкого касса безопасности.

6.218. Четкая идентификация компонентов уменьшает вероятность непреднамеренного выполнения работ по обслуживанию, испытаниям, ремонту или калибровке на неправильно выбранном канале.

6.219. Для целей идентификации могут использоваться бирки или цветовая маркировка.

7. РУКОВОДЯЩИЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ КОНКРЕТНЫХ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ И ОБОРУДОВАНИЯ

ДАТЧИКИ

7.1. Следует обеспечить, чтобы измерение параметров на станции соответствовало требованиям проектных основ СКУ и станции.

7.2. Измерение параметров станции включает как измерение текущего значения параметров в рамках определенного диапазона, так и определение дискретных состояний, которые могут быть выявлены с помощью концевых выключателей, вспомогательного реле и датчиков температуры, давления, расхода и уровня.

7.3. Измерение параметров на станции может выполняться прямым или косвенным методом, например путем вычисления, основанного на множественных измерениях или определении значения параметра на основании измерения других данных с известным соотношением с данным параметром.

7.4. В той мере, в какой это практически возможно, мониторинг условий на станции следует осуществлять путем проведения прямых измерений, а не путем использования данных, полученных на основании косвенных измерений.

7.5. Датчики для каждого контролируемого параметра и его диапазона следует подбирать с учетом характеристик точности, скорости реакции, эксплуатационных условий и рабочего диапазона, которые необходимы для мониторинга параметров в любых режимах работы станции, во время которых датчики должны осуществлять передачу информации. При проектировании датчиков и исполнительных устройств следует учитывать проектные запасы.

7.6. Следует обеспечить, чтобы информация о последствиях отказов датчиков по общей причине была включена в анализ, описанный в пунктах 4.30–4.34.

7.7. Следует обеспечить, чтобы никакая выявленная уязвимость к воздействию отказа по общей причине датчиков не приводила к возможному неполучению операторами информации и параметров, которые необходимы им для управления авариями и смягчения их последствий.

7.8. Если для охвата всего спектра контролируемых параметров требуется несколько датчиков, следует предусмотреть достаточную степень перекрытия между датчиками в каждой точке перехода для обеспечения того, чтобы насыщение сигнала или последствия наложения сигналов на кривой ответного сигнала не мешали выполнению требуемой функции.

7.9. Если при измерении переменной пространственная зависимость (когда измеренное значение переменной зависит от места расположения датчика) является важным фактором в обеспечении выполнения функции СКУ, следует определить минимальное количество и расположение датчиков.

СИСТЕМЫ УПРАВЛЕНИЯ

7.10. В требовании 60 публикации SSR-2/1 (Rev. 1) [1] указано: «На АЭС должны быть предусмотрены надлежащие и надежные системы управления для поддержания и ограничения соответствующих технологических параметров в установленных эксплуатационных диапазонах».

7.11. Автоматическое управление, поддерживающее основные параметры процессов в рамках эксплуатационных пределов, является частью системы глубокоэшелонированной защиты станции, и поэтому связанные с ним системы управления, как правило, являются важными для безопасности.

7.12. Следует предусмотреть, чтобы системы контроля обеспечивали плавный переход от автоматического к ручному управлению, а также при автоматическом переключении с процессора, работающего в неавтономном режиме (режиме онлайн), на резервный процессор.

7.13. Следует обеспечить, чтобы при сбое в подаче электропитания к системе с функциями управления происходило плавное переключение на резервное оборудование либо включалась блокировка исполнительных устройств со срабатыванием сигнализации и переходом на ручной режим управления оператором.

7.14. Следует обеспечить, чтобы последствия отказа системы автоматического управления не создавали условия, при которых превышаются критерии приемлемости либо допущения, принятые в отношении проектных аварий. Такие виды отказа, как множественное ложное срабатывание системы управления, следует также учитывать, если существует потенциальная возможность возникновения таких отказов при данном проектном решении системы. Для устранения вероятности множественных ложных срабатываний системы управления или снижения вероятности их возникновения до приемлемого уровня могут быть применены соответствующие проектные меры, такие как сегментация.

СИСТЕМА ЗАЩИТЫ

7.15. В требовании 61 публикации SSR-2/1 (Rev. 1) [1] указано:

> «На АЭС должна быть предусмотрена система защиты, способная определять условия, угрожающие безопасности станции, и автоматически запускать действия по обеспечению безопасности в целях срабатывания систем безопасности, необходимых для достижения и поддержания безопасного состояния станции».

7.16. Следует обеспечить, чтобы система защиты отслеживала параметры станции и выявляла отклонения от установленных для них пределов так, чтобы система защиты поддерживала параметры станции в пределах, установленных для каждой проектной аварии.

7.17. Система защиты в целом может состоять из нескольких систем.

Автоматические действия и действия оператора, направленные на обеспечение безопасности

7.18. Пункт 6.33 b) публикации SSR-2/1 (Rev. 1. 1) [1] гласит:

> «Проект [системы защиты] ... должен автоматизировать различные действия по обеспечению безопасности с целью срабатывания систем безопасности, с тем чтобы в течение обоснованно установленного периода времени с начала ожидаемых при эксплуатации событий или возникновения аварийных условий оператору не требовалось принимать меры....»

7.19. Для автоматического запуска и контроля всех действий по обеспечению безопасности системы защиты следует предусмотреть необходимые средства, кроме случаев, в которых обоснованным является исключительно ручное управление.

7.20. Как правило, для большинства функций системы защиты предусматривается автоматическое инициирование.

7.21. Примеры ситуаций, в которых допустимо только ручное управление, включают:

— запуск определенных задач обеспечения безопасности после завершения автоматической последовательности операций;
— действия по управлению в целях приведения станции в конечном счете в безопасное состояние после аварии;
— инициирование действий по обеспечению безопасности, в которых не было необходимости в течение длительного времени после постулируемого исходного события.

7.22. Для обоснования приемлемости только ручного способа управления следует применять и соблюдать с подтверждением этого соблюдения указанные ниже требования, согласно которым следует обеспечить, чтобы:

— системы безопасности обеспечивали операторов ясно представленной и достаточной информацией, позволяющей им обоснованно принимать решение о необходимости инициирования необходимых действий по обеспечению безопасности;
— оператор имел процедуры в письменной форме и прошел практическое обучение по выполнению задач по обеспечению безопасности;
— оператор имел в своем распоряжении достаточные средства управления станцией для выполнения требуемых действий;
— между операторами, выполняющими соответствующие действия, были установлены каналы связи для обеспечения корректного выполнения этих действий;
— был проведен надлежащий анализ учета человеческого фактора для обеспечения поддержания условий на станции в рамках рекомендованных критериев для каждого постулируемого исходного события;

— оператор располагал достаточным временем для оценки состояния станции и для выполнения требуемых действий[35]. Следует обеспечить, чтобы соответствующий анализ синхронизации учитывал имеющееся время и время, необходимое для выполнения оператором каждого требующегося действия. Анализ синхронизации позволяет определить запас по надежности, и по мере снижения запаса по надежности следует должным образом учитывать неопределенности в оценке разности между этими значениями времени.

7.23. Для ручного запуска механических систем безопасности и отдельных компонентов, требуемых для инициирования и контроля выполнения предписанных им функций безопасности, следует предусмотреть соответствующие средства.

7.24. Сигнал, подаваемый вручную для инициирования выполнения функции безопасности механической системой безопасности, следует вводить в месте, находящемся на максимально возможном приближении к конечному исполнительному устройству.

7.25. Ручное инициирование действий по обеспечению безопасности является формой глубокоэшелонированной защиты в случае ожидаемых при эксплуатации событий и аварийных условий и обеспечивает поддержку долгосрочной эксплуатации станции после аварии.

7.26. Механическими системами безопасности являются, например, отдельные группы регулирующих стержней, системы аварийной подачи питательной воды, система аварийного охлаждения активной зоны или система изоляции защитной оболочки (гермооболочки).

Отображение информации

7.27. Пункт 6.33 (c) публикации SSR-2/1 (Rev. 1) [1] гласит: «Проект [системы защиты] ... должен предоставлять оператору соответствующую информацию для контроля результатов автоматически предпринимаемых действий».

---

[35] В случае разработки новых проектов или внесения значительных модификаций (значительной модернизации) на станции рекомендуется выполнять проектирование таким образом, чтобы действия оператора для поддержания параметров станции в установленных пределах не требовались в течение первых 30 минут проектной аварии.

7.28. Следует предусмотреть, чтобы система защиты обеспечивала операторам индикацию измеренного значения каждого входного параметра, используемого для реализации функций системы защиты, данных о состоянии каждой функции отключения и функции активации в каждой отдельной группе, а также о состоянии срабатывания каждой системы.

Датчики и настройки системы защиты

7.29. Следует обеспечить, чтобы датчики, передающие системе защиты сигналы, направляли эти сигналы другим системам только через соответствующие буферные и изолирующие устройства.

7.30. Следует использовать в той мере, в какой это практически возможно, такие принципы проектирования, как функциональная неодинаковость (диверсность), резервирование и неодинаковость (диверсность) сигналов с целью предотвращения потери функций системы защиты.

7.31. Если для выполнения системой защиты предписанных ей функций необходимо применять множественные заданные уставки (например, разрешающие увеличение или снижение уровня мощности), при проектировании следует обеспечить, чтобы более ограничительная уставка устанавливалась автоматически или в административном порядке в случае, когда условия на станции уже не позволяют применять менее ограничительные уставки.

7.32. Иногда для достижения адекватного уровня защиты при определенном режиме эксплуатации или при определенной совокупности эксплуатационных условий целесообразно использовать множественные заданные уставки.

7.33. Если при проектировании предусматриваются регулируемые заданные уставки или возможность изменения заданной уставки, когда необходимо обеспечить функционирование данной системы защиты, следует обеспечить, чтобы устройства для регулирования или изменения уставок были частью системы защиты.

7.34. В системе защиты следует предусматривать средства для определения значений заданных уставок для каждого канала системы защиты.

Технологические байпасы

7.35. Технологический байпас или логика условий защитного отключения могут быть необходимы для замедления срабатывания системы безопасности в случае возникновения на станции конкретных условий. Например, технологической необходимостью является обеспечение того, чтобы защитные отключения, ограничивающие мощность реактора во время пуска, байпасировались в некоторой точке, чтобы позволить повышение мощности сверх уставки защиты по малой мощности.

7.36. В случае необходимости применения технологического байпаса следует обеспечить, чтобы оператор получал соответствующие сигналы предупреждения о приближении станции к состоянию, в котором требуется применение технологического байпаса.

7.37. На щите управления следует предусмотреть индикацию состояния технологических байпасов.

7.38. Следует обеспечить, чтобы система защиты автоматически выполняла одно из следующих действий, если условия для задействования технологического байпаса не будут соблюдены:

— отключение приведенного в действие технологического байпаса;
— перевод станции в состояние, при котором технологический байпас допустим; или
— инициирование соответствующих защитных действий.

Фиксация функций системы защиты

7.39. Пункт 6.33 (a) публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Проект [системы защиты] ... должен предотвращать действия оператора, которые могут угрожать эффективности системы защиты в эксплуатационных состояниях и аварийных условиях, однако не должен препятствовать правильным действиям оператора в аварийных условиях...».

7.40. Следует обеспечить, чтобы действия, инициированные системой защиты, фиксировались таким образом, чтобы включенное действие продолжало выполняться несмотря на то, что исходное состояние, которое привело к инициированию действия, перестало существовать.

7.41. Фиксирование действий, инициированных системой защиты, как правило, выполняется при поступлении сигналов на срабатывание на оборудование станции. «Удерживание» в сработавшем состоянии индивидуальных измерительных каналов не обязательно.

7.42. Следует обеспечить, чтобы после срабатывания функции защитной системы все предусмотренные для нее действия были завершены.

7.43. Рекомендации, изложенные в пункте 7.42, не направлены на ограничение действия устройств, предусмотренных для электрической защиты оборудования системы безопасности, приводимого в действие системой защиты. В публикации SSG-34 [7] изложены рекомендации по электрической защите узлов, важных для безопасности.

7.44. Следует обеспечить, чтобы при сбросе функции системы защиты приведенное в действие оборудование автоматически не возвращалось в нормальное состояние и такой возврат был возможен только в случае выполнения оператором специальных целенаправленных действий.

7.45. Средства для сброса функции безопасности следует предусматривать в самой системе безопасности.

Ложное инициирование срабатывания

7.46. Следует обеспечить, чтобы при проектировании защитной системы в той мере, в какой это практически возможно, сводилась к минимуму потенциальная возможность ложного инициирования срабатывания или ложных действий системы защиты.

7.47. Ложное инициирование срабатывания системы защиты может привести к:

— излишней нагрузке на оборудование и сокращению срока службы станции;
— необходимости выполнения других действий по обеспечению безопасности;
— снижению уверенности операторов в оборудовании, что потенциально может привести к последующему игнорированию ими достоверных сигналов;
— сокращению производственной мощности станции.

7.48. Следует обеспечить, чтобы ложное инициирование срабатывания системы безопасности не приводило станцию к небезопасному состоянию.

7.49. Если ложное инициирование срабатывания или ложное действие системы защиты может привести станцию к состоянию, при котором по-прежнему требуется выполнение защитных функций, то безопасные условия следует поддерживать посредством выполнения действий, инициируемых и выполняемых функциональными частями системы защиты или другими системами безопасности, которые не были задействованы в инициировании ложного срабатывания и не подверглись его воздействию.

Взаимодействие между системой защиты и другими системами

7.50. В требовании 64 публикации SSR-2/1 (Rev. 1) [1] указано: «Взаимовлияние систем защиты и систем управления на АЭС должно предотвращаться посредством разделения, путем исключения взаимосвязей или обеспечения соответствующей функциональной независимости».

7.51. Пункт 6.38 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Если сигналы используются совместно как системой защиты, так и какой-либо системой управления, то должно обеспечиваться разделение (например, посредством соответствующих развязывающих устройств), а система сигнализации должна быть отнесена к системе защиты».

7.52. Следует обеспечить, чтобы система защиты соответствовала всем требованиям по надежности, резервированию и независимости в случае отказа любого из компонентов или поступления сигнала, используемого совместно системой защиты и системой управления.

7.53. Пункт 6.32 (a) публикации SSR-2/1 (Rev. 1) [1] гласит: «Система защиты должна проектироваться с таким расчетом, чтобы она... была в состоянии подавлять действия системы управления, угрожающие безопасности...».

7.54. Если постулируемое исходное событие может вызвать действие системы управления, которое приводит станцию к состоянию, в котором требуется инициирование функции системы защиты, то следует обеспечить,

чтобы такое постулируемое исходное событие не препятствовало выполнению надлежащего действия системой безопасности, обеспечивающей реализацию требуемой функции системы защиты.

7.55. Не следует исключать вероятность того, что отказ в системе безопасности может сам по себе являться постулируемым исходным событием, которое запускает действие системы управления, для выполнения которого требуется система защиты.

7.56. Примеры используемых мер для предотвращения помех между системами управления и системами защиты, приводящих к некорректной работе систем, включают:

— использование раздельных каналов аппаратуры для систем защиты и контроля;
— использование дополнительного оборудования в группе безопасности для устранения потенциальных помех;
— использование барьеров или альтернативных мер на станции для ограничения ущерба в результате возникновения постулируемого исходного события; или
— комбинации этих мер, обеспечивающие достаточную способность группы безопасности и проекта станции поддерживать условия работы станции в рамках приемлемых пределов.

7.57. Целью изложенных в пунктах 7.52, 7.54 и 7.55 рекомендаций является обеспечение того, чтобы в случае возникновения таких отказов система защиты все еще была способна в полной мере соответствовать предъявляемым к ней требованиям. Требования к надежности, подлежащие выполнению, включают соблюдение критерия единичного отказа.

7.58. Если устройство может быть активировано системой защиты или системой более низкого класса безопасности, следует обеспечить, чтобы любое требование системы защиты по инициированию срабатывания ее защитной функции имело приоритет в активации устройства.

7.59. Например, сигналы на срабатывание могут быть посланы от системы управления для ведения нормальной эксплуатации или для осуществления эксплуатирующим персоналом контроля нормального функционирования всех элементов систем с одного и того же интерфейса, если требование системы защиты будет иметь приоритет над командами, посылаемыми системой управления.

ИСТОЧНИКИ ЭНЕРГОСНАБЖЕНИЯ

7.60. К источникам энергоснабжения СКУ, независимо от их типа (источники электроснабжения, источники пневмоэнергии, источники гидравлической энергии), следует применять требования в отношении класса безопасности, надежности, квалификации, изоляции, тестопригодности, ремонтопригодности и индикации вывода из эксплуатации, соответствующие требованиям, предъявляемым к надежности СКУ, которые эти источники обслуживают.

7.61. СКУ, которые должны находиться в состоянии готовности в любое время в эксплуатационных состояниях или в условиях проектной аварии, следует подсоединять к источникам бесперебойного электроснабжения, способным обеспечить системы электропитанием с допустимыми отклонениями, установленными в проектной основе СКУ.

7.62. СКУ могут быть переключены вручную или автоматически с нормального источника электроснабжения на резервный, когда это необходимо в связи со сложившимися обстоятельствами эксплуатации, при условии, что связанное с этим переключением прерывание в подаче питания не скажется на функциях СКУ. Как правило, систему переключения питания следует рассматривать как часть общей системы электроснабжения, и она должна иметь тот же класс безопасности, что и системы СКУ, которые она снабжает.

7.63. Некоторые современные СКУ могут снабжаться электропитанием напрямую от источника питания постоянного тока. Это обеспечивает преимущество в случае систем, для которых требуются бесперебойные источники питания, поскольку такой способ питания исключает необходимость использования инверторов, мотор-генераторов или устройств переключения источников питания в системах электроснабжения.

7.64. Источники питания способны создавать пути распространения электромагнитных помех, источник которых может находиться вне конкретных СКУ или возникать в других СКУ, которые связаны прямо или косвенно с одним и тем же источником питания (см. пункт 6.132.).

7.65. В публикации SSG-34 [7] изложены рекомендации, касающиеся источников электроснабжения и связанных с ними распределительных систем. Рекомендации для других форм энергоснабжения (таких как источники пневмоэнергии, источники гидравлической энергии и

источники механической энергии) представлены в публикации Серии норм безопасности МАГАТЭ, № NS-G-1.8, «Проектирование систем аварийного энергоснабжения атомных электростанций» [33] [36].

ЦИФРОВЫЕ СИСТЕМЫ

7.66. Цифровые системы включают, например, компьютерные системы и системы, программируемые с помощью языков описания аппаратных средств.

7.67. В требовании 63 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Если система, важная для безопасности на атомной электростанции, зависит от компьютеризированного оборудования, то должны быть установлены и осуществляться в течение всего срока эксплуатации этой системы, в особенности на стадии разработки программного обеспечения, надлежащие нормы и практика разработки и испытания компьютерных аппаратных средств и программного обеспечения. Весь процесс разработки должен осуществляться в рамках системы менеджмента качества».

Функции цифровых систем

7.68. Использование цифровых систем для реализации функций СКУ обеспечивает преимущества, включающие гибкость в выполнении комплексных функций, улучшение мониторинга станции и усовершенствование интерфейса с операторами, возможности самотестирования и самодиагностики, улучшение условий среды, облегчающее учет опыта эксплуатации благодаря очень существенному расширению возможностей регистрации данных, уменьшению физических размеров и снижению потребностей в кабельных коммуникациях. Цифровые системы могут обладать функциями тестирования и самопроверки, которые повышает уровень надежности системы.

7.69. Реализация функций СКУ в цифровых системах отличается от методов их реализации в аналоговых системах. При использовании цифровых технологий функции объединяются в одном или нескольких

---

[36] Также находится в разработке руководство по безопасности, касающееся проектирования вспомогательных и поддерживающих систем атомных электростанций.

процессорных блоках. Условия, когда функции объединены в процессорном блоке, сложны для анализа, и отказ процессорного блока может привести к одновременному отказу нескольких функций. Кроме того, одна функция может оказывать негативное воздействие на реализацию другой функции (без видимого «отказа») вследствие нежелательных взаимодействий.

7.70. Проведение полной верификации и валидации таких комплексных компонентов может оказаться сложным или практически неосуществимым делом, если они спроектированы некорректно. Могут возникать неизвестные ошибки, дублирование которых может происходить во всех резервированных компонентах или которые могут распространяться на другие системы, базирующиеся на одной платформе, так как программные модули, программируемые устройства или библиотеки являются общими для всех этих компонентов.

7.71. В цифровых системах осуществляется квантование входных сигналов в дискретные моменты времени. Происходит периодическая передача сигналов между элементами системы, и так же периодически появляются выходные сигналы. Вследствие этого колебания в нагрузке на обработку или нагрузке на коммуникацию в цифровой системе могут оказывать влияние на скорость передачи данных и скорость реакции, если эти системы будут спроектированы некорректно. Колебания нагрузки на обработку или нагрузки на коммуникацию могут быть обусловлены изменениями параметров станции, разными режимами работы систем или станции или возникновением отказов в оборудования.

7.72. В публикации [11] можно найти подробную информацию, касающуюся специфики цифровых систем.

7.73. При проектировании цифровых СКУ следует обеспечить, чтобы система выполняла свои функции безопасности в соответствии с требованиями к скорости реакции и точности при всех эксплуатационных условиях и всех возможных условиях загрузки данных.

7.74. Системы безопасности в СКУ следует разрабатывать так, чтобы их поведение было детерминированным, когда любая последовательность входных сигналов, отвечающая спецификации узла, всегда будет давать одинаковые выходные сигналы с одинаковой скоростью реакции, т.е. временная задержка между стимулом и реакцией будет иметь гарантированный максимум и минимум.

7.75. Обеспечение детерминированной скорости реакции может включать:

— исключение связанных с процессами прерываний, чтобы никакое из состояний станции не могло напрямую влиять на частоту прерываний, с которыми СКУ придется иметь дело;
— статическое распределение ресурсов во время проектирования;
— ограничение числа итераций циклов, обусловленных заданными пределами.

7.76. Скорость реакции и точность цифровых систем функционально зависит от частоты дискретизации и от периода цикла обработки. В некорректно спроектированных системах эти параметры могут также зависеть от быстродействия процессора.

7.77. Проектирование и анализ цифровых систем следует выполнять так, чтобы отказы отдельных компонентов (например, процессоров компьютера) приводили к предсказуемому диапазону приемлемых алгоритмов поведения системы.

7.78. Следует обеспечить, чтобы потеря питания или перезапуск цифровой системы не приводили к нежелательному изменению конфигурационных данных или программного обеспечения.

Цифровая коммуникация данных

7.79. При проектировании следует предусматривать, чтобы средства коммуникации данных для систем безопасности обеспечивали детерминированное время передачи.

7.80. Средства обеспечения детерминированного времени передачи могут включать применение:

— предопределенного контролируемого по времени алгоритма поведения, когда действия системы коммуникации данных определяются не клиентскими узлами, а заранее определены в проекте на основании временного плана;
— предопределенного объема коммуникации данных, когда размер сообщения, передаваемого в течение данного промежутка времени, определяется при проектировании заранее так, чтобы коммуникационная нагрузка всегда соответствовала пропускной способности системы коммуникации данных;

— предопределенной схемы коммуникации данных, когда отправитель и получатель сообщения, передаваемого в течение данного промежутка времени, определяются при проектировании заранее.

7.81. Следует обеспечить, чтобы цифровая коммуникация данных соответствовала рекомендациями, изложенными в пунктах 6.25–6.56.

7.82. Следует обеспечить, чтобы каждое сообщение, полученное и отправленное посредством цифровой коммуникации данных, автоматически проверялось и при возникновении ошибок сопровождалось соответствующим сигналом.

7.83. Ошибки могут включать искаженные данные, недостоверные данные (внеплановые сообщения) или неаутентичные сообщения (сообщения из неожиданных источников).

7.84. Если в коммуникационных системах используются средства шифрования сообщений или собственные (проприетарные) протоколы, следует обеспечить, чтобы такие средства не препятствовали обнаружению ошибок.

7.85. Действия, которые должны предприниматься при обнаружении ошибок в коммуникации данных, следует определить заранее.

7.86. Действия, которые могут предприниматься при обнаружении ошибок, включают автоматическое отклонение недостоверных или неаутентичных данных, исправление искаженных данных, если это возможно, или отклонение искаженных данных.

7.87. При проектировании следует обеспечить, чтобы отказы оборудования, используемого для коммуникации данных, и коммуникационного оборудования выявлялись, операторам направлялись соответствующие предупредительные сигналы и данные об отказах фиксировались для последующего анализа функционирования систем.

7.88. Наличие определенных типов ошибок в цифровой коммуникации данных само по себе не говорит об отказе системы, поскольку такие погрешности являются ожидаемыми, и коммуникационные протоколы построены так, чтобы они справлялись с определенными типами ошибок в определенном диапазоне частоты появления ошибок. В связи с этим применение рекомендации, изложенной в пункте 7.87, предполагает

наличие спецификации возможных ошибок при передаче данных. Критерии, например, могут определять максимально допустимый временной интервал между успешной передачей или максимальную частоту появления ошибок.

7.89. Средства обнаружения и устранения ошибок способствуют повышению надежности передачи сигнала.

7.90. Следует обеспечить, чтобы методы, используемые для обнаружения и устранения ошибок и выявления отказов в коммуникации данных соответствовали данному виду применения данных, частоте запросов на исполнение функций, использующих данные, и были сбалансированы с учетом привносимой ими сложности.

Коммуникационные средства в системах безопасности

7.91. Следует обеспечить, чтобы при возникновении любой неисправности в процессе коммуникации связанных с безопасностью данных система безопасности продолжала выполнение предписанной ей функции безопасности и переводилась в безопасное состояние.

7.92. Эта рекомендация часто может быть реализована посредством применения двух процессоров, совместно использующих данные через систему строго контролируемого доступа к общей памяти. Один процессор предназначен для выполнения функции безопасности, а другой — для коммуникации данных. Разделение вычислительных/логических функций и функций коммуникации и прерывания позволяет избежать отрицательного воздействия ошибок при реализации функций коммуникации и прерывания на детерминированное поведение и синхронизацию вычислительных и логических функций. Такое разделение, иногда называемое буферизацией, предназначено для предотвращения распространения ошибок и отказов в коммуникации, источник происхождения которых находится за пределами данной отдельной группы, на процессоры, обеспечивающие выполнение функций безопасности.

7.93. Следует обеспечить, чтобы принимающая система безопасности обрабатывала только предопределенные сообщения.

7.94. К конкретным элементам сообщений, подлежащих предопределению, относятся протокол сообщения, формат сообщения и набор достоверных (допустимых) сообщений.

Независимость коммуникации данных

7.95. Настоящий раздел дополняет рекомендации, изложенные в пунктах 6.25–6.56, в части, касающейся непосредственно коммуникации данных в цифровых системах.

Недопущение отказа по общей причине

7.96. Следует обеспечить, чтобы была спроектирована и реализована топологическая схема сети коммуникации данных и контроля доступа к носителям, позволяющая предотвратить возникновение отказа по общей причине систем безопасности.

Коммуникация между отдельными группами безопасности

7.97. Следует обеспечить, чтобы коммуникация, включая ошибки и отказы в коммуникации, в отдельной группе безопасности не препятствовала присоединенным отдельным группам безопасности в выполнении ими предписанных им функций безопасности.

7.98. Целью рекомендации, изложенной в пункте 7.97, является предотвращение распространения отказов между отдельными группами. Для этого, как правило, применяется сочетание методов валидации данных (см. пункты 7.82–7.94) и буферизации.

7.99. Не следует применять архитектуры с центральным концентратором или маршрутизатором, в которых сообщения от многих отдельных групп безопасности передаются по одной линии.

Коммуникация между системами, относящимися к разным классам безопасности

7.100. Следует обеспечить, чтобы коммуникация данных между цифровыми системами и устройствами, относящимися к разным классам безопасности, соответствовала рекомендациям, изложенным в пунктах 6.25–6.56. Следует обеспечить, чтобы команда на инициирование функции системы защиты имела приоритет при запуске устройства.

Компьютерная безопасность

7.101. В публикации [8] изложены рекомендации, касающиеся вопросов, требований и стратегий осуществления программ по обеспечению компьютерной безопасности (защищенности) на ядерных объектах. Данный раздел дополняет рекомендации, содержащиеся в публикации [8].

Взаимосвязь безопасности и физической безопасности

7.102. В требовании 8 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Меры по обеспечению безопасности, физической ядерной безопасности и механизмы для государственной системы учета и контроля ядерного материала должны разрабатываться и осуществляться на комплексной основе таким образом, чтобы одни не осуществлялись в ущерб другим».

7.103. Следует обеспечить, чтобы функционирование, равно как и отказ любого средства обеспечения компьютерной безопасности отрицательно не влияли на способность системы выполнять предписанные ей функции безопасности. При возникновении коллизии между безопасностью и физической безопасностью следует обеспечить реализацию проектных решений по обеспечению безопасности при условии принятия мер по устранению рисков, связанных с физической безопасностью (защищенностью). Настоятельно не рекомендуется допускать отсутствие мер по обеспечению физической безопасности, и такая ситуация может быть признана допустимой после ее рассмотрения строго на индивидуальной основе и при условии подготовки полного обоснования и проведения анализа рисков, связанных с физической безопасностью.

7.104. Следует обеспечить, чтобы виды отказов средств обеспечения компьютерной безопасности и последствия возникновения этих видов отказа для функций СКУ были известны, задокументированы и учтены при анализе опасностей для системы.

7.105. При использовании средств обеспечения компьютерной безопасности в человеко-машинном интерфейсе следует обеспечить, чтобы они не влияли негативно на возможности операторов в обеспечении безопасности станции.

7.106. Если это практически реализуемо, средства обеспечения физической безопасности, не содействующие также обеспечению безопасности станции, следует предусматривать в отдельных от СКУ устройствах.

7.107. Добавление к СКУ функций по обеспечению физической безопасности усложняет систему и может приводить к появлению потенциальных видов отказов в системе, угрожающих ее способности надежно выполнять предписанную ей функцию безопасности или повышающих вероятность ложного срабатывания.

7.108. Средства компьютерной безопасности, включенные в СКУ, следует разрабатывать в соответствии с рекомендациями раздела 2 настоящего Руководства по безопасности, и следует обеспечить, чтобы они прошли квалификацию на уровне квалификации системы, в которой они размещены.

7.109. Разработку, эксплуатацию и техническое обслуживание цифровых систем или компонентов следует проводить в соответствии с планом обеспечения компьютерной безопасности, в котором указаны и детализируются средства обеспечения компьютерной безопасности.

7.110. В план обеспечения компьютерной безопасности следует включить меры физического, логического и административного контроля, осуществляемые на стадии разработки СКУ.

7.111. При разработке цифровых систем и последующем монтаже, эксплуатации и техническом обслуживании цифровых систем следует обеспечить принятие мер, предотвращающих преднамеренное или непреднамеренное проникновение или повреждение программного обеспечения или данных, введение вредоносного кода, некорректное соединение с внешними сетями и хакерские атаки.

Контроль доступа к цифровым системам, важным для безопасности

7.112. Все соединения с данными для систем или компонентов следует размещать внутри ограждений таким образом, чтобы доступ как к ограждению, так и к пространству внутри ограждения контролировался в соответствии с пунктом 6.156.

7.113. В число подключений к данным входят сетевые подключения, соединения с внешней памятью и устройства доступа к переносным носителям, таким как карты памяти, флеш-карты и диски для хранения данных.

7.114. Неиспользуемые подключения к данным следует блокировать.

7.115. Подключения, необходимые для временного использования, например, соединение с компьютерами для проведения работ по техническому обслуживанию, следует блокировать на период бездействия.

7.116. К методам блокировки неиспользуемых подключений относятся демонтаж, физические меры и логические меры.

7.117. Если для блокировки подключений к данным применяются логические средства, следует предусмотреть дополнительные меры, обеспечивающие сохранение подключения в блокированном состоянии и обнаружение изменений в конфигурации подключения или в его состоянии и оценку влияния этих изменений на работоспособность системы.

7.118. Доступ к функциям, допускающим внесение изменений в программное обеспечение или конфигурационные данные, а также собственно такие изменения следует контролировать и регистрировать.

7.119. Мониторинг и регистрация могут осуществляться автоматически или ручными методами посредством применения административных процедур.

7.120. Следует обеспечить, чтобы использование метода было обосновано и обеспечивало необходимый уровень физической безопасности, не оказывая помех для выполнения функций безопасности.

7.121. Пункты 7.118–7.120 не применяются в случае изменений в конфигурационных параметрах, которые, в соответствии с проектными решениями, могут быть внесены операторами щита управления.

Физическая безопасность коммуникации с противоаварийными службами

7.122. Данные от СКУ на станции могут передаваться на другие объекты, размещенные на площадке станции (например, в центр технической поддержки), а также на объекты, находящиеся за пределами площадки

станции (например, в организации аварийного реагирования) с целью получения поддержки в осуществлении мер аварийного реагирования при условии, что такие подсоединения не будут оказывать негативного воздействия на СКУ.

7.123. Следует обеспечить, чтобы коммуникационные каналы между станцией и центром технической поддержки и между станцией и организацией аварийного реагирования, включая каналы, используемые для обмена информацией между людьми, были специально выделенными для данной цели и защищены от постороннего вмешательства.

7.124. В коммуникационный обмен данными может быть включена информация о состоянии фундаментальных функций безопасности, а также другая информация, требующаяся для поддержки действий по управлению аварийными ситуациями.

Средства обеспечения физической безопасности при эксплуатации

7.125. Для обнаружения угроз компьютерной безопасности и смягчения их последствий следует учесть использование активных средств обеспечения компьютерной безопасности.

7.126. Следует обеспечить, чтобы активные средства обеспечения компьютерной безопасности, предназначенные для защиты СКУ, не оказывали негативного воздействия на функции, важные для безопасности.

7.127. Активные средства обеспечения компьютерной безопасности могут приводить к усложнению системы, конкуренции в использовании системных ресурсов, повышению потенциальной возможности ложного срабатывания или появлению новых видов отказов. Во всех случаях следует учитывать возможность применения пассивных средств обеспечения компьютерной безопасности.

7.128. Желательно применять активные средства обеспечения компьютерной безопасности, только если система находится в автономном режиме (режиме офлайн). Сканирование применительно к СКУ предпочтительно проводить в автономном режиме (режиме офлайн).

7.129. Для компьютерных систем следует предусмотреть периодическую верификацию, а также верификацию, проводимую после технического обслуживания, для подтверждения должной конфигурации и должного функционирования средств обеспечения компьютерной безопасности.

7.130. Следует установить процедуры анализа и принятия мер по результатам, полученным в процессе мониторинга компьютерной безопасности.

Устройства, конфигурированные с использованием языков описания аппаратных средств

7.131. Устройства, конфигурированные с использованием языков описания аппаратных средств, представляют собой программируемые электронные модули, создающие логические структуры (такие как вентильная матрица или переключающая матрица), которые адаптируются разработчиком СКУ для выполнения определенных функций. Программируемые пользователем вентильные матрицы являются типичным примером этого класса.

7.132. Адаптация предполагает использование специальных программных средств для формального описания требований в отношении реализации этих функций.

7.133. Следует обеспечить, чтобы рекомендации данного раздела, касающиеся устройств, конфигурированных с использованием языков описания аппаратных средств, применялись вместе с рекомендациями, изложенными в разделе 2, посвященном жизненному циклу, с рекомендациями данного раздела, касающимися цифровых систем, и рекомендациями, изложенными в разделе 9 относительно программного обеспечения. Эти рекомендации применимы к устройствам, которые непосредственно выполняют функции по обеспечению безопасности.

7.134. Разработку приложений с использованием запрограммированных на аппаратном уровне устройств следует выполнять с учетом заранее определенных характеристик жизненного цикла в соответствии с рекомендациями раздела 2.

7.135. В планах разработки следует предусматривать обоснование применения каждого технического решения таким образом, чтобы оно было понятно третьим сторонам.

7.136. В планах использования запрограммированных на аппаратном уровне устройств следует предусматривать меры, обеспечивающие соответствие каждого изготовленного элемента проектной основе.

7.137. В проектных требованиях к запрограммированным на аппаратном уровне устройствам следует предусматривать требования по синхронизации, например по вентильным задержкам и времени вхождения в режим.

7.138. Следует обеспечить, чтобы процессы подбора запрограммированных на аппаратном уровне устройств и связанных с ними компонентных единиц, таких как библиотеки, блоки интеллектуальной собственности, включаемые в конечный продукт, и языки описания аппаратных средств, были соответственно определены и задокументированы в целях обеспечения их пригодности.

7.139. Блоки интеллектуальной собственности следует использовать только при соблюдении следующих условий:

— используемый блок интеллектуальной собственности следует заказывать у поставщиков, **отвечающих установленным требованиям,** которые при разработке блока интеллектуальной собственности применяют высококачественные технологии производства, включающие строгое соблюдение проектно-технологических процессов, подготовку четко нормированной и полезной документации, а также обеспечение легкости интеграции;
— следует проводить оценки продукта, обеспечивающие исключение появления опасностей.

7.140. Если необходимо внесения изменения в ранее разработанные изделия для обеспечения их приемлемости, такие изменения следует регламентировать, разработать, реализовать и верифицировать до проведения проверки на приемлемость.

7.141. Если выбранное запрограммированное на аппаратном уровне устройство включает вспомогательные средства (например, встроенное самотестирование), пригодность таких устройств для использования при реализации функции безопасности следует устанавливать путем оценки различных элементов, включая оценку процесса их разработки (а также процесса верификации) и проектирования.

7.142. Для программирования устройств, программируемых на аппаратном уровне, следует выбирать стандартизированные языки описания аппаратных средств, включающие квалифицированные (аттестованные) и совместимые программные инструменты.

7.143. Следует предусматривать, чтобы при проектировании запрограммированных на аппаратном уровне устройств:

— обеспечивалось детерминированное поведение запрограммированных на аппаратном уровне устройств. Детерминированность проектирования может быть достигнута, например, за счет применения проектирования с внутренней синхронизацией. Синхронизация проектирования способствует обеспечению корректности (устранению проблем, связанных с метастабильностью) и тестопригодности и позволяет в полной мере использовать программные инструменты для проектирования и верификации;
— использовались лишь запрограммированные на аппаратном уровне устройства, имеющие четко определенные характеристики реализации и поведения. Методы достижения четко определенных характеристик реализации и поведения включают разработку формализованного описания устройства, например, описания на уровне регистровых передач, строгое соблюдение семантических и синтаксических правил, применение «безопасного» подмножества языка описания аппаратных средств, а также использование предопределенных языковых правил и правил кодирования;
— насколько это возможно, поддерживалось использование методов верификации, основанных на доказательстве математических теорем;
— прямо учитывались все возможные случаи логических и эксплуатационных режимов запрограммированных на аппаратном уровне устройств, таких как возврат в исходное состояние, включение питания и нормальная эксплуатация;
— правильно учитывались все возможные варианты изменения характеристик синхронизации, возникающие в результате скачков напряжения источника питания, колебаний температуры и микроэлектронных процессов;
— обеспечивалась тестопригодность каждой функции, реализуемой в запрограммированном на аппаратном уровне устройстве.

7.144. Следует использовать анализ, выполняемый после завершения трассировки, для подтверждения соответствия проекта и реализации устройства технологическим нормам, определенным поставщиком, и согласованности с программными инструментами, используемыми для реализации.

7.145. Процесс проектирования запрограммированных на аппаратном уровне устройств следует включить в общий процесс разработки СКУ.

7.146. Следует обеспечить, чтобы верификация и валидация:

— применялись для подтверждения того, что не была запрограммирована непредусмотренная функция, которая в противном случае могла бы повлиять на функционирование запрограммированного на аппаратном уровне устройства;
— включали проведение испытаний всех путей прохождения сигнала в запрограммированном на аппаратном уровне устройстве;
— охватывали аспекты системы, характерные для запрограммированных на аппаратном уровне устройств;
— включали анализ и моделирование синхронизации.

7.147. Квалификация по условиям окружающей среды и методы анализа следует применять с целью демонстрации того, что использование ранее разработанных изделий или вспомогательных средств не окажет негативного влияния на способность систем, важных для безопасности, осуществлять свои функции по обеспечению безопасности.

ПРОГРАММНЫЕ ИНСТРУМЕНТЫ

7.148. Программные инструменты следует использовать в качестве средств поддержки применительно ко всем аспектам жизненного цикла разработки СКУ, если их использование будет приносить пользу и такие программные инструменты доступны.

7.149. Применение надлежащих программных инструментов может снизить риск возникновения дефектов при разработке СКУ и повысить вероятность обнаружения дефектов при проведении проверок, верификации и валидации. Благодаря этому использование программных инструментов может обеспечить повышение целостности процесса разработки СКУ и, таким образом, повысить уровень надежности

компонентов. Использование программных инструментов может также обеспечить достижение экономического эффекта благодаря сокращению затрат времени и усилий, которые необходимы для изготовления систем, компонентов и программного обеспечения. Программные инструменты могут использоваться для автоматической проверки соблюдения правил конструирования и норм составления надлежащих записей и последовательной документации в стандартных форматах, а также для обеспечения контроля за внесением изменений. Программные инструменты также позволяют сократить объем усилий, требующихся для проведения тестирования, и обеспечить автоматизированное ведение журналов. В некоторых конкретных технологиях разработки требуется использование программных инструментов.

7.150. В число программных инструментов, используемых при разработке СКУ, входят:

— программные инструменты, обеспечивающие наличие инфраструктуры и систем поддержки процесса разработки, таких как системы управления требованиями или интегрированные среды разработки;
— программное обеспечение для автоматизированного планирования цепей и кабельных трасс;
— трансформационные программные инструменты, такие как генераторы кодов, компиляторы, синтезаторы логики и средства, трансформирующие текст или схемы из одного уровня абстракции в другой, обычно более низкий уровень абстракции;
— программные инструменты для автоматизации проектирования электроники;
— программные инструменты для верификации и валидации, такие как статические анализаторы кодов, автоматизированные тестеры схем, мониторы тестового покрытия, ассистенты для доказательства теорем, симуляторы электронных схем и симуляторы станционных систем;
— программные инструменты для подготовки конфигурационных данных систем;
— программные инструменты для конфигурационного управления и контроля;
— программные инструменты для тестирования физической безопасности в целях выявления известных и неизвестных уязвимостей.

7.151. Ключевым элементом интегрированной среды поддержки проектирования является обеспечении надлежащего контроля и согласованности. В случае отсутствия готовых программных инструментов следует рассмотреть возможность разработки новых программных инструментов.

7.152. Преимущества и риски в случае использования программных инструментов следует сопоставлять с преимуществами и рисками, связанными с отказом от использования программных инструментов.

7.153. Важно, чтобы применяемый подход обеспечил выбор программных инструментов, ограничивающих возможность появления ошибок и дефектов, одновременно в максимальной степени расширяя возможности предотвращения или обнаружения дефектов. Использование программных инструментов может по-разному негативно влиять на процесс разработки систем. Например, применение программных инструментов при проектировании может привести к привнесению дефектов из-за появления искаженных выходных данных, или же верификационные инструменты могут не обеспечить выявления некоторых дефектов или типов дефектов.

7.154. Программные инструменты следует подбирать с расчетом на то, что они будут оставаться доступными на протяжении всего срока службы системы и будут совместимы с другими программными инструментами, используемыми при разработке систем.

7.155. Следует обеспечить, чтобы данные о функциональности и ограничениях применимости всех программных инструментов были определены и задокументированы.

7.156. Программные инструменты и получаемые от них выходные данные не следует применять вне заявленной функциональности или пределов применимости без предварительного обоснования.

7.157. Например, программные инструменты не могут заменить человека при необходимости вынесения экспертной оценки. В некоторых случаях поддержка, обеспечиваемая программными инструментами, является более подходящим методом, чем полная автоматизация процесса.

7.158. Программные инструменты следует верифицировать и оценивать с учетом требований по надежности данного программного инструмента, типа программного инструмента, потенциала программного инструмента

привносить дефекты или терять способность извещать пользователя о существующих дефектах, а также с учетом степени, в которой данный программный инструмент может оказывать воздействие на резервируемые элементы системы или на неодинаковые (диверсные) системы.

7.159. Примеры ситуаций, в которых объем проведения верификации и оценки может зависеть от конкретных обстоятельств, приводятся ниже:

— верификацию программных инструментов, способных привносить дефекты, следует проводить в большем объеме, чем в случае программных инструментов, у которых не было подтверждено наличия такой способности;
— верификацию программных инструментов, которые могут терять способность извещать пользователя о существующих дефектах, следует проводить в большем объеме, чем в случае программных инструментов, у которых не было обнаружено такой способности;
— верификация программных инструментов не является обязательной, если выходные данные программного инструмента подвергаются систематической и независимой верификации;
— меньшая строгость при верификации программных инструментов допустима, если обеспечивается смягчение последствий любых потенциальных дефектов, привносимых программными инструментами (например, посредством применения принципа неодинаковости или проектными мерами в системе).

7.160. При верификации и оценке программных инструментов следует учитывать опыт их предыдущего использования, включая опыт разработчиков и опыт, приобретенный в результате осуществления процессов, в которых эти программные инструменты применялись.

7.161. Процесс подбора, верификации и оценки программных инструментов следует обосновывать и документировать.

7.162. Конфигурационное управление следует применять ко всем программным инструментам.

7.163. Настройки программных инструментов, применяемые в процессе разработки, верификации или валидации базового оборудования, программных и аппаратных устройств, для которых применяется язык описания аппаратных средств, следует регистрировать в документации процесса разработки.

7.164. Такая документация полезна не только для обеспечения согласованности конечных программных средств; она также помогает в оценке происхождения дефекта, источником которого может быть исходный код, программный инструмент или настройки программных инструментов. Информация о применяемой настройке инструментов может быть чрезвычайно важной для оценки потенциала возникновения отказов по общей причине, обусловленных программными инструментами.

КВАЛИФИКАЦИЯ ПРОМЫШЛЕННЫХ ЦИФРОВЫХ УСТРОЙСТВ ОГРАНИЧЕННОЙ ФУНКЦИОНАЛЬНОСТИ ДЛЯ ПРИМЕНЕНИЯ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

7.165. Данный раздел содержит рекомендации по квалификации промышленных цифровых устройств ограниченной функциональности, используемых в системах безопасности атомной электростанции, которые не были специально разработаны для таких применений. Эти рекомендации содержат описание подхода, направленного на выполнение рекомендаций по квалификации, изложенных в пунктах 6.78–6.134 применительно к устройствам этой категории.

7.166. Устройство ограниченной функциональности имеет следующие характеристики:

— оно содержит ранее разработанные программные средства или программируемую логику;
— оно работает автономно и выполняет одну концептуально простую главную функцию, которую определяет изготовитель и которая не может быть изменена пользователем;
— оно не может быть перепрограммировано;
— если возможно проведение реконфигурации, его конфигурируемость ограничивается параметрами, зависящими от совместимости с подлежащим мониторингу или контролю процессом, или взаимосвязями с подключенным оборудованием.

7.167. Все остальные устройства не являются «промышленными цифровыми устройствами ограниченной функциональности», т.е. имеют следующие характеристики:

— в их составе используются коммерческие компьютеры (например, персональные компьютеры, промышленные компьютеры или программируемые логические контроллеры);
— они разработаны для платформы СКУ; или
— они разработаны специально для использования в атомной отрасли.

7.168. Следует обеспечить, чтобы подтверждение пригодности и корректности промышленных цифровых устройств ограниченной функциональности для выполнения отведенных им функций свидетельствовало о том, что:

— главные функции устройства соответствуют функциональным требованиям к их применению;
— срабатывание либо отказ в срабатывании функций, отличных от главных функций[37], не может угрожать безопасному выполнению главных функций;
— устройство не подвержено появлению систематических дефектов, которые могут с определенной вероятностью вызвать практически одновременный отказ по общей причине, если аналогичные устройства установлены в элементах систем СКУ, которые являются резервируемыми или неодинаковыми;
— процесс разработки осуществлялся системно и в соответствии с основными положениями раздела 2 настоящего Руководства по безопасности;
— обеспечение качества при изготовлении является достаточным основанием для приемки точно таких же или аналогичных моделей устройства, которые будут изготовлены позже.

7.169. Информация, полученная в процессе сертификации в целях обеспечения безопасности в других отраслях, может быть использована для подтверждения квалификации устройства. Наличия только сертификата недостаточно; более ценной может быть полученная в процессе сертификации информация.

---

[37] В число функций, отличных от главных функций, входят, например, функции, предназначенные для поддержания работоспособности или для конфигурирования устройства, и функции, не являющиеся необходимыми для данного целевого применения.

7.170. В случае невыполнения одной или нескольких из приведенных выше рекомендаций следует получить компенсирующие доказательства, которые прямо устраняют пробелы в подтверждении пригодности и корректности.

7.171. Следует обеспечить, чтобы такие компенсирующие доказательства:

— прямо касались требований, выполнение которых они должны подтверждать;
— были признаны применимыми к данному устройству.

7.172. Примеры методов получения компенсирующих доказательств включают:

— выполнение дополнительных задач, специфических для данного устройства, которые соответствуют предусматриваемому применению и другим элементам доказательств корректности;
— оценку применимого и достоверного опыта эксплуатации;
— верификацию проектных результатов;
— статистические испытания.

7.173. Пользователи могут конфигурировать устройства в соответствии с их предназначением. Следует обеспечить, чтобы такие изменения соответствовали критериям настоящего Руководства по безопасности, касающимся корректности проектирования и документации, и не приводили к денонсированию предыдущего опыта эксплуатации или результатов испытаний, которые учитывались при квалификации.

7.174. Следует определить ограничения, которые должны соблюдаться для безопасного использования устройства по назначению.

7.175. Такие ограничения, например, включают:

— ограничения применений, для которых устройство было квалифицировано (аттестовано);
— конкретные опции и неиспользуемые функции, которые будут включаться или отключаться;
— ограничения на окружающие условия эксплуатации или срок службы;
— меры, которые должны соблюдаться при эксплуатации, испытаниях и техническом обслуживании.

8. АСПЕКТЫ, СВЯЗАННЫЕ С ЧЕЛОВЕКО-МАШИННЫМ ИНТЕРФЕЙСОМ

ПУНКТЫ УПРАВЛЕНИЯ

Главный щит управления

8.1. В требовании 65 публикации SSR-2/1 (Rev. 1) [1] указано:

> «На АЭС должно быть предусмотрено помещение щита управления, из которого можно было бы безопасно управлять станцией во всех эксплуатационных состояниях как в автоматическом, так и в ручном режиме, и из которого можно было бы принимать меры по поддержанию безопасного состояния станции или по возвращению ее в безопасное состояние после возникновения ожидаемых при эксплуатации событий или аварийных условий».

8.2. В требовании 59 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Должны быть предусмотрены контрольно-измерительные приборы для определения значений всех основных параметров, от которых могут зависеть процесс деления, целостность активной зоны реактора, систем теплоносителя реактора и защитной оболочки на АЭС, для получения важной информации о станции, которая необходима для ее безопасной и надежной эксплуатации, для определения состояния станции в аварийных условиях и для принятия решений в целях управления аварией».

8.3. Пункт 5.57 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Оператор должен получать информацию, необходимую для:
> a) оценки общего состояния станции в любых условиях;
> b) эксплуатации станции в установленных пределах для параметров, связанных с системами и оборудованием станции (эксплуатационные пределы и условия);
> c) подтверждения автоматического инициирования срабатывания систем безопасности, когда это необходимо, и надлежащей работы соответствующих систем;

d) определения как необходимости ручного инициирования указанных действий по обеспечению безопасности, так и времени такого инициирования».

8.4. Следует обеспечить, чтобы СКУ позволяли операторам в пункте управления включать или переходить на ручное управление каждой из функций, необходимых для управления станцией и поддержания безопасности.

8.5. В помещении пункта управления следует предусмотреть достаточное количество экранов для мониторинга всех функций, важных для безопасности, в том числе для контроля состояния станции, статуса ее безопасности и динамики ключевых параметров станции.

8.6. Следует предусмотреть индикацию и средства управления, классифицируемые по безопасности, для выполнения аварийных эксплуатационных процедур и руководств по управлению тяжелыми авариями.

8.7. Рекомендация, изложенная в пункте 8.6, не направлена на исключение возможности использования других средств, подходящих для реализации целей применения аварийных эксплуатационных процедур и руководств по управлению тяжелыми авариями.

8.8. Следует обеспечить, чтобы в случае отказа или преднамеренного отключения системы или части системы, функционирование которой требуется для управления станцией и поддержания безопасности, такое состояние отображалось в пункте управления, а также в местах, в которых требуется доведение этой информации до сведения операторов.

8.9. Следует предусмотреть оповещение о любых изменениях в состоянии систем безопасности и отображение информации о состоянии в местах, в которых она требуется операторам.

8.10. К изменениям в состоянии систем, требующим подачи предупредительного сигнала, могут относиться отклонения от нормальных эксплуатационных пределов, потеря эксплуатационной готовности систем безопасности или неготовность резервного оборудования вследствие возникновения отказа, проведения технического обслуживания или испытаний.

8.11. Прогресс в расширении функциональности систем сигнализации позволил обеспечить реализацию таких необходимых функций, как обработка предупредительных сигналов, приоритизация предупредительных сигналов и контроль и управление, применяемые в отношении предупредительных сигналов, и эти функции помогают операторам эффективно осуществлять мониторинг событий на станции и реагировать на них.

8.12. Помещения главного щита управления и дополнительного щита управления следует проектировать так, чтобы никакие пожары, внутренние опасности или постулируемые исходные события не могли помешать операторам выполнять фундаментальные функции безопасности.

Дополнительный щит управления

8.13. В требовании 66 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Контрольно-измерительные приборы и оборудование для управления должны быть размещены предпочтительно в одном помещении (помещении дополнительного щита управления), физически, электрически и функционально отделенном от основного помещения щита управления АЭС. Помещение дополнительного щита управления должно быть оборудовано таким образом, чтобы можно было остановить реактор и поддерживать его в этом состоянии, отводить остаточное тепло и контролировать важнейшие параметры станции, если будет утрачена возможность осуществлять эти важнейшие функции безопасности из помещения основного щита управления».

8.14. В некоторых проектах станции может быть предусмотрено наличие более чем одного дополнительного щита управления или дополнительных пунктов управления, располагающихся вне помещения дополнительного щита управления.

8.15. В помещениях дополнительных щитов управления следует предусмотреть информационные табло для мониторинга условий на станции, необходимого для обеспечения реагирования на события, которые могут возникнуть вследствие ситуаций, в которых требуется эвакуация персонала из помещения главного щита управления.

8.16. В помещении дополнительного щита управления следует предусмотреть средства управления, средства индикации, средства сигнализации и табло, наличие которых будет достаточно для того, чтобы оператор мог привести станцию в безопасное состояние, убедиться в том, что станция приведена в безопасное состояние и поддерживается в этом состоянии, а также осуществлять мониторинг состояния станции и динамики ключевых параметров станции.

8.17. В случае, когда не представляется практически возможным обеспечить наличие в помещении дополнительного щита управления всех средств управления, необходимых для выполнения рекомендации, изложенной в пункте 8.16, могут использоваться средства управления, размещенные в локальных пунктах управления.

8.18. Следует предусмотреть средства, находящиеся вне помещения главного щита управления, позволяющие переносить приоритетное управление на новое место в случае, когда персонал покидает помещение главного щита управления.

АВАРИЙНЫЙ МОНИТОРИНГ

8.19. Пункт 6.31 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Должны предусматриваться контрольно-измерительные приборы и регистрирующие устройства, которые обеспечивают получение важной информации для контроля состояния важного оборудования и развития аварий, для прогнозирования местонахождения выбросов и объемов радиоактивного материала, который мог быть выброшен с объектов, предусмотренных для этой цели в проекте, и для послеаварийного анализа».

8.20. Следует обеспечить наличие на станции информационных табло для мониторинга аварийных условий на станции и отображения соответствующей информации в надлежащих местах (например, на главном щите управления или на дополнительных щитах управления) в соответствии с должностными функциями и обязанностями эксплуатационного персонала.

8.21. Набор табло для мониторинга аварийных условий обычно называется «системой аварийного мониторинга» или «системой мониторинга послеаварийной ситуации». Такие табло могут предусматриваться как часть какой-либо другой системы или могут быть агрегацией отдельных измерительных каналов.

8.22. Следует обеспечить, чтобы система аварийного мониторинга отображала значения переменных параметров, которые необходимы операторам станции в аварийных условиях, чтобы обеспечить им возможность:

a) предпринять заранее запланированные действия в ручном режиме с целью приведения станции в безопасное состояние;
b) установить факт выполнения фундаментальных функций безопасности;
c) определить потенциальную возможность разрушения или возникшее разрушение барьеров, предотвращающих выброс продуктов деления (например, разрушения оболочек твэлов, границы контура теплоносителя и защитной оболочки реактора);
d) определить состояние и эксплуатационные характеристики станционных систем, необходимых для ликвидации последствий, возникающих в случае проектных аварий и запроектных условий, и приведения станции в безопасное состояние;
e) определить необходимость принятия мер для защиты населения от выброса радиоактивных веществ;
f) применять на станции руководства по управлению тяжелой аварией.

8.23. Контрольно-измерительные приборы, выполняющие функции индикации, перечисленные в подпунктах (a)–(d) пункта 8.22, следует классифицировать как средства обеспечения безопасности, и следует предусматривать их наличие в оборудовании СКУ, способном функционировать во время проектных аварий и в запроектных условиях.

8.24. Классификация в качестве «системы безопасности» обусловливает необходимость применения в полном объеме критериев, изложенных в разделе 6, включая критерий единичного отказа для групп безопасности.

8.25. Следует обеспечить, чтобы контрольно-измерительные приборы для мониторинга тяжелых аварий были спроектированы и квалифицированы для всего спектра ожидаемых рабочих условий.

8.26. Не всегда представляется возможным провести полные типовые испытания контрольно-измерительных приборов, предназначенных для мониторинга тяжелых аварий, в наихудших вероятных условиях, которые могут возникнуть. В таких случаях испытания могут быть дополнены другими методами, включая (но не ограничиваясь ими) методы, описанные в пункте 6.82.

8.27. Следует обеспечить, чтобы функции аварийного мониторинга, способствующие применению руководств по управлению тяжелыми авариями:

a) не отключались в связи с работой, отказом или неправильным функционированием оборудования СКУ, которое не является частью аппаратуры для мониторинга тяжелых аварий;
b) не были зависимыми от внешнего энергоснабжения, либо для них в проекте была обеспечена возможность получения питания от источников, не относящихся к системе электроснабжения станции.

8.28. Для случаев, когда отказ в одном канале отображения информации, поступающей от контрольно-измерительных приборов, который выполняет функции, указанные в подпунктах (a)–(c) и (f) пункта 8.22, может привести к отображению неоднозначной информации, следует предусмотреть средства, позволяющие операторам устранить появившуюся неоднозначность.

8.29. Отказ в канале отображения информации может привести к различиям в данных, отображаемых парой резервированных табло. К средствам устранения неоднозначности относится использование дополнительных каналов или процедур с целью сопоставления неоднозначных показаний с другим параметром, соотношение которого с рассматриваемым показанием известно.

8.30. Следует обеспечить, чтобы контрольно-измерительные приборы для аварийного мониторинга охватывали весь диапазон значений параметров, которые могут регистрироваться в аварийных условиях.

8.31. Следует обеспечить, чтобы табло, отображающие данные аварийного мониторинга, были легко распознаваемыми в качестве таковых.

8.32. Следует предусмотреть электронные средства поддержки операторов (например, «систему отображения параметров безопасности»), чтобы операторы могли быстро определить состояние станции, убедиться в том,

что каналы аварийного мониторинга работают, проверить достоверность поступающих по ним показаний и определить значение показателей, косвенно измеряемых на основе прямых измерений.

8.33. Применение автоматизированных с помощью компьютеров средства поддержки операторов способствует повышению безопасности и обеспечивает большую уверенность в том, что предпринимаемые меры являются корректными.

8.34. При проектировании современных щитов управления система отображения параметров безопасности и функции системы аварийного мониторинга часто интегрируются в стандартный человеко-машинный интерфейс оператора. Сферу действия рекомендаций можно ограничить конкретными действиями или аварийными сценариями, или же она может охватывать все виды деятельности, включая пуско-наладку и ситуации при нормальной эксплуатации.

8.35. Для контрольно-измерительных приборов, выполняющих функции индикации, перечисленные в подпунктах (a)–(c) и (f) пункта 8.22, следует предусмотреть также наличие средств поддержки оператора, не зависящих от источника питания.

СИСТЕМЫ СВЯЗИ ОПЕРАТОРОВ

8.36. В требовании 37 публикации SSR-2/1 (Rev. 1) [1] указано:

> «На всех участках АЭС должны предусматриваться эффективные средства связи, которые облегчают безопасную эксплуатацию во всех режимах нормальной эксплуатации и могут быть использованы после возникновения любых постулируемых исходных событий и в аварийных условиях».

8.37. Пункт 5.66 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Должны предусматриваться соответствующие системы сигнализации и средства связи с таким расчетом, чтобы в эксплуатационных состояниях и аварийных условиях можно было предупредить об опасности всех лиц, находящихся на АЭС и на площадке, и дать им соответствующие инструкции».

8.38. Пункт 5.67 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Должны предусматриваться соответствующие и неодинаковые средства связи, требующиеся для обеспечения безопасности, внутри атомной электростанции и в непосредственной близости от станции, а также для связи с соответствующими учреждениями за пределами площадки».

8.39. Следует предусматривать системы связи для эксплуатационного персонала с целью обеспечения надежной коммуникации как на станции, так и за ее пределами без необходимости для операторов покидать местонахождение СКУ, мониторинг и контроль которых они обязаны осуществлять.

8.40. Следует обеспечить, чтобы системы, которыми снабжается эксплуатирующий персонал для коммуникации друг с другом и противоаварийными службами за пределами площадки станции, не могли быть выведены из строя индивидуальными средствами защиты, постулируемыми исходными событиями или единичными злоумышленными действиями.

8.41. Следует обеспечить, чтобы характеристики оборудования СКУ не создавали препятствий для коммуникации эксплуатирующего персонала.

8.42. Например, если оборудование СКУ создает помехи для работы средств радиосвязи, средства радиосвязи создают помехи для работы оборудования СКУ или индивидуальные средства защиты препятствуют использованию телефонов, может требоваться применение других видов связи.

8.43. Для главного щита управления, дополнительного щита управления и центра технической поддержки следует предусматривать по меньшей мере два неодинаковых метода связи:

a) с помещениями, в которых необходимо иметь средства связи во время ожидаемых при эксплуатации событий или в аварийных условиях;
b) со службами противоаварийного реагирования, такими как центр технической поддержки и организация противоаварийного реагирования;

c) со смежными объектами[38].

8.44. Примерами неодинаковых средств связи являются электронная почта, передача данных, факсимильная связь, каналы видеосвязи, стационарная проводная телефонная связь, спутниковые и сотовые телефоны, а также портативные радиостанции.

8.45. Следует обеспечить, чтобы неодинаковые каналы связи, упомянутые в пунктах 8.43 и 8.44:

a) были спроектированы так, чтобы на их работу не могли повлиять один и тот же отказ, внешняя угроза, внутренняя угроза или постулируемое исходное событие;
b) были в состоянии функционировать независимо как от станционных систем энергоснабжения, так и от систем энергоснабжения вне площадки станции.

8.46. Следует предусмотреть системы связи, предназначенные для передачи объявлений, адресованных всему персоналу на площадке и на станции.

ОБЩИЕ ПРИНЦИПЫ, СВЯЗАННЫЕ С УЧЕТОМ ЧЕЛОВЕЧЕСКОГО ФАКТОРА ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ КОНТРОЛЯ И УПРАВЛЕНИЯ

8.47. В требовании 32 публикации SSR-2/1 (Rev. 1) [1] указано:

> «На ранней стадии разработки проекта АЭС в процесс проектирования должен включаться систематический учет человеческих факторов, в том числе взаимодействия человек-машина, который должен проводиться в течение всего процесса проектирования».

8.48. Пункт 5.55 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Проект должен способствовать выполнению эксплуатационным персоналом его обязанностей и задач и должен ограничивать вероятность возникновения ошибок и их влияние во время

[38] К смежным объектам относятся другие объекты, на которые может повлиять эксплуатация энергоблоков атомной электростанции (например, другие энергоблоки на одной и той же площадке).

эксплуатации на безопасность. В процессе проектирования должно уделяться должное внимание планировке станции, компоновке оборудования и процедурам, включая процедуры технического обслуживания и инспектирования, с целью облегчения взаимодействия эксплуатационного персонала и станции во всех эксплуатационных состояниях».

8.49. Пункт 5.56 публикации SSR-2/1 (Rev. 1) [1] гласит:

«Взаимодействие человек-машина должно проектироваться с таким расчетом, чтобы операторы получали всеобъемлющую, но легко поддающуюся управлению информацию, с учетом времени, необходимого для принятия решений и соответствующих действий. Информация, необходимая оператору для принятия решения о действиях, должна быть представлена в ясной и недвусмысленной форме».

8.50. При проектировании человеко-машинного интерфейса следует использовать позитивные решения, примененные в образцовых проектах, и избегать проблем, которые приводили неудовлетворительному опыту эксплуатации.

8.51. При проектировании человеко-машинного интерфейса, требующегося для управления системами безопасности в супервизорном режиме, следует применять принципы глубокоэшелонированной защиты.

8.52. Следует обеспечить, чтобы СКУ предоставляла операторам информацию, необходимую для выявления изменений в состоянии системы, диагностики ситуации, управления работой системы (при необходимости) и верификации ручных и автоматических действий.

8.53. В удовлетворительно разработанном проекте учитываются когнитивные возможности обработки данных операторами, а также временные ограничения, связанные с процессами.

8.54. При проектировании следует обеспечить, чтобы максимальный промежуток времени между моментом задействования средства управления и приемом входного сигнала системой управления был приемлемым для операторов.

8.55. При проектировании СКУ следует обеспечить, чтобы стоящие перед операторами задачи могли выполняться в течение периода времени, установленного требованиями к системе.

8.56. Слишком быстрая или слишком медленная скорость информационного потока и реакции системы управления могут привести к ухудшению исполнения операторами своих функций.

8.57. По мере возможности СКУ следует проектировать так, чтобы эта система предупреждала и выявляла ошибки операторов, в случае которых может быть предпринято действие в неверном контексте или при неверной конфигурации оборудования. К таким проектным мерам относятся валидация изменений уставок для систем управления, мониторинга и защиты.

8.58. Следует обеспечить, чтобы СКУ выдавала простые и хорошо понятные предупреждения о ошибках операторов, которые могут быть выявлены, а также информацию о доступных простых и эффективных методах их исправления.

8.59. Следует обеспечить, чтобы никакая единичная ошибка оператора не могла привести к потере управления реактором.

8.60. Следует обеспечить, чтобы человеко-машинный интерфейс:

a) насколько это практически возможно, охватывал различные функции и обязанности эксплуатационного персонала разной специализации, который будут взаимодействовать с системами;
b) был разработан прежде всего с учетом функций оператора, ответственного за безопасную эксплуатацию оборудования;
c) поддерживал обеспечение информированности персонала пункта управления об общей ситуации, например, посредством настенных экранов, отображающих информацию о состоянии станции;
d) обеспечивал эффективный обзор состояния станции;
e) насколько это практически возможно, был максимально простым и соответствовал требованиям в отношении функций и решаемых задач;
f) был рассчитан на минимизацию обучения операторов его использованию;

g) представлял информацию так, чтобы операторы могли оперативно ее получать и воспринимать[39];
h) допускал отказ аналоговых индикаторов и электронных табло без существенного прерывания действий по управлению;
i) учитывал физиологические особенности человека[40], особенности моторики человека и антропометрические факторы.

8.61. Следует обеспечить, чтобы человеко-машинный интерфейс, процедуры, системы обучения и процессы обучения были согласованы друг с другом.

8.62. Представление информации следует интегрировать так, чтобы полученная при этом компоновка была гармонично организованной и позволяла обеспечить оптимальное понимание операторами текущего состояния станции и выполнение действий, необходимых для управления станцией.

8.63. Следует обеспечить, чтобы функционирование и внешний вид человеко-машинного интерфейса были единообразными во всех местах его расположения и на всех платформах, где отображается информация и откуда ведется управление, и характеризовались высокой степенью стандартизации.

8.64. Следует учесть необходимость использования единых формулировок и совместимого текста для всех имеющих описательный характер идентифицирующих обозначений и маркировок.

8.65. Следует обеспечить, чтобы во всех своих аспектах СКУ (включая средства управления и компоновку информационных табло) соответствовала имеющимся у операторов ментальным моделям и общепринятым нормам.

---

[39] Отображение информации в простой для понимания форме снижает когнитивную нагрузку оператора. Человеко-машинный интерфейс, спроектированный в соответствии с данной рекомендации, например, позволяет свести к минимуму необходимость выполнения операторами вычислений в уме и воспроизведения информацию по памяти.

[40] К физиологическим особенностям человека относятся, например, особенности визуального или слухового восприятия и биомеханика (досягаемость и возможность движений).

8.66. Под ментальными моделями подразумеваются представления у операторов о характеристиках поведения системы и ожидания относительно таких характеристик. Такие модели приобретаются в результате обучения, использования процедур и по мере накопления опыта.

8.67. Правила обозначения для каждого типа средств управления и индикации устанавливаются при проектировании и затем применяются повсеместно в идентифицирующих обозначениях, на схемах и в местах расположения средств управления и на табло, отображающих информацию об условиях на станции.

Аспекты взаимодействия человека и автоматики

8.68. Следует обеспечить, чтобы методология определения надлежащего распределения функций СКУ между человеком и СКУ была системной и применялась последовательным образом.

8.69. К факторам, которые могут повлиять на распределение функций между человеком и машиной, относятся:

— потенциальная рабочая нагрузка человека при всех режимах эксплуатации;
— требования к точности и воспроизводимости;
— временные факторы;
— типы и уровень сложности процесса принятия решений и необходимой логики действий;
— факторы окружающей среды;
— физиологические и антропометрические особенности человека.

8.70. Пункт 5.59 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Необходимость быстрого вмешательства оператора должна быть сведена к минимуму, и должно быть продемонстрировано, что оператор располагает достаточным временем для принятия решения о действиях и осуществления действий».

8.71. Следует предусмотреть, чтобы СКУ обеспечивали выполнение автоматических действий в случаях, когда операторы не способны надежно и своевременно выполнить действие в ручном режиме или когда применение ручного управления создает чрезмерную нагрузку для оператора.

8.72. Следует обеспечить, чтобы СКУ снабжала операторов информацией, необходимой для мониторинга каждой автоматической функции.

8.73. В СКУ следует предусмотреть наличие для операторов множественных средств верификации автоматических действий.

8.74. Следует обеспечить, чтобы информация, предназначенная для мониторинга действий, выполняемых автоматически, отображалась со скоростью и уровнем детализации (например, с указанием целей или задач, или же способов верификации), при которых оператор может эффективно контролировать такие действия.

8.75. Следует обеспечить, чтобы СКУ позволяла операторам осуществлять вручную инициирование или управление каждой из функций, необходимых для управления станцией и поддержания безопасности.

Разработки задач применительно к системам контроля и управления

8.76. Следует обеспечить, чтобы в рамках своих обязанностей оператор разработал адресные и предметные задачи, выполнение которых позволит поддерживать информированность персонала о текущем состояния станции и уровень рабочей нагрузки, негативно не отражающийся на работоспособности персонала и в то же время являющийся достаточным для сохранения постоянной бдительности.

8.77. В СКУ следует обеспечить наличие всех характеристик, которые были определены как необходимые в результате проведения анализа задач.

8.78. При проведении анализа задач следует рассматривать все состояния станции, все режимы эксплуатации станции и все группы эксплуатационного персонала (включающие, например, оператора реактора, оператора турбины, начальника смены, оператора, выполняющего действия по управлению вне главного щита управления, инженера по безопасности, а также эксплуатационный персонал и персонал, выполняющий работы по техническому обслуживанию). Следует обеспечить, чтобы анализ задач позволил получить проектные данные для таких характеристик СКУ, как безошибочность и точность отображаемой информации; время реакции системы; расположение оборудования; тип средств управления, табло и средств сигнализации; интеграцию «мягких» средств контроля в информационные табло.

8.79. Следует обеспечить, чтобы человеко-машинный интерфейс допускал возможность форматирования средств индикации и управления на видеодисплейных терминалах в конфигурации, являющиеся наиболее удобными для выполнения конкретной задачи, если это будет способствовать выполнению поставленных задач.

8.80. Такая возможность конфигурирования может оказаться полезной, например, в случае, когда использование разных конфигураций позволяет лучше учесть различный уровень опыта операторов или когда применение изменяемых схем конфигурации оказывается более эффективным при работе в разных режимах эксплуатации.

8.81. Следует обеспечить, чтобы все характеристики человеко-машинного интерфейса (форматы, терминология, установление последовательности, группирование и средства поддержки принятии решений для оператора) имели очевидную логику, основанную на условиях задач или другом непроизвольном обосновании.

8.82. Следует обеспечить наличие четкой взаимосвязи между каждым табло, средством управления и средством поддержки обработки данных и соответствующими задачами и функциями.

8.83. Следует обеспечить, чтобы человеко-машинный интерфейс снабжал операторов информацией в форме и формате, которые соответствуют результатам анализа задач.

8.84. В СКУ следует предусматривать варианты управления, охватывающие все возможные действия оператора, которые были определены в анализе задач.

8.85. В СКУ следует предусматривать для операторов множественные средства для выполнения действий.

8.86. Следует обеспечить, чтобы СКУ позволяла операторам выполнять задачи с минимальным количеством действий.

Положения, касающиеся доступности и условий работы

8.87. Пункт 5.61 публикации SSR-2/1 (Rev. 1) [1] гласит: «Рабочие места и условия работы эксплуатационного персонала должны проектироваться в соответствии с концепциями эргономики».

8.88. В зонах, в которых эксплуатационный персонал должен осуществлять мониторинг и управление станционными системами, следует обеспечить необходимые условия для работы и защиту персонала от воздействия опасных факторов.

8.89. К учитываемым стандартным условиям работы относятся освещение, температура, влажность, уровень шума и вибрации, а также наличие помещений для отдыха и душевых в случаях, когда требуется постоянный мониторинг.

8.90. К учитываемым опасностям относятся радиация, дым, а также выбросы токсичных веществ в атмосферу.

8.91. Пункт 5.60 публикации SSR-2/1 (Rev. 1) [1] гласит:

> «Проект должен быть составлен с таким расчетом, чтобы после события, воздействующего на станцию, условия окружающей среды в помещении щита управления или дополнительном помещении щита управления, а также в местах на пути доступа к этому дополнительному щиту управления не угрожали защите и безопасности эксплуатационного персонала».

8.92. Если рабочие станции человеко-машинного интерфейса распределены по объекту[41], следует обеспечить, чтобы эксплуатационный персонал имел своевременный и безопасный доступ к соответствующим разным местам их расположения.

8.93. Один из способов обеспечения подходящих условий доступа является прокладка отвечающего установленным требованиям маршрута к дополнительным щитам управления и другим местам вне главного щита управления, где операторы могут осуществлять необходимые действия, с принятием соответствующих мер для защиты от потенциальных внутренних и внешних опасностей.

---

[41] К примерам распределенных по объекту рабочих станций человеко-машинных интерфейсов относятся дополнительный щит управления и другие места, находящиеся вне главного щита управления, где операторы могут осуществлять необходимые действия.

РЕГИСТРАЦИЯ ИСТОРИЧЕСКИХ ДАННЫХ

8.94. Человеко-машинный интерфейс следует проектировать так, чтобы он обеспечивал возможность записи, хранения и отображения исторической информации в тех случаях, когда такая информация будет помогать эксплуатационному персоналу в выявлении закономерностей и тенденций, понимании прошлого или текущего состояния системы, проведении послеаварийного анализа или прогнозировании будущих последовательностей событий.

9. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

ОБЩИЕ ПОЛОЖЕНИЯ

9.1. Рекомендации, изложенные в данном разделе, относятся ко всем типам программного обеспечения, применяемого в оборудовании СКУ, важном для безопасности, или в связи с ним, например, операционным системам, ранее разработанному программному обеспечению или аппаратно-программному обеспечению, программным средствам, специально разрабатываемым для данного проекта, или программным средствам, разрабатываемым на основе существующих семейств аппаратных или программных модулей.

9.2. Цифровые системы требуют различных подходов к оценке надежности по сравнению с аналоговыми системами. Надежность определяется оценкой качества производственных операций и результатами верификации и валидации. Программное обеспечение в силу своего характера и предназначения допускает более значительную свободу в выборе проектных параметров, чем аппаратные средства (электрические или механические). Если в программные средства систематически не вводить ограничения, они могут стать предрасположенными к появлению дефектов и не поддающимися верификации. Усложнение программного обеспечения может обусловливать появление дополнительных дефектов в конструкции, затруднять их обнаружение и устранение, приводить к формированию видов и последствий отказов, отсутствующих в более простых конструкциях, а также снижать достоверность демонстрации соответствия таким критериям проектирования системы безопасности, как независимость, тестопригодность и надежность.

9.3. Рекомендации по системам менеджмента и процессам жизненного цикла, изложенные в разделе 2, имеют особенно важное значение в случае программного обеспечения, поскольку процессы, о которых идет речь в этом разделе, являются неотъемлемой частью эффективной разработки программного обеспечения.

9.4. В требовании 63 публикации SSR-2/1 (Rev. 1) [1] указано:

> «Если система, важная для безопасности на атомной электростанции, зависит от компьютеризированного оборудования, то должны быть установлены и осуществляться в течение всего срока эксплуатации этой системы, в особенности на стадии разработки программного обеспечения, надлежащие нормы и практика разработки и испытания компьютерных аппаратных средств и программного обеспечения. Весь процесс разработки должен осуществляться в рамках системы менеджмента качества».

9.5. Разработку программного обеспечения для систем следует выполнять в рамках заранее определенного жизненного цикла, должным образом планировать и документально оформлять, а также следует предусматривать их верификацию и валидацию (см. раздел 2).

ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

9.6. Следует обеспечить, чтобы для всех программных средств, которые должны соответствовать требованиям СКУ, включая повторно использованный или автоматически сгенерированный код, имелись задокументированные в должной форме требования, соответствующие рекомендациям настоящего раздела.

9.7. Требования к программному обеспечению следует устанавливать с применением заранее определенного набора методов, соответствующего важности системы для безопасности.

9.8. Методами разработки требований может предусматриваться применение языков спецификации, предполагающих использование строго определенного синтаксиса и семантики, моделей, анализа и пересмотра.

9.9. Следует обеспечить, чтобы у разработчиков требований к программному обеспечению было хорошее понимание проектной основы систем согласно разделу 3.

9.10. Понимание проектной основы систем необходимо для обеспечения того, чтобы требования к программному обеспечению соответствовали основным характеристикам системы. Связанные с этим вопросы включают:

— условия для потенциальных отказов;
— режимы эксплуатации;
— мониторинг в целях обеспечения безопасности;
— самоконтроль;
— выявление отказов;
— безопасные условия, которые должны быть достигнуты при обнаружении неустранимого отказа;
— другие алгоритмы отказобезопасного поведения;
— связи между входами и выходами, имеющие отношение к безопасности.

9.11. Следует обеспечить, чтобы спецификация требований к программному обеспечению:

a) определяла действия каждой отдельной единицы программных средств и ее взаимодействие с другими единицами системы;
b) разрабатывалась с учетом соответствующих процессов жизненного цикла СКУ (включая учет опасностей для системы, определенных в предыдущем анализе) и процессов, связанных с жизненным циклом СКУ, например, с учетом человеческого фактора и операций, связанных с компьютерной безопасностью (см. рис. 2 на стр. 14);
c) по мере возможности составлялась с указанием целей, которые необходимо достигнуть, а не методики их разработки и способов их реализации;
d) была полной, однозначно сформулированной, последовательной, легко читаемой, хорошо понятной для целевых групп пользователей (например, для специалистов в соответствующей области, инженеров по безопасности и разработчиков программного обеспечения), верифицируемой и прослеживаемой;
e) удовлетворяла системным требованиям, предъявляемым к компонентным единицам программного обеспечения, в том числе требованиям по качеству;

f) указывала при необходимости требуемые минимальные показатели погрешности, численной точности, содержала описание интерфейсов[42], требования в отношении независимости потоков выполнения, самоконтроля, характеристик синхронизации[43] и обеспечения физической безопасности[44];

g) предусматривала требуемый уровень надежности и эксплуатационной готовности[45];

h) учитывала способность компьютеров, программных инструментов и аналогичных существующих систем обеспечивать реализуемость требований, предъявляемых к программному обеспечению;

i) содержала соответствующие ссылки на дополнительную информацию, включала или содержала в качестве дополнения такую информацию, предназначенную для целевых групп пользователей, которая может быть, например, справочной информацией о конкретных требованиях, факторах риска, рекомендациях по разработке функций или средств безопасности, в той мере, в какой это необходимо для обеспечения понимания материала целевыми группами пользователей;

j) определяла функции, алгоритмы поведения или взаимодействия, которые являются особенно важными, но которые не реализуются программными средствами.

9.12. Следует обеспечить, чтобы проектные ограничения, если они необходимы, были определены, обоснованы и характеризовались прослеживаемостью.

---

[42] Примерами являются интерфейсы между программными средствами и оператором, между датчиками и исполнительными устройствами, между компьютерным оборудованием и другим программным обеспечением, а также между системами.

[43] Показатели синхронизации включают время, необходимое для обнаружения отказа и устранения последствий отказа.

[44] Примерами средств обеспечения физической безопасности являются проверка валидности и применение системы привилегий права доступа.

[45] Уровень надежности и эксплуатационной готовности может быть определен качественным или количественным способом, например, на основании соответствия дополнительным требованиям, предъявляемым к программному обеспечению, которые указаны в подпунктах (a)–(f) пункта 9.11, и процессам разработки (например, соответствия стандартам).

9.13. В целях облегчения верификации, валидации, прослеживаемости к документации более высокого уровня и демонстрации того, что все соответствующие проектные требования были учтены, следует обеспечить достаточную документированность происхождения каждого требования, предъявляемого к программному обеспечению.

9.14. Следует использовать систему отслеживания требований таким образом, чтобы можно было прослеживать требования, предъявляемые к программному обеспечению, на стадиях разработки, реализации, интеграции и валидации проекта.

9.15. Следует определить требования, предъявляемые к программному обеспечению, которые являются важными для безопасности.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.16. Следует обеспечить, чтобы готовое программное обеспечение характеризовалось однозначностью, было корректным и подтверждаемо полным в плане соответствия требованиям, предъявляемым к программному обеспечению, последовательным, хорошо структурированным, читаемым, понятным для целевых групп пользователей (специалистов в предметных областях, инженеров по безопасности и разработчиков программных средств), верифицируемым, валидируемым, прослеживаемым, обслуживаемым и задокументированным.

9.17. Проект программного обеспечения следует утвердить и актуализировать с применением заранее установленного набора методов, соответствующих важности системы для безопасности.

9.18. Такие методы могут включать в себя описания, логические диаграммы и графические представления с использование строго определенного синтаксиса и семантики, моделей, анализа и пересмотра.

9.19. Разработку программного обеспечения следует осуществлять с пониманием исходных предпосылок к требованиям безопасности.

9.20. Следует обеспечить, чтобы составные элементы программного обеспечения были разграничены в достаточной степени для обеспечения эффективной прослеживаемости требований в процессе проектирования.

9.21. При проектировании программного обеспечения для систем безопасности следует в максимальной степени добиваться простоты на всех уровнях, включая общую архитектуру, внешние интерфейсы, внутренние интерфейсы между модулями и детальное проектирование.

9.22. Обеспечение простоты при проектировании является ключевым средством достижения и демонстрации безопасности, но оно всегда сопряжено с компромиссами, например, в отношении функциональности, гибкости и стоимости. Хотя рекомендация, изложенная в пункте 9.21, применима только к системам безопасности, обеспечение простоты является оправданной целью для программного обеспечения в системах с классом безопасности более низкого уровня. Для систем с классом безопасности более низкого уровня соотношение между безопасностью и сложностью будет иным, и приемлемым является более высокая степень сложности.

9.23. Архитектуру программного обеспечения при проектировании следует структурировать так, чтобы можно было в будущем осуществлять модификацию, обслуживание и обновление.

9.24. Следует обеспечить, чтобы архитектура программного обеспечения была многоуровневой для обеспечения ранжирования уровней абстракции.

9.25. Рекомендуется по возможности использовать метод сокрытия информации в целях реализации принципа фрагментарного обзора и верификации, а также для облегчения работ по модификации.

9.26. В структуру программного обеспечения следует включать интерфейсы между программными средствами и внешними элементами.

9.27. При проектировании программного обеспечения следует предусматривать детальное проектирование всех модулей программного обеспечения.

9.28. Следует обеспечить, чтобы в описании модуля программного обеспечения были полностью определены его функция, его интерфейс с другими модулями и контекст его функции в общей структуре программного обеспечения.

9.29. Следует обеспечить, чтобы модули программного обеспечения, выполняющие аналогичные функции, имели единообразную структуру.

9.30. Следует обеспечить, чтобы интерфейсы модулей были единообразными.

9.31. Следует обеспечить, чтобы обе стороны каждого интерфейса между модулями согласовывались друг с другом, и следует последовательным образом использовать наименования параметров на входе и выходе интерфейса модулей и, насколько это возможно, предотвращать рекурсивные вызовы.

9.32. Если система является многопроцессорной с распределенным программным обеспечением, при разработке программных средств следует определить, какой процесс программного обеспечения реализуется на каком процессоре и где локализуются и отображаются данные.

9.33. Следует обеспечить при проектировании, чтобы программное обеспечение поддерживало детерминированное поведение и синхронизацию систем безопасности.

9.34. Следует обеспечить, чтобы коммуникационные протоколы соответствовали рекомендациям, изложенным в пунктах 7.79–7.94.

9.35. При доработке программного обеспечения следует учитывать необходимость наличия дополнительных возможностей для обнаружения дефектов и самоконтроля системы и предусматривать эти возможности в программном обеспечении (см. пункты 6.166–6.172)

9.36. Следует обеспечить, чтобы при обнаружении дефекта принимались соответствующие меры для соблюдения требований, предъявляемых к программному обеспечению, применительно к процессам восстановления, процедурам остановки, сообщениям об ошибках и журналам регистрации ошибок в целях гарантирования того, что система будет поддерживается в безопасном состоянии.

9.37. В проектной документации программного обеспечения следует предусматривать ограничения в отношении его реализации, которые необходимо соблюдать на стадии проектирования.

9.38. Такие ограничения в отношении реализации могут включать требование об обеспечении неодинаковости (диверсности), а также о применении определенных атрибутов языков программирования, компиляторов, библиотек подпрограмм и других вспомогательных программных средств.

9.39. Следует обеспечить, чтобы такие ограничения были обоснованными или прослеживаемыми до требований или ограничений более высокого уровня.

9.40. В случае систем, не являющихся системами безопасности, достаточной может быть прослеживаемость ограничений в отношении реализации в проприетарной системе (системе с закрытым исходным кодом) до стандартной документации поставщика.

9.41. При разработке архитектуры программного обеспечения следует учитывать ограничения в отношении модулей и интерфейсов, которые могут возникнуть вследствие решения о применении принципа неодинаковости.

9.42. При разработке программного обеспечения следует учитывать передовую практику в области обеспечения информационной безопасности во избежание формирования уязвимостей при проектировании, которые могут быть легко использованы вредоносными программами или хакерами в качестве инструмента эксплуатации.

9.43. В надлежащих случаях может проводиться независимая экспертиза разработки программного обеспечения.

РЕАЛИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.44. Следует обеспечить, чтобы реализация программного обеспечения:

— была корректной применительно к требованиям, предъявляемым к программному обеспечению, и полной применительно к проектированию, хорошо структурированной, читаемой, верифицируемой, прослеживаемой, обслуживаемой и должным образом задокументированной;

— была организована с применением заранее определенного сочетания методов соразмерно важности системы для безопасности, включая языки, программные инструменты, методы кодирования, анализ и тестирование;
— подтверждаемо учитывала все требования, предъявляемые к программному обеспечению и проектированию программного обеспечения.
— была простой и легко понятной, при этом читаемость и обслуживаемость являются приоритетными характеристиками по сравнению с легкостью программирования;
— включала читаемые формы исходного кода и исполняемого кода, результаты тестов блочного интерфейса и тестов интерфейса модулей, а также достаточную контекстуальную информацию для верификации правильности кода в соответствии с его спецификацией.

9.45. Следует обеспечить, чтобы все коды были надлежащим образом документально оформлены.

9.46. Применительно к системам безопасности наличие документации для всех компонентов кода (включая функции динамической поддержки и контроля дефектов) будет обеспечивать соблюдение рекомендаций по тестированию, содержащихся в настоящем Руководстве по безопасности.

9.47. Правила кодирования следует устанавливать перед началом процесса кодирования и следует проводить верификацию соблюдения этих правил.

9.48. Следует обеспечить последовательное применение структур данных и правил присвоения имен.

9.49. При реализации программного обеспечения следует обеспечить, чтобы применялись:

— определенные процедуры контроля изменений (включая анализ последствий);
— конфигурационное управление;
— надлежащее тестовое покрытие результатов всех изменений.

9.50. Следует обеспечить, чтобы использованный язык программирования (языковое подмножество) был адекватным с точки зрения выразительных возможностей, исключения незащищенности, уровня абстракции, поддержки модуляризации и сокрытия информации, компиляции и проверки в процессе исполнения, а также обработки ошибок.

9.51. Следует обеспечить, чтобы язык программирования, используемый для систем безопасности, облегчал достижение простоты реализации.

9.52. Выбор используемых языков программирования и методов функционального определения (например, логических диаграмм или графических представлений) следует основывать на системной оценке требований, предъявляемых к функциональности и целостности используемых процессов.

9.53. Следует обеспечить, чтобы выбор языка программирования для систем безопасности был обоснован и задокументирован.

9.54. Следует обеспечить, чтобы синтаксис и семантика языка, используемого для систем безопасности, были полными, доступными и строго определенными.

9.55. Функции программного обеспечения — это программные элементы, предназначенные для выполнения специфической задачи. Они могут обеспечиваться с помощью языка программирования, библиотек программ или быть заранее разработанными.

9.56. Следует обеспечить, чтобы функции программного обеспечения использовались с целью максимизации простоты и были определены, имели четко сформированные интерфейсы и их вызов всегда осуществлялся с соблюдением соответствующих ограничений в отношении их использования.

9.57. В случае использования операционной системы следует обеспечить, чтобы она была тщательно протестирована с получением удовлетворительных результатов и чтобы ее пригодность для конкретного применения была должным образом обоснована.

9.58. Применительно к системам безопасности следует обеспечить, чтобы программное обеспечение операционной системы в полной мере отвечало рекомендациям, изложенным в настоящем Руководстве по безопасности.

9.59. В целях минимизации ошибок следует выбрать подходящий набор программных инструментов для реализации. Соответствующие рекомендации изложены в пунктах 7.148–7.164.

9.60. Рекомендации, содержащиеся в данном разделе, применимы ко всем возможным комбинациям использования кода генерации и классической разработки программного обеспечения.

9.61. Обеспечение неодинаковости при разработке программного обеспечения (т.е. использование независимых групп разработчиков и/или разных методов, языков, характеристик синхронизации, порядков функции или алгоритмов) можно рассматривать в качестве средства снижения вероятности и последствий отказов по общей причине в программном обеспечении. Вместе с тем использование неодинакового программного обеспечения может привести к проектным ограничениям, которые в свою очередь могут стать причиной новых отказов.

9.62. При использовании одинакового программного обеспечения, такого как операционная система, сетевая коммуникационная программа или другие вспомогательные программные средства, следует принять меры предосторожности, гарантирующие, что независимость систем, поддерживающих разные уровни глубокоэшелонированной защиты, не будет поставлена под угрозу.

9.63. Следует обеспечить, чтобы группы специалистов, занимающиеся реализацией программного обеспечения, были обучены методам разработки, обеспечивающим физическую безопасность (защищенность).

ВЕРИФИКАЦИЯ И АНАЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

9.64. Требования к программному обеспечению, разработку и реализацию программного обеспечения следует верифицировать на соответствие спецификации требований, предъявляемых к СКУ.

9.65. Верификацию прослеживаемости следует проводить на постоянной основе для обеспечения того, чтобы недостатки выявлялись как можно раньше, и, следовательно, внесение необходимых изменения оставалось практически реализуемым.

9.66. Результаты каждого этапа жизненного цикла программного обеспечения следует верифицировать на соответствие требованиям, установленными для предыдущих этапов.

9.67. Следует подготовить план верификации программного обеспечения, в котором задокументированы:

a) используемые методы верификации;
b) детали процедур (или ссылки на эти процедуры), которые будут использоваться при применении каждого метода, включая его охват и глубину;
c) порядок подтверждения того, что нефункциональные требования и ограничения соблюдаются;
d) критерии определения момента, когда была выполнена достаточная верификация, включая целевые показатели ее полноты с учетом результатов предыдущего этапа и структурного охвата функциональных тестов, а также того, как данные результаты будут продемонстрированы;
e) средства, с помощью которых будут фиксироваться результаты;
f) средства, с помощью которых будут фиксироваться и устраняться несоответствия и дефекты;
g) группа или группы, проводящие верификацию, и их независимость от разработчиков программного обеспечения.
h) функции всех программных инструментов, используемых для верификации, включая ожидаемые результаты и ограничения в его использовании (например, предметные области, языки и процессы);
i) обоснование для каждого элемента, указанного выше в подпунктах (a)–(h), и подтверждение того, что верификация будет достаточной для программного обеспечения в системе, относящейся к применяемому классу безопасности.

9.68. В верификацию следует включать применение:

— выполняемых вручную (неавтоматизированных) проверок, таких как анализ, сквозной контроль, инспекции и аудит;
— статического анализа исходного кода;
— динамического анализа.

9.69. Статический анализ следует выполнять на финальной версии программного обеспечения.

9.70. В зависимости от важности системы для безопасности используются разные методы статического анализа. При проведении статического анализа применяются такие методы как проверка соответствия проектирования стандартам кодирования, анализ контроля, потока данных информации, символического выполнения, а также формальная верификация кода.

9.71. Следует верифицировать все нефункциональные требования, реализованные в программном обеспечении.

9.72. Для коррекции обнаруженных отклонений и обеспечения дополнительной уверенности в гарантоспособности программного обеспечения следует использовать соответствующий эксплуатационный опыт.

9.73. Соответствующий эксплуатационный опыт может служить дополнением к методам верификации, не являясь его заменой.

9.74. Рекомендации по использованию инструментальных средств для верификации и анализа программного обеспечения изложены в пунктах 7.148–7.164.

9.75. Для верификации и валидации процесса реализации программного обеспечения следует выбрать стратегию тестирования (например, стратегию «снизу вверх» или стратегию «сверху вниз»).

9.76. В спецификации тестовых (контрольных) примеров следует предусмотреть надлежащее тестирование:

— интерфейсов (таких как интерфейсов модуль–модуль, интерфейсов программное обеспечение–аппаратные средства, интерфейсов границ системы);
— механизмов передачи данных и интерфейсных протоколов;
— условий исключений;
— полного диапазона каждого входного параметра (с применением таких методов, как разбиение на классы эквивалентности и анализ граничных значений);
— всех режимов работы системы.

9.77. В целях облегчения проведения регрессионного тестирования следует обеспечить, чтобы планы тестирования гарантировали, что тесты являются повторяемыми и их результаты фиксируются.

9.78. Кроме того, желательно, чтобы при проведении повторных тестов участие человека было сведено к минимуму.

9.79. В публикации GS-G-3.1 [3] содержатся рекомендации по обеспечению пригодности измерительной и тестовой аппаратуры, используемой при проведении тестирования.

9.80. Следует анализировать спецификации тестовых примеров и их эффективность, и любые расхождения с целевыми показателями, указанными в плане проведения верификации, следует устранять или обосновывать.

9.81. Следует обеспечить, чтобы верификация проводилась группами специалистов, отдельными специалистами или группами специализированной организации, не зависящими от проектировщиков и разработчиков.

9.82. Для выявления уязвимостей в физической безопасности (защищенности) программного обеспечения следует проводить проверку кода с помощью автоматизированных программных средств, а также вручную с целью анализа критических участков кода (например, обработки входов/выходов и обработки исключений).

9.83. Все выходы СКУ следует контролировать в процессе верификации, и любые отклонения от ожидаемых результатов следует анализировать и документально фиксировать.

9.84. Любые несоответствия результатов верификации по сравнению с планом проведения верификации (например, в том, что касается тестового покрытия), следует устранить или обосновать.

9.85. Следует обеспечить, чтобы все выявленные ошибки были исследованы на предмет выявления причин и устранены с применением установленных процедур выполнения модификаций, а также регрессионного тестирования в надлежащих случаях.

9.86. В анализ ошибок следует включить оценку применимости к другим элементам СКУ.

9.87. Следует фиксировать данные о количестве и типах выявленных отклонений, анализировать их с целью учета в процессе разработки, а также использовать их для осуществления соответствующих технологических усовершенствований в текущих и будущих проектах. (См. пункты 6.50–6.77 в публикации GS-G-3.1 [3] и пункты 6.42–6.69 в публикации GS-G-3.5 [4].)

9.88. В документацию по верификации и анализу следует включить упорядоченный перечень доказательств того, что продукты, получаемые в результате процесса разработки, являются полными, правильными и согласованными.

9.89. Результаты верификации, включая протоколы испытаний, следует задокументировать и хранить с обеспечением доступа к ним для целей контроля качества и проведения сторонних оценок.

9.90. Для обеспечения прослеживаемости проектной документации следует использовать последовательные ссылки между документацией каждой стадии жизненного цикла и функциональными требованиями.

9.91. Следует обеспечить, чтобы документация по результатам тестирования была прослеживаемой к спецификациям тестовых примеров и основывалась на них и в ней было указано, какие результаты оказались не соответствующими ожидаемым значениям и как возникшие проблемы были решены.

9.92. Следует обеспечить, чтобы тестовое покрытие было четко задокументировано.

9.93. Применительно к системам безопасности следует предусмотреть возможность прослеживать каждый тестовый пример, используя матрицу прослеживаемости, отражающую связи между требованиями, предъявляемыми к программному обеспечению, его разработкой, реализацией и тестированием.

9.94. Применительно к системам безопасности полученную прикладную программу следует направить на тестирование для того, чтобы убедиться в компьютерной безопасности (например, для тестирования на возможность проникновения), подтвердить, что общие уязвимости в защите найти сложно, и обеспечить возможность непрерывного совершенствования процессов разработки и реализации программных продуктов.

9.95. Следует обеспечить, чтобы тестовая документация была достаточной и позволяла воспроизводить процесс тестирования с уверенностью в том, что будут получены аналогичные результаты.

РАНЕЕ РАЗРАБОТАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

9.96. Применительно к системам безопасности следует обеспечить, чтобы ранее разработанное программное обеспечение, используемое в системах безопасности СКУ, было квалифицировано на том же уровне, что и программное обеспечение, разработанное специально для данного применения.

9.97. Следует обеспечить, чтобы функции ранее разработанного программного обеспечения соответствовали рекомендациям, изложенным в пунктах 2.108–2.117.

9.98. Применительно к системам, важным для безопасности, которые не являются системами безопасности, для ранее разработанного программного обеспечения следует иметь пользовательскую документацию, содержащую описание:

a) обеспечиваемых функций;
b) интерфейсов, включая роли, типы, форматы, диапазоны и ограничения входов, выходов, сигналов об исключениях, параметров и конфигурационных данных;
c) разных алгоритмов поведения и соответствующих условий перехода (если это применимо);
d) любых ограничений, которые должны соблюдаться при использовании ранее разработанного программного обеспечения;
e) обоснования того, что ранее разработанное программное обеспечение является корректным относительно описания согласно указанным выше подпунктам (a)–(d), представленного в пользовательской документации;
f) обоснования пригодности функций для СКУ.

ПРОГРАММНЫЕ ИНСТРУМЕНТЫ

9.99. Рекомендации, касающиеся программных инструментов, изложены в пунктах 7.148–7.164.

СТОРОННЯЯ ОЦЕНКА

9.100. Стороннюю оценку программного обеспечения систем безопасности следует проводить параллельно с процессом разработки программных средств.

9.101. Цель такой сторонней оценки — получить экспертное заключение об адекватности системы и используемого в ней программного обеспечения независимо от поставщика системы и/или программного обеспечения, а также эксплуатирующей организации. Такая оценка может проводиться регулирующим органом или организациями, являющимися приемлемыми для регулирующего органа.

9.102. Важно получить разрешение разработчика программного обеспечения на проведение сторонней оценки.

9.103. В оценку следует включить проверку:

— процесса разработки (например, посредством аудита обеспечения качества и технических инспекций, включая проверку документации всего жизненного цикла, например, планов, спецификаций программного обеспечения и документов по всему объему тестирования);
— конечного программного обеспечения (например, посредством проведения статического анализа, инспекции, аудита и тестирования), включая любые последующие модификации.

СПРАВОЧНЫЕ МАТЕРИАЛЫ

[1] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Безопасность атомных электростанций: проектирование, Серия норм безопасности МАГАТЭ, № SSR-2/1 (Rev. 1), МАГАТЭ, Вена (2016).

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Система управления для установок и деятельности, Серия норм безопасности МАГАТЭ, № GS-R-3, МАГАТЭ, Вена (2008). (Новая редакция данной публикации выпущена под заголовком «Лидерство и менеджмент для обеспечения безопасности», Серия норм безопасности МАГАТЭ, № GSR Part 2, МАГАТЭ, Вена (2017)).

[3] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Применение системы управления для установок и деятельности, Серия норм безопасности МАГАТЭ, № GS-G-3.1, МАГАТЭ, Вена (2009).

[4] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Система управления для ядерных установок, Серия норм безопасности МАГАТЭ, № GS-G-3.5, МАГАТЭ, Вена (2014).

[5] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Оценка безопасности установок и деятельности, Серия норм безопасности МАГАТЭ, № GSR Part 4 (Rev. 1), МАГАТЭ, Вена (2016).

[6] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Глоссарий МАГАТЭ по вопросам безопасности: терминология, используемая в области ядерной безопасности и радиационной защиты (издание 2007 года), МАГАТЭ, Вена (2008).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016).

[8] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Компьютерная безопасность на ядерных установках, Серия изданий МАГАТЭ по физической ядерной безопасности, № 17, МАГАТЭ, Вена (2012).

[9] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Модификации на атомных станциях, Серия норм безопасности МАГАТЭ, № NS-G-2.3, МАГАТЭ, Вена (2004).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (1999).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

[12] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Разработка и применение вероятностной оценки безопасности уровня 1 для атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-3, МАГАТЭ, Вена (2014).

[13] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Разработка и применение вероятностной оценки безопасности уровня 2 для атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-4, МАГАТЭ, Вена (2014).
[14] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Детерминистический анализ безопасности атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-2, МАГАТЭ, Вена (2014).
[15] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Ввод в эксплуатацию атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-28, МАГАТЭ, Вена (2016).
[16] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Техническое обслуживание, надзор и инспекции при эксплуатации на атомных электростанциях, Серия норм безопасности МАГАТЭ, № NS-G-2.6, МАГАТЭ, Вена (2005).
[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).
[18] МЕЖДУНАРОДНАЯ КОНСУЛЬТАТИВНАЯ ГРУППА ПО ЯДЕРНОЙ БЕЗОПАСНОСТИ, Глубокоэшелонированная защита в ядерной безопасности, INSAG-10, МАГАТЭ, Вена (1998).
[19] МЕЖДУНАРОДНАЯ КОНСУЛЬТАТИВНАЯ ГРУППА ПО ЯДЕРНОЙ БЕЗОПАСНОСТИ, Основные принципы безопасности атомных электростанций 75-INSAG-3 Rev.1, INSAG-12, МАГАТЭ, Вена (2015).
[20] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Защита от внутренних пожаров и взрывов при проектировании атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.7, МАГАТЭ, Вена (2008).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, IAEA, Vienna (1998).
[23] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Проектирование и аттестация сейсмостойких конструкций для атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.6, МАГАТЭ, Вена (2008).
[24] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Учет внешних событий, исключая землетрясения, при проектировании атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.5, МАГАТЭ, Вена (2008).
[25] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Управление старением атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-2.12, МАГАТЭ, Вена (2014).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[27] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Предупредительные и защитные меры в отношении угроз, исходящих от внутреннего нарушителя, Серия изданий МАГАТЭ по физической ядерной безопасности, № 8, МАГАТЭ, Вена (2009).
[28] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Рекомендации по физической ядерной безопасности, касающиеся физической защиты ядерных материалов и ядерных установок (INFCIRC/225/Revision 5), Серия изданий МАГАТЭ по физической ядерной безопасности, № 13, МАГАТЭ, Вена (2012).
[29] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Пределы и условия для эксплуатации и эксплуатационные процедуры для атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-2.2, МАГАТЭ, Вена (2004).
[30] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Эксплуатирующая организация для атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-2.4, МАГАТЭ, Вена (2004).
[31] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Ведение эксплуатации атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-2.14, МАГАТЭ, Вена (2008).
[32] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Аспекты радиационной защиты при проектировании атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.13, МАГАТЭ, Вена (2008).
[33] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Проектирование систем аварийного энергоснабжения атомных электростанций, Серия норм безопасности МАГАТЭ, № NS-G-1.8, МАГАТЭ, Вена (2004).

Приложение I

БИБЛИОГРАФИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ПО СИСТЕМАМ КОНТРОЛЯ И УПРАВЛЕНИЯ

I–1. В требовании 9 публикации SSR-2/1 (Rev. 1) [I–1] указано: «Узлы АЭС, важные для безопасности, должны проектироваться согласно соответствующим национальным и международным сводам положений и нормам».

I–2. В настоящем Руководстве по безопасности изложены рекомендации высокого уровня, которые широко признаются в государствах — членах МАГАТЭ. Помимо рекомендаций, публикуемых МАГАТЭ, также существует большое количество национальных и международных стандартов, содержащих более подробные рекомендации по методам проектирования и характеристикам систем, которые дополняют требования, изложенные в публикации SSR-2/1 (Rev. 1) [I–1]. Предполагается, что для проектировщиков, пользователей и регулирующих органов информация, содержащаяся в этих стандартах, будет полезной.

I–3. За подготовку большинства международных стандартов по системам контроля и управления (СКУ) для атомных электростанций, отвечают две организации, разрабатывающие стандарты: a) Международная электротехническая комиссия (МЭК), подкомитет 45, и b) Институт инженеров по электротехнике и электронике (ИИЭЭ), Комитет по атомной энергетике. Каждая из этих организаций разработала большое количество стандартов. Обе организации издают стандарты, которые соответствуют общепринятым принципам, лежащим в основе требований, изложенных в публикации SSR-2/1 (Rev. 1) [I–1], а также рекомендаций, содержащихся в настоящем Руководстве по безопасности. Следовательно, стандарты любой из этих организаций могут быть использованы в качестве дополнительного материала к рекомендациям настоящего Руководства по безопасности.

I–4. Цель данного приложения — помочь пользователям понять корреляцию между настоящим Руководством по безопасности и стандартами МЭК и ИИЭЭ. В таблице I–1 приведен перечень стандартов МЭК (IEC) и ИИЭЭ (IEEE), имеющих тесную корреляцию с рекомендациями настоящего Руководства по безопасности. В таблице I–1 перечислены не все стандарты, входящие в эти две группы стандартов, однако она позволяют найти ключевой стандарт в каждой группе стандартов МЭК и ИИЭЭ.

I–5. В таблице I–2 показана корреляция этих ключевых стандартов с основными разделами настоящего Руководства по безопасности.

ТАБЛИЦА I–1. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ, ИМЕЮЩИЕ ТЕСНУЮ КОРРЕЛЯЦИЮ С НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ

IEC 60515	Nuclear power plants — Instrumentation important to safety — Radiation detectors — Characteristics and test methods (Атомные электростанции — Контрольно-измерительные приборы, важные для безопасности — Радиационные детекторы — Характеристики и методы испытаний)
IEC 60568	Nuclear power plants — Instrumentation important to safety — In-core instrumentation for neutron fluence rate (flux) measurements in power reactors (Атомные электростанции — Контрольно-измерительные приборы, важные для безопасности — Внутриреакторные датчики для измерения плотности нейтронного потока в энергетических реакторах)
IEC 60671	Nuclear power plants — Instrumentation and control systems important to safety — Surveillance testing (Атомные электростанции — Системы контроля и управления, важные для безопасности — Контрольные испытания)
IEC 60709	Nuclear power plants — Instrumentation and control systems important to safety — Separation (Атомные электростанции — Системы контроля и управления, важные для безопасности — Разделение)
IEC 60737	Nuclear power plants — Instrumentation important to safety — Temperature sensors (in-core and primary coolant circuit) — Characteristics and test methods (Атомные электростанции — Контрольно-измерительные приборы, важные для безопасности — Датчики температуры (внутриреакторные и первого контура) — Характеристики и методы) испытаний
IEC 60780	Nuclear facilities — Electrical equipment important to safety — Qualification (Ядерные установки — Электрическое оборудование, важное для безопасности — Квалификация)

ТАБЛИЦА I–1. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ, ИМЕЮЩИЕ ТЕСНУЮ КОРРЕЛЯЦИЮ С НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ (продолжение)

IEC 60880	Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions (Атомные электростанции — Системы контроля и управления, важные для безопасности — Аспекты программного обеспечения для компьютеризированных систем, выполняющих функции категории А)
IEC 60964	Nuclear power plants — Control rooms — Design (Атомные электростанции — Пункты управления — Проектирование)
IEC 60980	Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations (Рекомендованная практика сейсмической квалификации электрического оборудования системы безопасности для атомных электростанций)
IEC 61226	Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions (Атомные электростанции — Контроль и управление, важные для безопасности — Классификация функций контроля и управления)
IEC 61468	Nuclear power plants — In-core instrumentation — Characteristics and test methods of self-powered neutron detectors (Атомные электростанции — Внутриреакторные контрольно-измерительные приборы — Характеристики и методы тестирования нейтронных детекторов с автономным питанием)
IEC 61500	Nuclear power plants — Instrumentation and control important to safety — Data communication in systems performing category A functions (Атомные электростанции — Контроль и управление, важные для безопасности — Коммуникация данных в системах, выполняющих функции категории А)
IEC 61501	Nuclear reactor instrumentation — Wide range neutron fluence rate meter — Mean square voltage method (Контрольно-измерительные приборы ядерных реакторов — Широкодиапазонные измерители плотности нейтронного потока — Метод среднеквадратического значения напряжения)

ТАБЛИЦА I–1. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ, ИМЕЮЩИЕ ТЕСНУЮ КОРРЕЛЯЦИЮ С НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ (продолжение)

IEC 61513	Nuclear power plants — Instrumentation and control important to safety — General requirements for systems (Атомные электростанции — Контроль и управление, важные для безопасности — Общие требования к системам)
IEC 61772	Nuclear power plants — Control rooms — Application of visual display units (VDUs) (Атомные электростанции — Пункты управления — Применение устройств визуальной индикации (УВИ))
IEC 61839	Nuclear power plants — Design of control rooms — Functional analysis and assignment (Атомные электростанции — Проектирование пунктов управления — Функциональный анализ и присвоение функций)
IEC 61888	Nuclear power plants — Instrumentation important to safety — Determination and maintenance of trip setpoints (Атомные электростанции — Контрольно-измерительные приборы, важные для безопасности — Определение и поддержание уставок аварийной защиты)
IEC 62003	Nuclear power plants — Instrumentation and control important to safety — Requirements for electromagnetic compatibility testing (Атомные электростанции — Контроль и управление, важные для безопасности — Требования к проверке на электромагнитную совместимость)
IEC 62138	Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing categories B or C functions (Атомные электростанции — Контроль и управление, важные для безопасности — Аспекты программного обеспечения для компьютеризированных систем, выполняющих функции категории B или C)
IEC 62241	Nuclear power plants — Main control room — Alarm functions and presentation (Атомные электростанции — Блочный пункт управления — Функции и представление сигнализации)
IEC 62340	Nuclear power plants — Instrumentation and control systems important to safety — Requirements for coping with common cause failure (CCF) (Атомные электростанции — Системы контроля и управления, важные для безопасности — Требования к решению проблемы отказа по общей причине (ООП))

ТАБЛИЦА I–1. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ, ИМЕЮЩИЕ ТЕСНУЮ КОРРЕЛЯЦИЮ С НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ (продолжение)

IEC 62397	Nuclear power plants — Instrumentation and control important to safety — Resistance temperature detectors (Атомные электростанции — Контроль и управление, важные для безопасности — Резистивные датчики температуры)
IEC 62566	Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions (Атомные электростанции — Контроль и управление, важные для безопасности — Разработка интегральных схем, программируемых на языке описания аппаратуры, для систем, выполняющих функции категории А)
IEC 62671	Nuclear power plants — Instrumentation and control important to safety — Selection and use of industrial digital devices of limited functionality (Атомные электростанции — Контроль и управление, важные для безопасности — Выбор и использование промышленных цифровых устройств ограниченной функциональности)
IEEE Std. 1023	IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities (Практические рекомендации ИИЭЭ по применения учета человеческого фактора к системам, оборудованию и установкам атомных электростанций и других ядерных объектов)
IEEE Std. 308	IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations (Стандартные критерии ИИЭЭ для энергетических систем класса 1Е атомных электростанций)
IEEE Std. 323	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations (Стандарт ИИЭЭ по квалификации оборудования класса 1Е атомных электростанций)
IEEE Std. 338	IEEE Standard for Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems (Стандарт ИИЭЭ по критериям для периодических контрольных испытаний систем безопасности атомных электростанций)

ТАБЛИЦА I–1. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ, ИМЕЮЩИЕ ТЕСНУЮ КОРРЕЛЯЦИЮ С НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ (продолжение)

IEEE Std. 344	IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations (Стандарт ИИЭЭ по сейсмической квалификации оборудования атомных электростанций)
IEEE Std. 379	IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Стандарт ИИЭЭ по применению критерия единичного отказа к системам безопасности атомных электростанций)
IEEE Std. 384	IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits (Стандарт ИИЭЭ по критериям независимости оборудования и контуров класса 1E)
IEEE Std. 497	IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations (Стандарт ИИЭЭ по критериям, применяемым в отношении контрольно-измерительных приборов для аварийного мониторинга на атомных электростанциях)
IEEE Std. 603	IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Стандарт ИИЭЭ по критериям для систем безопасности атомных электростанций)
IEEE Std. 7–4.3.2	IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (Стандарт ИИЭЭ по критериям для цифровых компьютеров в системах безопасности атомных электростанций)
IEEE Std. 1012	IEEE Standard for Software Verification and Validation (Стандарт ИИЭЭ по верификации и валидации программного обеспечения)
IEEE Std. 1074	IEEE Standard for Developing Software Life Cycle Processes (Стандарт ИИЭЭ по разработке процессов жизненного цикла программного обеспечения)
ISO/IEC 15288	Systems and software engineering — System life cycle processes (Разработка систем и программного обеспечения — Процессы жизненного цикла систем)
ISO/IEC 12207	Systems and software engineering — Software life cycle processes (Разработка систем и программного обеспечения — Процессы жизненного цикла программного обеспечения)

Примечание: ISO (ИСО): Международная организация по стандартизации

ТАБЛИЦА I–2. КОРРЕЛЯЦИЯ МЕЖДУ РАЗДЕЛАМИ НАСТОЯЩЕГО РУКОВОДСТВА ПО БЕЗОПАСНОСТИ И МЕЖДУНАРОДНЫМИ СТАНДАРТАМИ

Настоящее Руководство по безопасности	Международные стандарты по СКУ
1. Введение	
2. Система менеджмента для проектирования СКУ:	IEC 61513, IEEE 74.3.2
— Применение моделей жизненного цикла	IEC 61513, IEEE 74.3.2, ISO/IEC 15288
3. Проектные основы СКУ:	IEC 61513, IEEE 603
— Определение функций контроля и управления	IEC 61226
— Содержание проектной основы СКУ	IEC 61513
4. Архитектура контроля и управления	IEC 61513, IEC 62340
5. Классификация безопасности для функций, систем и оборудования контроля и управления	IEC 61226
6. Общие рекомендации для всех СКУ, важных для безопасности:	
— Общие положения	IEC 61513, IEC 60709, IEEE 379, IEEE 384
— Проектирование в целях обеспечения надежности	
— Квалификация оборудования	IEC 60780, IEC 980, IEC 62342, IEEE 344, IEEE 323, IEC 2003
— Проектирование с учетом проблем старения и устаревания	
— Контроль доступа к системам, важным для безопасности	IEC 61513
— Испытания и тестопригодность в период эксплуатации	IEC 60671, IEEE 338

ТАБЛИЦА I–2. КОРРЕЛЯЦИЯ МЕЖДУ РАЗДЕЛАМИ НАСТОЯЩЕГО РУКОВОДСТВА ПО БЕЗОПАСНОСТИ И МЕЖДУНАРОДНЫМИ СТАНДАРТАМИ (продолжение)

Настоящее Руководство по безопасности	Международные стандарты по СКУ
— Ремонтопригодность	IEC 61513
— Меры по выводу их эксплуатации для проведения испытаний или обслуживания	IEC 61513
— Заданные уставки	IEC 61888
— Маркировка и идентификация узлов, важных для безопасности	
— Настоящее Руководство по безопасности	Международные стандарты по СКУ
7. Руководящие принципы проектирования конкретных систем контроля и управления и оборудования:	
— Датчики	IEC 60515, IEC 61501, IEC 60568, IEC 61468, IEC 60737
— Системы управления	
— Система защиты	IEEE 603
— Источники энергоснабжения	IEC 61225, IEEE 308
— Цифровые системы	IEC 61513, IEEE 74.3.2, IEC 61500, IEC 62671
— Устройства, конфигурированные с использованием языков описания аппаратных средств	IEC 62566
— Программные инструменты	IEC 60880, IEC 62138

ТАБЛИЦА I–2. КОРРЕЛЯЦИЯ МЕЖДУ РАЗДЕЛАМИ НАСТОЯЩЕГО РУКОВОДСТВА ПО БЕЗОПАСНОСТИ И МЕЖДУНАРОДНЫМИ СТАНДАРТАМИ (продолжение)

Настоящее Руководство по безопасности	Международные стандарты по СКУ
8. Аспекты, связанные с человеко-машинным интерфейсом:	
— Пункты управления	IEC 60964, IEC 61772, IEC 62241, IEEE 576
— Дополнительные щиты управления	IEC 60965
— Аварийный мониторинг	IEEE 497
— Системы связи операторов	
— Общие принципы, связанные с учетом человеческого фактора при проектировании СКУ	IEC 61839, IEC 61772, IEEE 1023, IEEE 1082
— Регистрация исторических данных	
9. Программное обеспечение	IEC 60880, IEC 62138, IEEE 7–4.3.2, IEEE 1012, Ст-т IEEE 1074, ISO/IEC 12207

I–6. Была проведена совместная работа по исключению коллизий между рекомендациями, представленными в настоящем Руководстве по безопасности, и стандартами МЭК и ИИЭЭ. Члены комитетов МЭК и ИИЭЭ участвовали в подготовке настоящего Руководства по безопасности, и обе эти организации по разработке стандартов рецензировали проекты настоящего Руководства по безопасности с целью выявления и устранения расхождений.

I–7. Вместе с тем пользователям необходимо осознавать и принимать в расчет тот факт, что между стандартами МЭК и ИИЭЭ имеются важные различия.

I–8. При разработке своих стандартов МЭК применяет Требования безопасности и Руководства по безопасности МАГАТЭ в качестве основополагающих документов. Вследствие этого в стандартах МЭК содержание сосредоточено на узлах (элементах), важных для безопасности, и используются руководящие материалы МАГАТЭ по СКУ в качестве источника общих рекомендаций.

I–9. Содержание стандартов ИИЭЭ сфокусировано главным образом на узлах (элементах) безопасности, и, следовательно, рекомендации этой организации напрямую применяются к меньшему кругу функций, систем и оборудования по сравнению с настоящим Руководством по безопасности. Вместе с тем рекомендации ИИЭЭ могут быть применены также к узлам (элементам), связанным с безопасностью (узлам, важным для безопасности, которые не являются системами безопасности) на основе дифференцированного подхода.

I–10. В стандартах ИИЭЭ настоящее Руководство по безопасности не используется в качестве справочного материала. Стандарт IEEE 603 Std. (см. таблицу I–1) является эквивалентом настоящего Руководства по безопасности в системе стандартов ИИЭЭ. В то же время настоящее Руководство по безопасности и стандарты ИИЭЭ разработаны с использованием одинаковых принципов проектирования СКУ. Следует отметить, что в стандартах ИИЭЭ термин «безопасность» (safety), термин-прилагательное «связанный с безопасностью» (safety related) и термин «1E» часто употребляются в качестве эквивалента термина «безопасность» (safety), используемого МАГАТЭ. В ИИЭЭ отсутствует термин, эквивалентный используемому МАГАТЭ термину-прилагательному «связанный с безопасностью» (safety related).

I–11. В публикации [I–2] приводится более обширная библиография стандартов по проектированию СКУ.

СПРАВОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРИЛОЖЕНИЯ I

[I–1] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Безопасность атомных электростанций: проектирование, Серия норм безопасности МАГАТЭ, № SSR-2/1 (Rev. 1), МАГАТЭ, Вена (2016).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

Приложение II

КОРРЕЛЯЦИЯ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ И ПУБЛИКАЦИЯМИ СЕРИИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ, №№ NS-G-1.1 И NS-G-1.3

II–1. В данном приложении представлены таблицы, в которых указаны разделы настоящего Руководства по безопасности, охватывающие содержание двух предыдущих Руководств по безопасности NS-G-1.1[1] и NS-G-1.3[2].

ТАБЛИЦА II–1. КОРРЕЛЯЦИЯ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ И ПУБЛИКАЦИЕЙ СЕРИИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ, № NS-G-1.1

Серия норм безопасности, № NS-G-1.1	Настоящее Руководство по безопасности
1. Введение	1. Введение
2. Технические требования к компьютеризированным системам	2. Система менеджмента для проектирования СКУ 9. Программное обеспечение: Общие положения
3. Применение требований по управлению безопасностью к компьютеризированным системам	2. Система менеджмента для проектирования СКУ 9. Программное обеспечение: Сторонняя оценка
4. Планирование проекта	2. Система менеджмента для проектирования СКУ
5. Требования к компьютерным системам	2. Система менеджмента для проектирования СКУ

[1] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Программное обеспечение для компьютерных систем, важных для безопасности атомных электростанций, Серия норм МАГАТЭ по безопасности № NS-G-1.1, МАГАТЭ, Вена (2000).

[2] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, «Системы СКУ, важные для безопасности атомных электростанций, Серия норм МАГАТЭ по безопасности», № NS-G-1.3, МАГАТЭ, Вена (2002).

ТАБЛИЦА II–1. КОРРЕЛЯЦИЯ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ И ПУБЛИКАЦИЕЙ СЕРИИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ, № NS-G-1.1 (ПРОДОЛЖЕНИЕ)

Серия норм безопасности, № NS-G-1.1	Настоящее Руководство по безопасности
6. Разработка компьютерных систем	2. Система менеджмента для проектирования СКУ 6. Общие рекомендации для всех СКУ, важных для безопасности 7. Руководящие принципы проектирования конкретных СКУ и оборудования 8. Аспекты, связанные с человеко-машинным интерфейсом
7. Требования к программному обеспечению	9. Программное обеспечение: Требования к программному обеспечению
8. Разработка программного обеспечения	9. Программное обеспечение: Разработка программного обеспечения
9. Реализация программного обеспечения	9. Программное обеспечение: Реализация программного обеспечения
10. Верификация и анализ	9. Программное обеспечение: Верификация и анализ программного обеспечения
11. Интеграция компьютерных систем	2. Система менеджмента для проектирования СКУ
12. Валидация компьютерных систем	2. Система менеджмента для проектирования СКУ
13. Установка и пуск в эксплуатацию	2. Система менеджмента для проектирования СКУ
14. Эксплуатация	2. Система менеджмента для проектирования СКУ
15. Модификации после поставки	2. Система менеджмента для проектирования СКУ
Приложение: Использование и валидация существующего программного обеспечения	2. Система менеджмента для проектирования СКУ 9. Программное обеспечение: ранее разработанное программное обеспечение

Примечание: СКУ: система контроля и управления.

ТАБЛИЦА II–2. КОРРЕЛЯЦИЯ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ И ПУБЛИКАЦИЕЙ СЕРИИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ, № NS-G-1.3

Серия норм безопасности МАГАТЭ, № NS-G-1.3	Настоящее Руководство по безопасности
1. Введение	1. Введение
2. Системы контрольно-измерительных приборов, важных для безопасности:	См. [II–1]
— Определение систем КИПиУ	3. Проектные основы для СКУ
— Классификация систем КИПиУ	5. Классификация безопасности функций, систем и оборудования СКУ
3. Проектные основы	3. Проектная основа для СКУ
4. Общие принципы проектирования:	
— Требования к рабочим характеристикам	2. Система менеджмента для проектирования СКУ: Деятельность, осуществляемая в течение жизненного цикла: Спецификация требований
— Обеспечение надежности при проектировании	6. Общие рекомендации для всех СКУ, важных для безопасности: Проектирование в целях обеспечения надежности
— Независимость	4. Архитектура контроля и управления: Независимость 6. Общие рекомендации для всех СКУ, важных для безопасности: Проектирование в целях обеспечения надежности: Независимость
— Виды отказов	7. Общие рекомендации для всех СКУ, важных для безопасности: Проектирование в целях обеспечения надежности: Виды отказов

ТАБЛИЦА II–2. КОРРЕЛЯЦИЯ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ И ПУБЛИКАЦИЕЙ СЕРИИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ, № NS-G-1.3 (продолжение)

Серия норм безопасности МАГАТЭ, № NS-G-1.3	Настоящее Руководство по безопасности
— Контроль доступа к оборудованию	6. Общие рекомендации для всех СКУ, важных для безопасности: Контроль доступа к системам, важным для безопасности 7. Руководящие принципы проектирования конкретных систем контроля и оборудования и оборудования: Цифровые системы: Компьютерная безопасность
— Уставки	6. Общие рекомендации для всех СКУ, важных для безопасности: Заданные уставки
— Взаимодействие человек-машина	8. Аспекты, связанные с человеко-машинным интерфейсом
— Аттестация оборудования	6. Общие рекомендации для всех СКУ, важных для безопасности: Квалификация оборудования
— Качество	2. Система менеджмента для проектирования СКУ
— Обеспечение электромагнитной совместимости при проектировании	6. Общие рекомендации для всех СКУ, важных для безопасности: Квалификация оборудования: Внутренние и внешние опасности: Квалификация по электромагнитной совместимости
— Испытания и возможность проведения испытаний	6. Общие рекомендации для всех СКУ, важных для безопасности: испытания и тестопригодность в период эксплуатации
— Возможность проведения технического обслуживания	6. Общие рекомендации для всех СКУ, важных для безопасности: ремонтопригодность

ТАБЛИЦА II–2. КОРРЕЛЯЦИЯ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ ПО БЕЗОПАСНОСТИ И ПУБЛИКАЦИЕЙ СЕРИИ НОРМ БЕЗОПАСНОСТИ МАГАТЭ, № NS-G-1.3 (продолжение)

Серия норм безопасности МАГАТЭ, № NS-G-1.3	Настоящее Руководство по безопасности
— Документация	2. Система менеджмента для проектирования СКУ: Деятельность, свойственная всем стадиям жизненного цикла: Документация
— Идентификация узлов, важных для безопасности	6. Общие рекомендации для всех СКУ, важных для безопасности: маркировка и идентификация узлов, важных для безопасности
9. Принципы проектирования систем:	
— Системы безопасности — Системы защиты	7. Руководящие принципы проектирования конкретных систем и оборудования СКУ: системы защиты
— Источники энергоснабжения	7. Руководящие принципы проектирования конкретных СКУ и оборудования: Источники энергоснабжения
— Цифровые компьютерные системы	7. Руководящие принципы проектирования конкретных СКУ и оборудования: Цифровые системы
6. Взаимодействие человек-машина	8. Аспекты, связанные с человеко-машинным интерфейсом
7. Процесс проектирования систем КИПиУ, важных для безопасности	2. Система менеджмента для проектирования СКУ: Деятельность, осуществляемая в течение жизненного цикла: модификации

СПРАВОЧНЫЙ МАТЕРИАЛ ДЛЯ ПРИЛОЖЕНИЯ II

[II–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna (2011).

Приложение III

ОБЛАСТИ, В КОТОРЫХ ГОСУДАРСТВА-ЧЛЕНЫ ПРИДЕРЖИВАЮТСЯ РАЗЛИЧНОЙ ПРАКТИКИ

ВВЕДЕНИЕ

III–1. Существует ряд областей, в которых академические основы или инженерно-техническая практика, поддерживающие применение критериев безопасности при проектировании систем контрольно-измерительных приборов и управления (СКУ), не являются общепринятыми в государствах-членах. В данном приложении описываются области, в которых такие различия были выявлены в процессе подготовки настоящего Руководства по безопасности. Предполагается, что с течением времени практика государств-членов будет меняться.

ОПРЕДЕЛЕНИЕ НАДЕЖНОСТИ ЦИФРОВЫХ СИСТЕМ

III–2. Ошибки в программном обеспечении могут приводить к отказам по общей причине в резервированных цифровых системах, если одно и то же программное обеспечение используется для множества резервируемых систем. Следовательно, чтобы оценить надежность цифровой системы, необходимо оценить вероятность отказа системы вследствие отказа аппаратных (технических) средств и — в случае некоторых государств-членов — вероятность ошибок в программном обеспечении. В случае других государств-членов ошибки в проектировании (включая ошибки в программном обеспечении) и связанные с ними последствия анализируются надлежащим образом только посредством качественного анализа архитектуры и проектирования.

III–3. При разработке проектной основы СКУ некоторые государства-члены обеспечивают согласованность между требованиями к надежности СКУ и вероятностным анализом безопасности посредством установления конкретного численного (количественного) показателя надежности для каждой СКУ, важной для безопасности. Поэтому эти государства-члены считают численные оценки надежности цифровых систем необходимым элементом подтверждения надежности.

III–4. В случае государств-членов, применяющих численные показатели надежности в отношении программного обеспечения, заявленная высокая надежность программного обеспечения в настоящее время не может быть подтверждена. Поэтому необходимо с осторожностью походить к проектам, в которых будет применяться одна компьютеризированная система для достижения вероятности отказа при запросе (pdf) ниже 10^{-4} применительно к программному обеспечению.

III–5. Некоторые регулирующие органы, применяющие численные оценки надежности цифровых систем, установили пределы уровня надежности, которые они считают обоснованными для СКУ. Например, заявленный показатель надежности СКУ, базирующихся на общей платформе, вне зависимости от применяемой технологии, ограничивается показателем, равным 10^{-5} pfd, а заявленный показатель надежности любой отдельной СКУ, базирующейся на общей компьютеризированной платформе, ограничивается показателем 10^{-4} pfd, не зависимо от степени, в которой используются принципы, изложенные в настоящем Руководстве по безопасности (например, резервирование).

III–6. Некоторые государства-члены используют качественный подход к определению надежности программного обеспечения. Такой качественный подход, как правило, основывается на жестких требованиях в отношении детерминированного поведения программного обеспечения в целях проведения верификации и валидации в полном объеме. Набор жестких проектных требований, обеспечивающий проведение полной верификации и валидации, позволяет достичь высокого уровня достоверности показателей надежности программного обеспечения.

ОЦЕНКА УЯЗВИМОСТЕЙ ПО ОБЩЕЙ ПРИЧИНЕ В СИСТЕМАХ БЕЗОПАСНОСТИ

III–7. В пункте 4.32 настоящего Руководства по безопасности содержится следующая рекомендация:

> «Следует провести анализ последствий от каждого постулируемого исходного события в рамках анализа безопасности, в сочетании с анализом отказов по общей причине, которые могут повлечь ненадлежащее выполнение защитной системой своих функций».

В отношении этой рекомендации имеется согласие в целом, однако в том, что касается конкретно объема анализа, радиологических последствий, являющихся приемлемыми в случае возникновения постулируемого исходного события в сочетании с отказом по общей причине в системе безопасности, или типа аналитических методов, используемых для определения радиологических последствий, общего согласия нет.

Объем анализа

III–8. Объем анализа, описанного в пункте 4.32, выполнение которого требуют регулирующие органы, включает, например:

— анализ отказов по общей причине в системе безопасности в сочетании с постулируемыми исходными событиями, которые считаются ожидаемыми при эксплуатации событиями и проектными аварийными условиями;
— анализ отказов по общей причине в системе безопасности в сочетании с постулируемым исходным событием, частота возникновения которого превышает 10^{-3} в год.

Приемлемые последствия

III–9. К примерам последствий, которые регулирующие органы могут признать приемлемыми для случаев, когда постулируемое исходное событие возникает в сочетании с отказом по общей причине в системе безопасности, относятся:

— последствия ожидаемого при эксплуатации события, возникающего в связи с отказом по общей причине в системе защиты реактора, которые не приводят к:
  • нахождению какого-либо лица в любой точке в пределах границ зоны отчуждения в течение 2-х часов после начала выброса продуктов деления, или границ малонаселенной зоны в течение всего периода выброса продуктов деления с получением дозы облучения всего тела свыше 25 мЗв или дозы воздействия йода на щитовидную железу свыше 300 мЗв; или
  • превышению проектных пределов для системы теплоносителя первого контура;

— последствия проектной аварии, возникающей в сочетании с отказом по общей причине в системе защиты реактора, которые не приводят к:
  • нахождению какого-либо лица в любой точке в пределах границ зоны отчуждения в течение 2-х часов после начала выброса продуктов деления, или границ малонаселенной зоны в течение всего периода выброса продуктов деления с получением дозы облучения всего тела свыше 0,25 Зв или дозы воздействия йода на щитовидную железу свыше 3 Зв; или
  • превышению проектных пределов для системы теплоносителя первого контура или защитной оболочки реактора;
— последствия проектной аварии, возникающей в сочетании с отказом по общей причине в системе защиты реактора, при которых оставшиеся системы безопасности должны быть способны:
  • обеспечить соблюдение дозовых пределов, согласованных регулирующим органом и лицензиатом;
  • предотвратить отказ системы теплопереноса первого контура вследствие превышения давления;
  • предотвратить чрезмерное повышение температуры топлива;
  • предотвратить разрушение топлива;
  • ограничить скорость выработки энергии и общую выработку энергии до такой степени, при которой целостность защитной оболочки реактора не ставится под угрозу;
  • поддерживать реактор в подкритическом состоянии в течение времени, достаточного для обеспечения применения альтернативных средств, обеспечивающих подкритичность;
— использование предусмотренных согласно принципу неодинаковости (диверсности) и других средств для предотвращения или ослабления последствий отказа по общей причине с целью обеспечения достаточно высокой степени надежности функционирования системы;
— последствия проектной аварии, не превышающие предельно-допустимые уровни дозы в случае отказа системы безопасности.

Аналитические подходы

III–10. При определении последствий в рамках анализа, описанного в пункте 4.32, некоторые регулирующие органы требуют использования консервативных методов; другие регулирующие органы разрешают применять метод улучшенной оценки. В публикации «Детерминистический анализ безопасности атомных электростанций», Серия норм безопасности МАГАТЭ, № SSG-2 [III–1], описываются консервативные методы и методы улучшенной оценки.

III–11. В случаях, когда для выполнения функций системы защиты используются цифровые системы, анализ, описанный в пункте 4.32 может показывать, что отказы по общей причине в цифровой системе защиты способны приводить к недопустимым последствиям при определенных сочетаниях отказов по общей причине и постулируемых исходных событий. При возникновении подобной ситуации часто требуется система неодинакового привода для резервирования функций системы защиты.

III–12. Превалирует общее мнение относительно того, что система неодинакового привода способна эффективно смягчать последствия конкретных постулируемых исходных событий, возникающих в сочетании с постулируемым отказом по общей причине системы защиты. Вместе с тем существуют разные подходы к классификации по безопасности, использованию цифровых систем неодинакового привода для резервирования цифровой системы защиты и использованию ручного привода для ослабления последствий отказа по общей причине системы защиты.

Классификация по безопасности

III–13. Некоторые регулирующие органы требуют, чтобы системы неодинакового привода классифицировались как системы безопасности. Другие регулирующие органы допускают, что эти системы относятся к классу безопасности более низкого уровня. Третьи регулирующие органы основывают определение класса безопасности на информации о показателях надежности, заявленных для системы неодинакового привода.

Технологии для системы неодинакового привода

III–14. Некоторые регулирующие органы требуют, чтобы системы неодинакового привода были отнесены к аппаратным системам. Другие регулирующие органы рекомендуют воздерживаться от использования, но и не запрещают применение цифровых систем. Третьи регулирующие органы допускают использование цифровых систем, если будет продемонстрирована надлежащая неодинаковость (диверсность).

Применение выполняемых вручную действий для неодинакового привода

III–15. В общем случае применение ручного привода может признаваться в качестве основанного на принципе неодинаковости (диверсности) резервирования системы защиты, однако условия, при которых может применяться ручной привод, варьируются. К принятой практике относится следующее:

— выполняемые вручную действия могут использоваться, если действие не требуется в течение менее чем 30 минут и анализ человеческого фактора подтверждает, что надлежащее решение может быть принято и реализовано в пределах этих временных рамок;
— выполняемые вручную действия могут использоваться, если действие не требуется в течение менее чем 20 минут;
— выполняемые вручную действия могут использоваться для активации инженерно-технических средств безопасности, но не для аварийного останова реактора;
— выполняемые вручную действия могут использоваться без ограничений.

III–16. Несмотря на проиллюстрированный выше спектр различной практики, применяемой регулирующими органами, исходя из конкретной ситуации регулирующий орган может использовать другие подходы.

СПРАВОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРИЛОЖЕНИЯ III

[III–1] МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ, Детерминистический анализ безопасности атомных электростанций, Серия норм безопасности МАГАТЭ, № SSG-2, МАГАТЭ, Вена (2014).

ОПРЕДЕЛЕНИЯ

Приведенные ниже определения предназначены конкретно для настоящей публикации, и они либо отсутствуют, либо отличаются от определений, приведенных в Глоссарии МАГАТЭ по вопросам безопасности. Терминология, используемая в области ядерной безопасности и радиационной защиты (издание 2007 года), МАГАТЭ, Вена (2007):

https://www-pub.iaea.org/MTCD/publications/PDF/IAEASafetyGlossary2007/Glossary/SafetyGlossary_2007r.pdf

Символ «» обозначает определение, которое отличается от определения, приведенного в Глоссарии МАГАТЭ по вопросам безопасности.*

анализ опасностей. Процесс анализа системы в течение ее жизненного цикла с целью выявить присущие опасности и сопутствующие опасности, а также требования и ограничения, направленные на их устранение, предотвращение или контроль.

Примечание: Объем анализа опасностей выходит за пределы проектных аварий и включает ненормальные события и эксплуатацию станции с деградировавшими системами и оборудованием станции.

аппаратно-программное обеспечение (firmware). Программное обеспечение, имеющее тесную связь с характеристиками аппаратного обеспечения, на котором оно установлено.

архитектура. Организационная структура систем контроля и управления станции, которые являются важными для безопасности.

валидация*. Подтверждение посредством анализа и предоставления других доказательств того, что обеспечивается полное и надлежащее выполнение системой установленных требований.

верификация*. Подтверждение посредством анализа и предоставления объективных доказательств того, что результаты какой-либо деятельности соответствуют целям и требованиям, определенным для такого вида деятельности.

готовность (эксплуатационная)*. Способность узла (единицы оборудования), характеризуемая состоянием выполнять требуемую функцию в определенных условиях, в определенный момент времени или в течение определенного отрезка времени при наличии необходимых внешних ресурсов.

детерминированная синхронизация. Характеристика системы или компонента, согласно которой время задержки между стимулом и реакцией имеет гарантированные максимальное и минимальное значения.

детерминированное поведение. Характеристика системы или компонента, согласно которой любая данная входная последовательность, соответствующая спецификациям узла (единицы оборудования), всегда дает одинаковые выходные результаты.

запрограммированное на аппаратном уровне устройство. Запрограммированное на аппаратном уровне устройство может быть сконфигурированной (для систем контроля и управления на атомной электростанции) интегральной схемой с языками описания аппаратных средств и соответствующими программными инструментами.

калибровка*. Набор операций, устанавливающих при определенных условиях отношение между значениями величин, показания которых были получены с помощью измерительного прибора или измерительной системы, или значениями, представленными мерами физических величин или эталонным материалом, и соответствующими значениями, зафиксированными в нормах.

компонент*. Элемент, входящий в состав системы. Компонент может являться частью как аппаратных (технических) средств, так и программного обеспечения и может подразделяться на другие элементы.

Примечание: Термины «оборудование», «компонент» и «модуль» часто употребляются как взаимозаменяемые. Взаимосвязь между этими терминами еще не стандартизирована.

конфигурационный базис. Набор конфигурационных единиц, формально определенный и утвержденный на данное время в течение жизненного цикла единицы оборудования.

неодинаковость (диверсность)*. Наличие двух или более резервных систем или элементов для выполнения определенной функции, при котором разные системы или элементы наделяются разными признаками таким образом, чтобы уменьшалась возможность отказа по общей причине, включая общий отказ.

Примечание 1: Если термин «неодинаковость» употребляется с дополнительным определительным признаком, он имеет общее значение, выражающее «наличие двух или более разных способов или средств достижения конкретной цели», при этом определительный признак указывает на характеристики разных применяемых способов, например, функциональная неодинаковость, неодинаковость оборудования, неодинаковость сигналов.

Примечание 2: См. также статью «функциональная неодинаковость» в Глоссарии МАГАТЭ по вопросам безопасности.

нефункциональные требования (также именуемые требованиями к качеству). Требования, в которых указываются присущие узлу (единице оборудования) свойства и характеристики, которые не входят в число требуемых функций и алгоритмов поведения. Например, анализируемость, гарантируемость, контролируемость, эксплуатационная готовность, совместимость, документирование, целостность, ремонтопригодность, надежность, безопасность, физическая безопасность, эксплуатационная пригодность и верифицируемость.

опасность. Потенциальная возможность причинения ущерба/повреждения.

сопутствующая опасность. Фактор, способствующий возникновению угрозы ущерба/повреждения.

отдельная группа. Набор единиц оборудования, включая их соединения, которые образуют один резерв какой-либо резервной системы или группы безопасности. В отдельные группы могут входить многоканальные системы.

программируемая пользователем вентильная матрица. Интегральная схема, которая может программироваться на месте изготовителем системы контроля и управления. Она включает программируемые логические блоки (комбинаторные или последовательные), программируемые переключатели блоков и программируемые блоки для входов и/или выходов. Функция затем определяется разработчиком системы контроля и управления, а не изготовителем схемы.

разработка требований. Процесс разработки, включающий деятельность по подготовке, документированию и хранению набора требований.

ранее разработанный блок. Разработанный ранее блок, который можно использовать в языке описания аппаратных средств. К ранее разработанным блокам относятся, например, библиотеки, макрокоманды или ядра, являющиеся интеллектуальной собственностью. Для использования ранее разработанного блока в запрограммированном на аппаратном уровне устройстве может потребоваться значительная доработка.

ранее разработанное изделие. Уже существующее изделие, доступное в качестве коммерческого или проприетарного продукта, для которого рассматривается возможность использования в СКУ. В число ранее разработанных изделий входят аппаратные средства, ранее разработанное программное обеспечение, готовые коммерческие устройства, цифровые устройства, включающие как аппаратные, так и программные средства, или аппаратные (технические) устройства, конфигурированные с применением языком описания аппаратных средств, или ранее разработанные функциональные блоки.

статический анализ. Анализ системы или компонента на основе ее или его формы, структуры, содержания или документации.

типовое испытание. Тест на соответствие, выполняемый на одном или нескольких изделиях, представляющих данную продукцию.

функциональные требования. Требования, в которых указываются требуемые функции или алгоритмы поведения узла (единицы оборудования).

человеко-машинный интерфейс. Средство взаимодействия эксплуатационного персонала с системами контроля и управления и компьютерными системами, связанными со станцией. Интерфейс включает средства отображения информации, средства управления и средства взаимодействия с системой поддержки оператора.

язык описания аппаратных средств. Язык, позволяющий формально описать функции и/или структуру электронного компонента для целей документирования, моделирования или обобщения данных.

СОСТАВИТЕЛИ И РЕЦЕНЗЕНТЫ

Алпеев, А.	Научно-технический центр по ядерной и радиационной безопасности Ростехнадзора, Российская Федерация
Alvarado, R.	Комиссия по ядерному регулированию, Соединенные Штаты Америки
Asikainen, S.	«Теоллисууден войма оий», Финляндия
Babcock, B.	«Онтарио пауэр дженерейшн», Канада
Benitez-Read, J.	Национальный институт ядерных исследований, Мексика
Bicer, C.	Управление по атомной энергии Турции, Турция
Боева, Т.	атомная электростанция «Козлодуй», Болгария
Bouard, J.-P.	«Электрисите де Франс», Франция
Bowell, M.	Управление по ядерному регулированию, Соединенное Королевство
Curtis, D.	консультант
Debor, J.	консультант
Duchac, A.	Международное агентство по атомной энергии
Edvinsson, H.	«Ваттенфалль», Швеция
Eriksson, K.-E.	атомная электростанция «Оскарсхамн», Швеция
Faya, A.	Федеральное управление по ядерному регулированию, Объединенные Арабские Эмираты
Fichman, R.	«Онтарио пауэр дженерейшн», Канада
Furieri, E.-B.	Национальная комиссия по ядерной энергии, Бразилия

Gassino, J.	Институт радиационной защиты и ядерной безопасности, Франция
Гончуков, В.	Ростехнадзор, Российская Федерация
Göring, M.	«Ваттенфалль», Германия
Harber, J.	«Атомик энерджи оф Кэнада лимитед», Канада
Hohendorf, R.	«Онтарио пауэр дженерейшн», Канада
Johnson, G.	Международное агентство по атомной энергии
Karasek, A.	«ЧЕЗ», Чешская Республика
Kawaguchi, K.	Управление по ядерному регулированию, Япония
Kim, B.-Y.	Корейский институт ядерной безопасности, Республика Корея
Клопков, В.	Ростехнадзор, Российская Федерация
Lee, J.-S.	Корейский научно-исследовательский институт атомной энергии, Республика Корея
Li, H.	Комиссия по ядерному регулированию, Соединенные Штаты Америки
Lindskog, U.	атомная электростанция «Оскарсхамн», Швеция
Mangi, A.	Ядерный регулирующий орган Пакистана, Пакистан
Ngo, C.	«Кандеско», Канада
Odess-Gillett, W.	«Вестингауз», Соединенные Штаты Америки
Park, H.-S.	Корейский институт ядерной безопасности, Республика Корея
Parsons, A.	«АМЕК», Соединенное Королевство
Piljugin, E.	Общество по безопасности установок и реакторов, Германия
Poulat, B.	Международное агентство по атомной энергии

Régnier, P.	Институт радиационной защиты и ядерной безопасности, Франция
Santos, D.	Комиссия по ядерному регулированию, Соединенные Штаты Америки
Seidel, F.	Федеральное ведомство по радиационной защите, Германия
Шумов, С.	Специализированный научно-исследовательский институт приборостроения, Российская Федерация
Sjövall, H.	«Теоллисууден войма оий», Финляндия
Stattel, R.	Комиссия по ядерному регулированию, Соединенные Штаты Америки
Svensson, C.	атомная электростанция «Оскарсхамн», Швеция
Takala, H.	Управление по радиационной и ядерной безопасности, Финляндия
Takita, M.	Управление по ядерному регулированию, Япония
Tate, R.	Управление по ядерному регулированию, Соединенное Королевство
Thuy, N.	«Электрисите де Франс», Франция
Welbourne, D.	консультант
Ястребенецкий, М.	Государственный научно-технический центр по ядерной и радиационной безопасности, Украина
Yates, R.	Управление по ядерному регулированию, Соединенное Королевство
Zeng, Z.-C.	Комиссия по ядерной безопасности Канады, Канада

ЗАКАЗ В СТРАНАХ

В указанных странах платные публикации МАГАТЭ могут быть приобретены у перечисленных ниже поставщиков или в крупных книжных магазинах.

Заказы на бесплатные публикации следует направлять непосредственно в МАГАТЭ. Контактная информация приводится в конце настоящего перечня.

ГЕРМАНИЯ

Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Телефон: +49 (0) 211 49 874 015 • Факс: +49 (0) 211 49 874 28
Эл. почта: kundenbetreuung.goethe@schweitzer-online.de • Сайт: www.goethebuch.de

ИНДИЯ

Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Телефон: +91 22 4212 6930/31/69 • Факс: +91 22 2261 7928
Эл. почта: alliedpl@vsnl.com • Сайт: www.alliedpublishers.com

Bookwell
3/79 Nirankari, Delhi 110009, INDIA
Телефон: +91 11 2760 1283/4536
Эл. почта: bkwell@nde.vsnl.net.in • Сайт: www.bookwellindia.com

ИТАЛИЯ

Libreria Scientifica “AEIOU”
Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Телефон: +39 02 48 95 45 52 • Факс: +39 02 48 95 45 48
Эл. почта: info@libreriaaeiou.eu • Сайт: www.libreriaaeiou.eu

КАНАДА

Renouf Publishing Co. Ltd
22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Телефон: +1 613 745 2665 • Факс: +1 643 745 7660
Эл. почта: order@renoufbooks.com • Сайт: www.renoufbooks.com

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Тел: +1 800 462 6420 • Факс: +1 800 338 4550
Эл. почта: oorders@rowman.com Сайт: www.rowman.com/bernan

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Научно-технический центр по ядерной и радиационной безопасности
107140, Москва, Малая Красносельская ул, д. 2/8, кор. 5, РОССИЙСКАЯ ФЕДЕРАЦИЯ
Телефон: +7 499 264 00 03 • Факс: +7 499 264 28 59
Эл. почта: secnrs@secnrs.ru • Сайт: www.secnrs.ru

СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ

Bernan / Rowman & Littlefield
15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Тел: +1 800 462 6420 • Факс: +1 800 338 4550
Эл. почта: orders@rowman.com • Сайт: www.rowman.com/bernan

Renouf Publishing Co. Ltd
812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Телефон: +1 888 551 7470 • Факс: +1 888 551 7471
Эл. почта: orders@renoufbooks.com • Сайт: www.renoufbooks.com

ФРАНЦИЯ

Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Телефон: +33 1 42 01 49 49 • Факс: +33 1 42 01 90 90
Эл. почта: formedit@formedit.fr • Сайт: www.form-edit.com

ЧЕШСКАЯ РЕСПУБЛИКА

Suweco CZ, s.r.o.
Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Телефон: +420 242 459 205 • Факс: +420 284 821 646
Эл. почта: nakup@suweco.cz • Сайт: www.suweco.cz

ЯПОНИЯ

Maruzen-Yushodo Co., Ltd
10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Телефон: +81 3 4335 9312 • Факс: +81 3 4335 9364
Эл. почта: bookimport@maruzen.co.jp • Сайт: www.maruzen.co.jp

***З*аказы на платные и бесплатные публикации можно направлять напрямую по адресу:**

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Телефон: +43 1 2600 22529 или 22530 • Факс: +43 1 26007 22529
Эл. почта: sales.publications@iaea.org • Сайт: www.iaea.org/books

18-02421R

Обеспечение безопасности с помощью международных норм

«Обязанность правительств, регулирующих органов и операторов во всем мире — обеспечивать полезное, безопасное и разумное применение ядерных материалов и источников излучения. Нормы безопасности МАГАТЭ предназначены способствовать этому, и я призываю все государства-члены пользоваться ими.»

Юкия Амано
Генеральный директор

МЕЖДУНАРОДНОЕ АГЕНТСТВО ПО АТОМНОЙ ЭНЕРГИИ
ВЕНА
ISBN 978–92–0–406118–5
ISSN 1020–5845