ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 60987— 2011

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризованных систем

IEC 60987:2007
Nuclear power plants —
Instrumentation and control systems important to safety —
Hardware design requirements for computer-based systems
(IDT)

Издание официальное

Москва
Стандартинформ
2012

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 Подготовлен Автономной некоммерческой организацией «Измерительно-информационные технологии» (АНО «Изинтех») и Открытым акционерным обществом «Всероссийский научно-исследовательский институт по эксплуатации атомных электростанций» (ОАО «ВНИИАЭС») на основе аутентичного перевода на русский язык стандарта, указанного в пункте 4, выполненного Российской комиссией экспертов МЭК/ТК 45

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 322 «Атомная техника»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 12 декабря 2011 г. № 771-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 60987:2007 «Атомные станции. Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризированных систем» (IEC 60987:2007 «Nuclear power plants — Instrumentation and control systems important to safety — Hardware design requirements for computer-based systems»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

Содержание

Введение

a) Технические положения, основные вопросы и организация стандарта

Основные принципы конструирования аппаратуры ядерного приборостроения, специально применяемой в системе безопасности атомных станций, впервые были сформулированы в стандартах ядерной области для аппаратных систем в Руководстве по безопасности МАГАТЭ 50-SG-D3, которое было заменено на Руководство МАГАТЭ NS-G-1.3.

Первое издание МЭК 60987 относится к 1989 г., и в нем были рассмотрены аспекты проектирования аппаратных цифровых систем для систем, важных для безопасности, т. е. систем безопасности и систем, связанных с безопасностью.

Несмотря на то, что многие требования, представленные в первом издании, остаются актуальными, существовали важные факторы, потребовавшие его переработки. Особо следует отметить, что:

- был разработан новый стандарт, который подробно описывает общие требования к ядерным системам, важным для безопасности (см. МЭК 61513);
- значительно увеличилось использование ранее разработанных платформ для систем, а не только заказов на разработки новых платформ.

b) Место настоящего стандарта в структуре серии стандартов МЭК ПК 45А

Стандартом первого уровня серии стандартов МЭК ПК 45А по компьютеризированным системам, важным для безопасности на атомных станциях, является МЭК 61513. МЭК 60987 является документом второго уровня серии стандартов МЭК ПК 45А и рассматривает типовые вопросы проектирования аппаратных средств автоматизированных систем.

МЭК 60880 и МЭК 62138 являются документами второго уровня и рассматривают аспекты программного обеспечения компьютеризированных систем, используемых для выполнения функций, важных для безопасности на атомных станциях. МЭК 60880 и МЭК 62138 дают прямую ссылку на МЭК 60987 по вопросу проектирования аппаратных средств.

МЭК 60987 ссылается на требования к квалификации оборудования, представленные в МЭК 60780. Для модулей, используемых при конструировании определенной системы, важной для безопасности, может применяться метод квалификации вместе с использованием строгих программ обеспечения качества. Данный метод характеризуется и подтверждается опытом эксплуатации в ядерной или другой области применения, как описано в МЭК 60780.

Детальная информация о структуре серии МЭК ПК 45А представлена в пункте d) настоящего введения.

c) Рекомендации и ограничения по применению настоящего стандарта

Необходимо отметить, что настоящий стандарт не устанавливает дополнительные функциональные требования к системам классов 1 или 2 (см. МЭК 61513, в котором представлены требования к классификации системы).

В настоящем стандарте были разработаны специальные рекомендации (с тем, чтобы гарантировать производство очень надежных систем) по таким аспектам, как:

- общий подход к разработке компьютеризированных аппаратных средств;
- общий подход к верификации аппаратных средств и аспектам аппаратных средств валидации компьютеризированной системы.

Компьютерные технологии продолжают развиваться, и подобный настоящему стандарт не может включать в себя ссылки на все современные технологии и методы проектирования. Для обеспечения дальнейшей актуальности стандарта особое значение было уделено основным принципам, а не определенным технологиям проектирования аппаратных средств. Для вновь разработанных новых методов проектирования необходимо оценить их соответствие, адаптируя и применяя принципы разработки, представленные в настоящем стандарте.

Область применения настоящего стандарта включает в себя цифровые аппаратные средства систем классов 1 и 2. Они также включают в себя мультипроцессорные распределенные системы и однопроцессорные системы, область применения которых охватывает оценку и использование ранее разработанных элементов, например, серийных готовых изделий (COTS), а также разработку новых аппаратных средств.

d) Описание структуры серии стандартов МЭК ПК 45А и взаимосвязь с другими документами МЭК и документами других организаций (МАГАТЭ, ИСО)

Документом высшего уровня серии стандартов МЭК ПК 45А является МЭК 61513. Этот стандарт касается требований к системам контроля и управления, важных для безопасности атомных станций (АС), и лежит в основе серии стандартов ПК 45А.

В МЭК 61513 имеются непосредственные ссылки на другие стандарты ПК 45А по общим вопросам, связанным с категоризацией функций и классификацией систем, оценкой соответствия, разделением систем, защитой от отказов по общей причине, аспектами программного и технического обеспечений компьютерных систем и проектированием пультов управления. Стандарты, на которые имеются непосредственные ссылки, следует использовать на втором уровне совместно с МЭК 61513 в качестве согласованной подборки документов.

К третьему уровню серии стандартов МЭК ПК 45А, на которые в МЭК 61513 нет непосредственных ссылок, относятся стандарты, связанные с конкретным оборудованием, техническими методами или конкретной деятельностью. Обычно документы, в которых по общим вопросам имеются ссылки на документы второго уровня, могут использоваться самостоятельно.

Четвертому уровню, продолжающему серию стандартов МЭК ПК 45А, соответствуют технические отчеты, не являющиеся нормативными документами.

Для МЭК 61513 принята форма представления, аналогичная форме представления базовой публикации по безопасности МЭК 61508, с его структурой общего жизненного цикла безопасности и структурой жизненного цикла системы; в нем приведена интерпретация общих требований МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 для применения в ядерной области. Согласованность с этим стандартом будет способствовать соответствию требованиям МЭК 61508, интерпретированным для ядерной области. В этой структуре МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3, применительно к ядерной области.

В МЭК 61513 приведены ссылки на стандарты ИСО, а также на документ МАГАТЭ 50-С-QA по вопросам, связанным с обеспечением качества.

В серии стандартов МЭК ПК 45А последовательно реализуются и детализируются принципы и базовые аспекты безопасности, предусмотренные правилами МАГАТЭ по безопасности атомных электростанций, а также серией документов МАГАТЭ по безопасности, в частности требованиями NS-R-1 «Безопасность атомных электростанций: Проектирование» и руководством по безопасности NS-G-1.3 «Системы контроля и управления, важные для безопасности атомных электростанций». Термины и определения, применяемые в стандартах серии МЭК ПК 45А, согласованы с терминами и определениями, применяемыми в МАГАТЭ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

АТОМНЫЕ СТАНЦИИ

Системы контроля и управления, важные для безопасности. Требования к разработке аппаратного обеспечения компьютеризованных систем

Nuclear power plants. Instrumentation and control systems important to safety.
Hardware design requirements for computer-based systems

Срок действия с 2012—07—01 до 2017—07—01

1 Область применения

1.1 Общие положения

Настоящий стандарт распространяется на аппаратные средства компьютерных систем классов 1 и 2 (как определено в МЭК 61513).

Структура настоящего стандарта не имеет существенных отличий по сравнению с изданием 1989 г., однако некоторые вопросы рассматриваются в стандартах, издаваемых в настоящее время (например, МЭК 61513, для проектирования архитектуры системы), а также, где это возможно, даются ссылки на новые стандарты. Текст настоящего стандарта изменен с тем, чтобы отражать процессы разработки аппаратных средств для компьютерных систем, использование ранее разработанных (например, готовых коммерческих изделий) аппаратных средств и изменения в терминологии.

Компьютерные аппаратные средства, используемые для загрузки программного обеспечения и его проверки, в качестве составной части системы, важной для безопасности, в настоящем стандарте не рассматриваются.

Примечание 1 — Аппаратные средства компьютерной системы категории 3 не рассматриваются в настоящем стандарте, и для таких систем рекомендуется разработать необходимые документы в целях их использования в торговых отношениях.

Примечание 2 — В 2006 г. в рамках МЭК ПК 45А обсуждалась разработка нового стандарта, отражающего требования к «очень сложным» аппаратным средствам. Если бы такой стандарт был в это время разработан, то использовался бы при разработке «очень сложных» аппаратных средств вместо МЭК 60987.

1.2 Использование настоящего стандарта для оценки ранее разработанных аппаратных средств (например, коммерческих продуктов)

Несмотря на то, что главная цель настоящего стандарта состоит в изложении основных аспектов разработки новых аппаратных средств, процессы, определенные в настоящем стандарте, могут также использоваться для оценки и использования ранее разработанных аппаратных средств, таких как готовые коммерческие аппаратные средства. Текст настоящего стандарта содержит руководство по интерпретации требований стандарта для оценки ранее разработанных аппаратных средств. В частности, применяются требования по обеспечению качества в пункте 4.3 относительно управления конфигурацией.

Ранее разработанные устройства могут использовать аппаратно-программное обеспечение (как определено в 3.8), и там, где встроенное программное обеспечение широко используется и фактически «прозрачно» для пользователя, МЭК 60987 должен использоваться для контроля процесса оценки таких устройств. Примером использования такого подхода является оценка современных процессоров, содержащих микрокод. Такой микрокод, как правило, является неотъемлемой частью «аппаратных средств» и поэтому целесообразно проводить оценку процессора (включая микрокод) как единого компонента аппаратных средств, с применением настоящего стандарта.

Издание официальное

Программное обеспечение, которое не является аппаратно-программным, как описано выше, должно рассматриваться или проверяться в соответствии с требованиями соответствующего стандарта на программное обеспечение (например, МЭК 60880 для систем класса 1 и МЭК 62138 — для систем класса 2).

1.3 Использование настоящего стандарта при разработке программируемых логических устройств

Устройства управления и контроля могут включать в себя программируемые логические устройства, для которых разработчик устройств управления и контроля в отличие от изготовителя микросхем применяет специальную систему проектирования логических устройств. Примерами таких устройств являются сложные программируемые логические устройства и программируемые пользователем вентильные матрицы.

Программируемость этих устройств предполагает применение специальных процессов разработки этих устройств. Некоторые особенности процесса разработки программного обеспечения и процессов проектирования, применяемых для таких устройств, подобны употребляемым для логических схем проектирования при создании элементов на дискретных компонентах и интегральных схемах. Поэтому процессы разработки и верификации, применяемые к программируемым логическим устройствам, должны отвечать соответствующим требованиям, представленным в настоящем стандарте (т. е. необходимо учесть специфические особенности процессов разработки таких устройств). Поскольку для поддержки процессов разработки программируемых логических устройств используются инструментальные средства программного обеспечения, то эти технологические средства должны строго следовать требованиям по разработке программных средств, представленным в соответствующем стандарте по программному обеспечению, т. е. МЭК 60880 (системы класса 1) или МЭК 62138 (системы класса 2).

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы. Если указана дата публикации, то именно данное издание следует использовать. При отсутствии даты публикации используют последнее издание указанного документа, включая любые изменения.

МЭК 60780 Атомные станции. Электрооборудование, относящееся к системам безопасности. Квалификация (IEC 60780, Nuclear power plants — Electrical equipment of the safety system — Qualification)

МЭК 60812 Методы анализа надежности систем. Процедура анализа типов отказов и их последствий (FMEA) [IEC 60812, Analysis techniques for system reliability — Procedures for failure mode and effects analysis (FMEA)]

МЭК 60880 Атомные электростанции. Системы контроля и управления, важные для безопасности. Аспекты программного обеспечения компьютерных систем, выполняющих функции категории А (IEC 60880, Nuclear power plants — Instrumentation and control systems important to safety — Software aspects for computer-based systems performing category A functions)

МЭК 61000 (все части) Электромагнитная совместимость (EMC) [IEC 61000 (all parts), Electromagnetic compatibility (EMC)]

МЭК 61025 Анализ, осуществляемый с помощью дерева отказов (FTA) [IEC 61025, Fault tree analysis (FTA)]

МЭК 61513:2001 Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования к системам (IEC 61513:2001, Nuclear power plants — Instrumentation and control for systems important to safety — General requirements for systems)

МЭК 62138 Атомные электростанции. Устройства управления и контроля, важные для безопасности. Аспекты программного обеспечения для компьютерных систем, выполняющих функции категории В или С (IEC 62138, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions

ИСО 9001 Системы управления качеством. Требования (ISO 9001, Quality management systems — Requirements)

Руководство МАГАТЭ NS-G 1.3 Системы контроля и управления, важные для безопасности на атомных электростанциях (IAEA NS-G 1.3, Instrumentation and control systems important to safety in nuclear power plants)

Руководство МАГАТЭ 50-C/SG-Q:1996 Гарантия качества безопасности на атомных электростанциях и других ядерных установках (IAEA 50-C/SG-Q:1996, Quality assurance for safety in nuclear power plants and other nuclear installations)

3 Термины и определения

В настоящем стандарте применены термины и сокращения по МЭК 61513, а также следующие термины с соответствующими определениями:

3.1 **автоматизированная тестовая аппаратура** (automated test equipment; ATE); ATA: —.

3.2 **готовое коммерческое изделие** (commercial off the shelf; COTS); ГКИ: Подгруппа ранее разработанных продуктов.

3.3 **разнообразие** (diversity): Наличие двух или более различных путей или средств достижения установленной цели. Разнообразие специально создается как защита от отказа по общей причине. Оно может быть достигнуто наличием систем, которые физически отличаются одна от другой, или с помощью функционального разнообразия, если аналогичные системы достигают установленной цели различными путями.

[МЭК 60880:2006, определение 3.14]

Примечание — Это определение шире используемого в IAEA NS-G-1.3: «наличие двух или более систем или компонентов, предназначенных для выполнения определенной функции, где различные системы или компоненты обладают различными свойствами, чтобы уменьшить возможность общего отказа».

[МЭК 61226:2005, определение 3.5]

3.4 **аппаратно-программное обеспечение** (firmware): Программное обеспечение, которое тесно связано с особенностями аппаратных средств, на которые оно установлено. Наличие аппаратно-программного обеспечения, как правило, очевидно пользователю аппаратного средства и может фактически рассматриваться как неотъемлемая часть разработки аппаратных средств (хорошим примером такого программного обеспечения является микрокод процессора). Как правило, аппаратно-программное обеспечение может изменяться только пользователем посредством замены компонентов аппаратных средств (например, микросхемы процессора, карты, программируемого постоянного запоминающего устройства), которые используют это программное обеспечение с компонентами, использующими измененное программное обеспечение (аппаратное программное обеспечение). В этом случае конфигурационное управление компонентами аппаратных средств пользователями оборудования фактически обеспечивает конфигурационное управление аппаратно-программным обеспечением. Аппаратно-программное обеспечение фактически рассматривается в настоящем стандарте как программное обеспечение, встроенное в аппаратное средство.

3.5 **анализ типов отказов и их последствий** (failure modes and effects analysis; FMEA): —

3.6 **анализ, осуществляемый с помощью дерева отказов** (fault tree analysis; FTA): —

3.7 **атомная станция** (nuclear power plant; NPP); AC: —

3.8 **ранее разработанный** (pre-developed): Уже существующий элемент, доступный в виде коммерческого или запатентованного продукта и рассматриваемый для использования в компьютеризированной системе.

Примечание — Данное определение соответствует определению ранее разработанного программного обеспечения, представленного в МЭК 61513:2001.

3.9 **квалификационный период** (qualified life): Период, в течение которого путем тестирования, анализа или испытаний подтверждают способность конструкций, системы или компонентов функционировать в соответствии с удовлетворяющими критериями приемлемости при соблюдении определенных условий эксплуатации и с сохранением при этом способности выполнять свои функции по безопасности в случае проектной аварии или землетрясения.

[Глоссарий МАГАТЭ по безопасности: 2006]

3.10 **выявленный отказ аппаратного средства** (revealed hardware failure): Отказ аппаратного средства, который был автоматически обнаружен и подтвержден, например отказ платы, автоматически обнаруженный контрольными средствами с последующей выдачей сигнала тревоги.

3.11 **система, связанная с безопасностью** (safety-related system): Система, важная для безопасности, которая не является частью системы безопасности.

[Глоссарий МАГАТЭ по безопасности: 2006]

3.12 **система безопасности** (safety system): Система, важная для безопасности, предназначенная для обеспечения гарантированной безопасной остановки реактора или устранения остаточного тепла в активной зоне, или уменьшения последствий прогнозируемых нештатных ситуаций и проектных аварий.

[Глоссарий МАГАТЭ по безопасности: 2006]

3.13 **единичный отказ** (single failure): Отказ, который приводит к потере способности системы или элемента выполнять предписанные им функции безопасности, а также любые последующие отказы, являющиеся результатом этого.

[Глоссарий МАГАТЭ по безопасности: 2006]

3.14 **критерий единичного отказа** [single failure criterion (SFC)]: Критерий (или требование), применяемый к системе таким образом, чтобы она обязательно сохраняла способность выполнять свою функцию в случае любого единичного отказа.

[Глоссарий МАГАТЭ по безопасности: 2006]

3.15 **система, важная для безопасности** (system important to safety): Система, которая является частью группы безопасности и/или чье нарушение функционирования или отказ может привести к радиационному облучению персонала промплощадки или лиц из населения.

[Глоссарий МАГАТЭ по безопасности: 2006]

3.16 **валидация системы** (system validation): Подтверждение экспертизой и предоставлением другого свидетельства того, что система полностью отвечает заданным техническим условиям (функциональность, время реакции, устойчивость к дефектам и ошибкам, надежность).

[МЭК 60880:2006, определение 3.42]

3.17 **невыявленный отказ аппаратного средства** (unrevealed hardware failure): Отказ аппаратного средства, который не был автоматически обнаружен системой и который становится очевидным только при попытке использовать функцию, за которую отвечает поврежденное аппаратное средство. Такие отказы могут быть выявлены при функциональном тестировании или эксплуатации системы.

3.18 **верификация** (verification): Подтверждение экспертизой и представление иного объективного доказательства того, что результаты функционирования отвечают целям и требованиям, определенным для такого функционирования (ИСО 12207).

[МЭК 62138:2004, определение 3.35]

4 Структура проекта

4.1 Общие положения

Проект по созданию компьютеризированных систем, важных для безопасности, должен состоять из нескольких этапов. Каждый этап должен быть в некоторой степени автономным, но зависеть от других этапов, которые, в свою очередь, будут зависеть от него. В совокупности различные этапы проекта составляют общий жизненный цикл системы безопасности (см. раздел 5 МЭК 61513, в котором рассмотрены требования к жизненным циклам системы). МЭК 61513 допускает параллельное проведение этапов проекта при условии, что это не нарушает целостность процесса разработки.

Для процесса производства аппаратных средств должен быть разработан план обеспечения качества.

4.2 Составные части проекта

Требования к жизненному циклу создания аппаратных средств, представленных в настоящем стандарте, определяют следующие основные факторы:

a) жизненный цикл создания аппаратных средств должен быть согласован с полным жизненным циклом системы (см. приложение А);

b) каждый промежуточный этап жизненного цикла создания аппаратных средств должен состоять из четко определенных и задокументированных действий;

c) для того, чтобы включить в проект уже существующие аппаратные средства (например, коммерческие), перед использованием они должны быть соответствующим образом проверены, подвергнуты контролю и испытаны;

d) для выполнения задач на каждом этапе должны быть подготовлены соответствующие средства (запасные части, средства проверки и технического обслуживания) и помещения (лаборатории, цеха, площадки и т. д.);

e) каждый этап должен включать в себя опубликование соответствующих документов;

f) каждый этап должен заканчиваться верификацией (см. раздел 7);

g) каждый шаг верификации сопровождается опубликованием отчета о выполненном анализе, достигнутых результатах и каких-либо изменениях конструкции по итогам проведения верификации;

h) график всех работ должен быть построен так, чтобы гарантировать необходимое время для:

1) разрешения любых взаимодействий между фазами создания аппаратных средств и программного обеспечения, требуемых для гарантии совместимости аппаратных средств/программного обеспечения системы,

2) обеспечения достаточного времени для документирования, проведения испытаний, верификации и действий по обеспечению качества.

4.3 Обеспечение качества

Процессы создания и разработки должны соответствовать конкретным требованиям МАГАТЭ 50-C/SGQ (соответствие ИСО 9001 является одним из показателей соответствия этим требованиям).

План обеспечения качества аппаратных средств должен существовать в качестве отдельного(ых) документа(ов) или части общего плана обеспечения качества. Данный план должен включать в себя использование уже существующих аппаратных средств и, при необходимости, разработок новых аппаратных средств. Данный план должен также включать в себя все работы, выполняемые операторами АС, владельцем, подрядчиками и субподрядчиками, как часть процесса разработки.

4.3.1 План обеспечения качества аппаратных средств должен включать в себя следующие этапы, поскольку они применимы к любой конкретной системе или разработке:

a) проектирование и разработка;
b) поставки;
c) изготовление;
d) установка и ввод в эксплуатацию;
e) эксплуатация и техническое обслуживание.

4.3.2 Перед началом процесса проектирования не требуется, чтобы все вышеупомянутые этапы были рассмотрены, но перед началом каждого этапа план, включающий требования к данному конкретному этапу, уже должен выполняться.

4.3.3 План обеспечения качества аппаратных средств охватывает одновременно организацию, управление и выполнение операций, относящихся к обеспечению качества, и включает в себя:

a) контроль документации;
b) проектирование;
c) поставку товаров и услуг;
d) конфигурационное управление инструкциями по строительству, процедурами строительства и чертежами;
e) конфигурационный контроль комплектующих и изделий, используемых для изготовления аппаратных средств системы;
f) действия по управлению качеством, например, официальные проверки;
g) контроль испытаний оборудования;
h) контроль погрузочно-разгрузочных работ, хранения, перевозок аппаратных средств;
i) испытания;
j) контроль несоответствий и операции по исправлению дефектов;
k) регистрация действий по обеспечению качества;
l) внутренние проверки.

5 Требования к аппаратным средствам

5.1 Общие положения

5.1.1 Требования к аппаратным средствам определяются требованиями к системам, важным для безопасности, и являются частью спецификации компьютерной системы (см. раздел 6 МЭК 61513:2001). Спецификация компьютерной системы является изложением характеристик интегрированной аппаратно-программной системы; в спецификации формулируются цели и функции компьютерной системы (системы могут разрабатываться для определенного применения или в целом, т. е. в виде разработки платформы, основанной на полученных стандартных требованиях к системе).

5.1.2 Требования к аппаратным средствам должны быть описаны в спецификации этих средств или в другом документе.

5.1.3 Форма изложения требований к аппаратурным средствам не должна затруднять их понимание, т. е. требования к аппаратным средствам должны быть четкими.

5.1.4 Функциональные требования к аппаратным средствам должны быть однозначными с обеспечением возможности их тестирования и верификации и практически осуществимыми.

5.1.5 Технические условия на аппаратные средства должны представлять собой общее изложение требований с определением аппаратурных функций, важных для безопасности (однако если эти функции и требования представлены в комбинации с системным программным обеспечением, они должны определяться в технических условиях на систему). В технических условиях должны также быть определены требования к разработке аппаратных средств и их надежности, а также к условиям окружающей среды.

5.1.6 Требования к аппаратным средствам компьютерных систем включают в себя общие требования к аппаратуре и требования, непосредственно относящиеся только к аппаратным средствам компьютерной системы (например, к кабельной сети, обработке поверхности корпусов).

5.1.7 Функциональные требования к аппаратным средствам должны описывать то, что должно быть сделано, а не как это сделано. Однако использование уже существующих компонентов/платформ может привести к разработке аппаратных средств «снизу—вверх». Прежде чем отобрать такие уже существующие компоненты для использования, необходимо провести оценку для подтверждения того, что особенности функционирования аппаратных средств (например, типы отказа) совместимы с требованиями системы. Если будут найдены какие-нибудь аномалии, они должны быть урегулированы посредством изменения проекта аппаратных средств или проекта системы (должна быть гарантия, что требования к ядерной безопасности системы не ставятся под угрозу).

5.2 Требования к функциям и рабочим характеристикам аппаратных средств

5.2.1 Требования к функциям и рабочим характеристикам аппаратных средств вытекают из требований к системам, важным для безопасности.

5.2.2 Функциональные требования и требования к рабочим характеристикам аппаратных средств вместе с требованиями к программному обеспечению (в степени, необходимой для рассмотрения всех требований к аппаратным средствам) должны быть проверены на соответствие требованиям к системам, важным для безопасности.

5.2.3 Все части системы, вплоть до уровня ее составных элементов, содержащие программное обеспечение, должны быть идентифицированы в соответствии с 1.2 следующим образом:

a) функциональные требования к аппаратным средствам должны включать в себя (но не ограничиваться) определение:

1) назначения оборудования всей компьютерной системы и каждой подсистемы,

2) числа и типа датчиков и исполнительных механизмов, присоединенных к компьютерной системе,

3) числа и типов устройств для человеко-машинных интерфейсов, таких как дисплеи, печатающие устройства и клавиатуры;

b) каждый компонент или подсистема, поставляемые поставщиками и предназначенные для включения в систему, должны быть снабжены спецификациями, включающими в себя все аспекты безопасности функционирования конкретного устройства. При отсутствии такой спецификации необходимо провести анализ для определения особенностей проекта аппаратных средств и подтверждения пригодности таких компонентов или подсистем;

c) требования к рабочим характеристикам аппаратных средств должны включать в себя (для любого применения):

1) требуемую скорость сбора данных,

2) требуемую производительность обработки данных,

3) требуемую точность вычисления,

4) требуемую надежность/готовность,

5) требуемый интерфейс коммуникаций (протоколы, скорость передачи данных),

6) требуемые точности вычислений и преобразований,

7) требуемые параметры подавления помех,

8) требуемое время отклика,

9) физические ограничения размера,

10) географические требования (например, длину линии передачи данных),

11) требуемый уровень резервной мощности (если требуется),

12) требования к условиям эксплуатации,

13) требования к источникам электроэнергии;

d) должны быть определены любые ограничения, наложенные на разработку аппаратных средств системой, или на разработку программного обеспечения.

5.3 Требования к надежности/готовности

5.3.1 Требования к надежности/готовности аппаратных средств должны соответствовать общим требованиям, предъявляемым к надежности системы. Требования к надежности/готовности должны включать в себя описание типов допустимых отказов, не вызывающих потерю всех функций или ограниченную потерю конкретной функции. Должны быть определены цели надежности аппаратных средств.

Примечание — Надежность аппаратных средств в данном контексте касается случайных отказов аппаратных средств и исключает любое рассмотрение отказов из-за логических погрешностей проекта.

5.3.2 Независимо от требований, предъявляемых к надежности/готовности аппаратных средств, полная архитектура систем управления и контроля АС должна соответствовать критериям единичного отказа МАГАТЭ NS-G-1.3 (см. 3.6).

5.3.3 В требованиях к оборудованию должны быть представлены плановые показатели параметров надежности аппаратных средств, таких как «среднее время между (выявленными) отказами», «среднее время между (невыявленными) отказами», «среднее время на ремонт для (выявленных) отказов». Любое требование надежности должно быть подкреплено подробным анализом проекта аппаратных средств, например, анализом подэлемента, уровня карты или компонента.

5.3.4 Для анализа надежности и последствий отказа системы аппаратных средств применимы следующие методы:

- анализ дерева отказов, описывающий и проводящий оценку условий и факторов, вызывающих или способствующих возникновению определенных нежелательных явлений (см. МЭК 61025 в рамках данного метода);

- анализ характера и последствий отказов, описывающий отказы, последствия которых оказывают значительное влияние на рабочие характеристики системы, например, на надежность, безопасность, эксплуатационную готовность (см. МЭК 60812 в рамках данного метода).

Там, где это необходимо, для обеспечения гарантии того, что любые потенциальные отказы аппаратных средств не приведут к нежелательным последствиям для ядерной безопасности, к системам аппаратных средств классов 1 и 2, должен применяться соответствующий метод анализа.

5.3.5 С использованием такого метода, как анализ дерева отказов с известными данными по отказу компонента, можно получить вычисленные значения характеристик надежности аппаратных средств системы. Такой подход должен использоваться при анализе аппаратных средств системы класса 1 (см. МЭК 61513), если отсутствует необходимый эксплуатационный опыт, подтверждающий достижимость целей надежности аппаратных средств. Такой метод должен также применяться для систем класса 2 или, в качестве альтернативы, для подтверждения соответствия надежности, обеспеченной на основе качественных причин (например, надежности качества компонентов, аппаратного резервирования, эксплуатационного опыта, отношения выявленных отказов аппаратных средств к невыявленным отказам аппаратных средств и т. д.), особенно если требования к надежности аппаратных средств не являются жесткими.

5.3.6 Должна быть определена стратегия и средства обеспечения надежности компьютерной системы на протяжении всего срока ее службы. Эти меры должны представлять собой требования к техобслуживанию, являющиеся частью требований надежности. Требования к техобслуживанию должны включать в себя требования, предотвращающие возникновение неполадок во время техобслуживания, которые могут привести к отказам по общей причине. Техническое обслуживание различных групп оборудования считается наиболее вероятной причиной таких неполадок, и поэтому системы должны быть разработаны так, чтобы сократить потребность использования подобных методов техобслуживания. Там, где требуется использование техобслуживания, которое может потенциально привести к отказам по общей причине, в требованиях к проекту должна быть определена минимизация риска таких отказов.

5.3.7 Требования к техобслуживанию должны включать в себя (применительно к любой конкретной системе):

a) требования к эксплуатации системы во время технического обслуживания аппаратных средств;

b) замену комплектующих, например, воздушных фильтров;

c) требования регулярной замены подсистем, модулей и компонентов;

d) определение степени повторной валидации аппаратных средств (например, проведение испытаний), необходимой после техобслуживания аппаратных средств.

5.4 Требования к условиям эксплуатации

5.4.1 В требования к условиям эксплуатации аппаратных средств должны быть включены физические ограничения, условия размещения, климатические, сейсмические, химические, электрические и

радиационные условия помещения. Должны также быть включены любые специальные требования, применяемые во время установки и ввода в эксплуатацию аппаратных средств.

5.4.2 Степень защищенности от магнитных, электромагнитных и электрических возмущений должна быть определена условиями эксплуатации и проверена в соответствии с применяемыми стандартами, например, МЭК 61000. Электромагнитная эксплуатационная среда потенциально может подвергаться влиянию со стороны большого числа источников электрического возмущения, например, переключателей, мобильных телефонов, реле, портативной радиоаппаратуры, электростатических разрядов, молний, замыканий на землю.

5.4.3 Конкретные электромагнитные уровни аттестации должны соответствовать практичным оценкам условий эксплуатации при всех вероятных худших случаях.

5.4.4 Требования к аппаратным средствам должны определять любые запрещенные расходные материалы и требования к специальным используемым материалам или особым видам процессов производства.

5.4.5 Если необходим конкретный процесс аттестации аппаратных средств, то он должен быть задокументирован в требованиях к аппаратным средствам.

5.5 Требования к документации

Требования к документации на аппаратные средства являются частью технических требований к документации на компьютеризированные системы (см. МЭК 61513). Поставляемая документация должна включать в себя:

a) документацию проекта (компоненты аппаратных средств системы, разработку аппаратных средств интерфейсов, и т. д.);

b) руководства по работе операторов;

d) руководства по техническому обслуживанию.

6 Проектирование и разработка

6.1 Общие положения

Настоящий раздел распространяется на проектирование и разработку систем, подсистем и модулей.

6.1.1 Информация на входе процесса разработки и проектирования новых аппаратных средств должна базироваться на технических условиях на аппаратные средства. Процесс проектирования должен включать в себя различные этапы проектирования, необходимые для производства аппаратных систем, соответствующих техническим условиям, предъявляемым к разработке и проектированию аппаратных средств.

6.1.2 Самым общим уровнем проектирования можно считать «предварительное» проектирование, состоящее из анализа различных проектных альтернатив с целью определения архитектуры системы в отношении подсистем и модулей.

6.1.3 За предварительным проектом должен следовать один или несколько детализированных уровней проектирования. Детализированный уровень должен расширять предварительный проект до более подробных описаний на уровне подсистем, модулей и компонентов с тем, чтобы описание проекта стало достаточно полным для реализации.

6.1.4 Обычно создается комплект прототипов аппаратных средств, предназначенный, с одной стороны, для демонстрации удовлетворительного взаимодействия модулей и с другой стороны для обеспечения совместной работы аппаратных и программных средств для демонстрации их совместимости.

6.1.5 Ранее разработанные компоненты (например, COTS) могут использоваться для всех аппаратных средств системы или для подгруппы компонентов аппаратных средств. Подразделы 6.2—6.7 рассматривают главным образом ситуацию, при которой требуется проектирование аппаратных средств на заказ; однако там, где это возможно, предоставляют также руководство, определяющее, каким образом требования этих подразделов могут применяться для использования ранее разработанных компонентов.

6.2 Процесс проектирования

6.2.1 Все характеристики работы системы, определенные в требованиях к аппаратным средствам, должны быть проанализированы и указаны в проектной документации; следует также показать, что проект соответствует, по крайней мере, установленным рабочим характеристикам. Эти характеристики должны включать в себя точность вычислений, время отклика, время цикла, условия внешнего окружения и требования к электропитанию (для ранее разработанных компонентов технические условия

аппаратных средств должны быть проверены в соответствии с требованиями к аппаратным средствам системы с тем, чтобы гарантировать соответствие ранее разработанных компонентов указанным требованиям либо проверку качества функционирования аппаратных средств в ходе проведения испытаний).

6.2.2 Лица, отвечающие за изменение проекта и требований к аппаратным средствам, должны обращать внимание на возможные обстоятельства, препятствующие выполнению требований к данным средствам (последствия любых изменений должны быть полностью оценены и задокументированы).

6.2.3 Проектировщики аппаратных средств должны провести и зарегистрировать результаты испытаний, необходимых для подтверждения требуемых рабочих характеристик. Такие испытания могут проводиться как на аппаратных средствах, так и на аппаратных средствах со встроенным программным обеспечением, т. е. испытания проводят на этапе испытания совместимости системы.

6.2.4 Проектировщики должны определить мероприятия по техническому обслуживанию, необходимые для соответствия требованиям к рабочим характеристикам и надежности, выявленным во время полного эксплуатационного цикла оборудования. Эти мероприятия могут включать в себя эксплуатационные испытания, калибровку, ремонт, периодические замены запчастей и процедуры технического обслуживания. Такие действия должны проводиться для обеспечения достаточной уверенности в правильности эксплуатации оборудования, сокращения вмешательства человека в работу оборудования и для сведения к минимуму работ, привести их к поломке. Целью обозначенных выше мероприятий является снижение вероятности ошибок (например, потенциальных ошибок общего отказа), появляющихся во время технического обслуживания.

6.2.5 Должны быть представлены данные, подтверждающие, что установленный срок службы реален и будет достигнут.

6.3 Надежность

6.3.1 Требования к надежности должны быть определены в документации с требованиями к аппаратным средствам (см. 5.3).

6.3.2 Для анализа безопасности уровня системы во время проектирования необходимо провести анализ потенциальных возможностей отказов аппаратных средств. Там, где используются связанные цепи системы или связанные системы (у каждой из которых могут быть те же или различные цепи оборудования) для осуществления функции ядерной безопасности, в этот анализ должно быть включено надлежащее рассмотрение потенциала отказов аппаратных средств по общей причине. Потенциальными причинами отказа аппаратных средств по общей причине могут быть:

- одновременное или последовательное техническое обслуживание нескольких групп оборудования (особенно тогда, когда такие действия могут вызвать невыявленные отказы аппаратных средств);
- периодическое проведение испытаний;
- совпадающие невыявленные случайные отказы аппаратных средств на нескольких группах оборудования, влияющие на выполнение функции(й) по обеспечению ядерной безопасности;
- скрытые недостатки проекта, затрагивающие группы оборудования, не выявленные в процессе проектирования.

6.3.3 Методы, используемые для анализа надежности аппаратных средств и последствий отказов аппаратных средств системы, включают в себя анализ дерева отказов и анализ характера и последствий отказа (см. 5.3.4).

6.3.4 Проектирование аппаратных средств должно минимизировать потенциальное воздействие на ядерную безопасность следующих факторов:

- техническое обслуживание;
- отказ системы из-за случайного отказа аппаратных средств;
- отказ аппаратных средств из-за внешних факторов.

6.3.5 Если проектируемая надежность аппаратных средств считается не соответствующей для определенного назначения, то должны быть проведены корректирующие действия. Такие действия могут быть проведены в форме изменения проекта или выполнены в виде эксплуатационных изменений (таких, как увеличение частоты испытаний в реальных условиях). Однако должны быть предприняты меры предосторожности при выборе увеличенного числа испытаний в реальных условиях, поскольку любые интенсивные действия, осуществленные на предприятии, эксплуатирующем данное оборудование, являются рискованными, поскольку могут привести к появлению повреждений (т. е. влияние системы на безопасность испытания в реальных условиях может быть отрицательным). Теоретически все испытания должны проводиться при условии, что потенциальные ошибки в процессе испытания не оказали бы влияния на ядерную безопасность, например, во время отключений электричества на станции

или если оборудование, подлежащее проверке, оказалось изолированным от эксплуатирующей станции.

6.3.6 Там, где используется вероятностный анализ безопасности для обоснования безопасности на АС, проектируемые вероятностные значения надежности аппаратных средств (например, полученные из анализа дерева отказов) могут быть включены в анализ АС и таким образом способствовать точности расчета общей надежности станции.

6.4 Техническое обслуживание

Проект аппаратных средств должен включать в себя конкретные требования к техобслуживанию, представленные в технических условиях к аппаратным средствам. Кроме того, там, где это возможно, проект должен включать в себя характеристики, способствующие снижению риска появления неполадок при проведении технического обслуживания. Примерами таких характеристик являются:

- компоненты, требуемые для замены в случае отказа, должны быть легкодоступны;
- заменяемые компоненты должны быть четко определены с тем, чтобы персонал по техническому обслуживанию мог легко проверить, используются ли правильные компоненты;
- должно быть соответствующее расстояние между терминалами;
- должно быть обеспечено требуемое число специализированных терминалов, используемых для проведения калибровки/испытаний (для предотвращения разъединения электропроводки станции и облегчения проведения таких операций);
- для сокращения потенциала погрешностей при проведении технического обслуживания проект аппаратных средств должен включать в себя структурную схему размещения оборудования с четкой маркировкой.

6.5 Интерфейсы

Требования к интерфейсам системы для предотвращения отказов через них предоставлены в 6.1.1.2.1 МЭК 61513.

6.6 Модификация

В рамках технических условий к аппаратным средствам аппаратные средства должны быть разработаны так, чтобы они могли быть в дальнейшем изменены (см. раздел 12).

6.7 Отказы в системе электроснабжения

В рамках технических условий на аппаратные средства компьютеризированная система должна быть разработана так, чтобы она была невосприимчивой к последствиям краткосрочных отказов в системе электроснабжения и возможным скачкам электроснабжения (напряжение/частота). Должна быть также представлена информация о свойствах системы и таких колебаниях напряжения для сообщения операторам и персоналу технического обслуживания (это оповещение не относится к аппаратным средствам и, следовательно, не входит в область применения настоящего стандарта).

6.8 Выбор компонентов

Там, где должны использоваться уже существующие компоненты, проект компонентов должен быть совместимым с их предназначением в аппаратных средствах системы.

6.9 Проектная документация

6.9.1 Проектная документация на аппаратные средства системы должна содержать описание аппаратных средств, а также изложение способа, который при их внедрении позволит обеспечить соответствие положениям спецификации требований к аппаратным средствам. Рекомендуется придерживаться стандартных форм документации и использовать автоматизированные средства проектирования.

6.9.2 Структура проектной документации, описывающей аппаратные средства компьютерной системы, должна состоять из нескольких документационных «уровней». Проектная документация на каждом «уровне» должна включать в себя подробный проект компонентов данного уровня, а также требования к аппаратным средствам для компонентов более низких уровней. Документация на изготовление/сборку, фабричное испытание, установку, ввод в эксплуатацию, техническое обслуживание и эксплуатацию аппаратных средств должна разрабатываться по ходу процесса разработки проекта.

6.9.3 В предварительной документации определяют архитектуру аппаратных средств, т. е. структуру и взаимосвязи между частями системы. В предварительной документации указывается общая схема размещения оборудования и блочные схемы подсистем и модулей более низких уровней. Предварительная документация должна включать в себя также требования к аппаратным средствам, необходимые для детального проектирования, например:

- число и типы центральных и других процессоров;

- требования к запоминающим устройствам;
- число и типы интерфейсов;
- число и типы каналов передачи данных и шин.

6.9.4 При завершении проектирования и разработки аппаратных средств должна быть подготовлена окончательная документация, содержащая полное и заключительное описания, охватывающие детальное проектирование вплоть до нижнего уровня, а также возможности, ограничения и другие характеристики аппаратных средств.

6.9.5 Окончательные документы должны включать в себя следующую информацию:

a) обзор проекта;

b) перекрестные ссылки к проектной документации;

c) описание деления системы аппаратных средств на подсистемы;

d) описание каждой подсистемы в отношении основных модулей и компонентов (например, блок-схемы, функциональные схемы на уровне вентилей);

e) описание интерфейсов подсистемы. Интерфейсы должны быть описаны, используя логические, физические, электрические и другие способы выражения;

f) описание интерфейсов компьютерной системы. Следует определить интерфейсы связи с любой системой, установленной внутри или вне АС, в том случае, если предусмотрена или существует прямая связь с этими системами, и указать специальные интерфейсы, а также конкретные требования к аппаратным средствам;

g) физическое размещение. Должно быть представлено описание и схемы физического размещения оборудования;

h) данные, относящиеся к качеству (см. раздел 8), включая указание на любые необходимые действия (например, на замену компонентов), необходимые для поддержания определенного качественного цикла. Там, где необходимо, должны быть также представлены данные, относящиеся к ограничению срока годности запасных частей;

i) требования к проведению технического обслуживания;

j) анализ выполнения требований к надежности и безотказности при создании аппаратных средств.

7 Верификация и валидация

7.1 Общие положения

7.1.1 Процесс проектирования и разработки должен включать в себя официальный контроль соответствия оборудования на каждом этапе проектирования и разработки требованиям, предъявленным на предыдущем этапе.

7.1.2 Верификацию аппаратных средств следует начинать с верификации требований к проекту оборудования с оценкой их соответствия требованиям к эффективности системы и завершать, когда программные средства интегрируются с аппаратными средствами. Соответствующие требования к верификации результатов интеграции аппаратных/ программных средств систем классов 1 и 2 представлены в МЭК 60880 и МЭК 62138.

7.2 План верификации

7.2.1 Для документирования методов верификации проекта аппаратных средств и контроля процесса верификации должен быть подготовлен план верификации. План верификации должен быть подготовлен до начала проведения верификации.

В плане должна быть отражена информация о персонале/организации, структуре процесса верификации, используемых методах, уровне верификации, который должен быть достигнут, графике, а также о других важных мероприятиях проекта, связанных с верификацией:

a) С целью наиболее раннего выявления и исправления ошибок верификацию проводят параллельно с процессом проектирования (создавая адекватные условия для конфигурационного контроля).

b) Мероприятия по проведению официальной верификации не должны проводиться до того, пока проект или его часть, подлежащие верификации, не будут сданы разработчиками. Сданные для верификации проект и сопутствующая документация должны быть подвергнуты официальному конфигурационному контролю.

c) После проведения верификации все изменения в проекте должны быть проверены в соответствии с разделом 7.7.

7.3 Независимость верификации

7.3.1 Для систем класса 1 отдельные лица или группы лиц, проводящие верификацию проекта, должны быть независимыми экспертами по отношению к разработчикам проекта; например, они могут быть из разных отделов одной организации или из разных организаций. Для систем класса 2 лица, проводящие верификацию, не должны проектировать изделия, подлежащие верификации. Однако персонал, ответственный за верификацию, может быть из той же организации, что и разработчики проекта. В дополнение к этим требованиям:

a) проверяющий персонал должен иметь соответствующую техническую квалификацию;

b) любые результаты верификации и ответы разработчиков проекта на эти результаты должны быть официально задокументированы;

c) верификация должна проводиться в соответствии с задокументированными процедурами.

7.3.2 При проектировании аппаратных средств класса 2, когда для проверки аппаратных средств используется автоматизированное испытательное оборудование, независимые детальные требования, указанные выше, применяются к персоналу, разрабатывающему автоматизированное испытательное оборудование, а не к персоналу, контролирующему проводимые на этом испытательном оборудовании испытания. Однако при разработке аппаратных средств класса 1 персонал не отвечает за проведение испытаний аппаратных средств, которые он проектировал (проводимых как с использованием, так и без использования автоматизированного испытательного оборудования).

7.4 Методы

Для верификации проекта допускается использовать критические обзоры, ревизии, анализы, тесты или испытания, проводимые на автоматизированном испытательном оборудовании, а также сочетание этих методов. Проверяющий персонал должен определить, какие методы верификации следует использовать. Обоснование методов верификации должно подробно документироваться, для того чтобы обеспечить контроль со стороны лиц, непосредственно не занятых проектированием или верификацией проекта.

a) При выборе соответствующего метода верификации следует учитывать:

- классификацию системы по безопасности (т. е. классы 1 или 2, для класса 1 требуются более строгие методы);

- анализы и испытания, проводимые в рамках процесса проектирования интегрированных аппаратных средств и программного обеспечения с прилагаемой документацией, пригодной для поддержки верификации и валидации, т. е. следует убрать такие действия в процессе верификации и валидации аппаратных средств, неэффективно использующих ресурсы, дублируя работу;

- предшествующие мероприятия по верификации, приведенные на аппаратных средствах или системах, содержащих аппаратные средства (т. е. такие, где было установлено, что оборудование соответствует требованиям);

- проектные характеристики, например, размеры, завершенность/новизна используемых принципов, типы отказов и сложность системы;

- сопутствующие данные, которые можно получить при выполнении других мероприятий, таких как мероприятия по обеспечению качества или оценке условий окружающей среды.

b) Соответствующие средства и методы должны быть предусмотрены для испытания подсистем и электронных компонентов для обеспечения их тщательного тестирования. Следует использовать автоматические средства для улучшения сходимости показаний и тщательности испытания там, где необходимо.

c) Контрольные приборы или тестовые инструментальные средства, используемые во время верификации или испытаний, должны быть соответствующим образом откалиброваны и поверены для обеспечения точности вычислений, тогда как процедуры должны гарантировать использование только калиброванных инструментов.

d) Испытательные инструменты, применяемые для программного обеспечения, должны быть утверждены до их использования и включены в конфигурационный контроль.

e) Результаты всего официального тестирования должны быть зарегистрированы (неофициальное тестирование может быть проведено во время процесса проектирования как предшественника официального тестирования). Проверяемые отчеты официального тестирования должны быть доступны для подтверждения того, что все испытания были проведены и любые испытательные аномалии были выявлены.

7.5 Документация

Все мероприятия по верификации должны быть официально и достаточно подробно документированы для обеспечения контроля со стороны лиц, непосредственно не занятых разработкой и верифика-

цией. Эти документы включают в себя план проведения программы верификации, требования, процедуры испытаний, результаты испытаний, результаты анализа изменений проекта и отклонения, обнаруженные при верификации аппаратных средств.

a) Тестовые процедуры должны быть подробно записаны, в них должны быть предусмотрены пошаговые инструкции для верификации аппаратных средств, и они должны содержать детальную информацию об испытательных устройствах.

b) Процедуры испытаний должны содержать однозначный критерий «удовлетворительно/неудовлетворительно».

c) Процедуры испытаний, реализованные при помощи программного обеспечения, должны быть задокументированы и включены в документацию, относящуюся к испытаниям.

7.6 Отклонения от нормы (несоответствия)

Отклонения от нормы (несоответствия), выявленные во время верификации, должны быть официально задокументированы и переданы персоналу, отвечающему за проектирование, для принятия решения. Ответ разработчиков проекта должен быть официально задокументирован для обеспечения контроля, гарантирующего то, что по поводу всех отклонений ответ получен, и все несоответствия скорректированы или приняты. Когда несоответствия проекту приняты, все последствия от этих несоответствий для документации системы должны быть полностью утверждены.

7.7 Изменения и модификации

7.7.1 Все изменения в проекте должны быть оценены для определения последствий для проекта, чтобы определить, какая документация требует исправлений и какие процессы проектирования и верификации следует повторить.

7.7.2 Модифицированные части проекта должны быть идентифицированы в соответствии с установленными процедурами контроля качества.

7.8 Верификация монтажа (установки оборудования)

Верификация монтажа системы должна быть проведена в соответствии с разделом 10.

7.9 Валидация

Системную валидацию аппаратных средств и программного обеспечения системы проводят в соответствии с МЭК 61513, МЭК 60880 или МЭК 62138.

7.10 Верификация уже существующих платформ оборудования

При использовании уже существующей платформы должна быть проверена ее пригодность для намеченного использования. Процесс оценки должен учитывать следующие аспекты проекта:

a) процесс проектирования, использованный при разработке аппаратных средств, т. е. оценка в соответствии с требованиями, указанными в разделе 6;

b) опыт эксплуатации (когда фактические данные по надежности аппаратных средств подтверждают, что цели надежности аппаратных средств достижимы, то в этом случае появляется уверенность в качестве функционирования аппаратных средств при предложенном применении). Соответствующие данные по опыту эксплуатации, которые подтверждают необходимую цель надежности аппаратных средств, могут использоваться для корректировки несоответствий в используемых методах разработки, указанных в перечислении a);

c) если в перечислении a) не представлена достоверная информация для подтверждения соответствия своему назначению аппаратных средств, то может быть проведена дополнительная работа для подтверждения оценки, например, тестирование, анализ, обоснование.

8 Квалификация

В МЭК 60780 представлены требования к квалификации аппаратных средств, которые должны применяться в ядерной отрасли. Информационная схема структуры квалификации представлена в приложении В.

9 Изготовление

Если подсистемы, модули и компоненты, используемые в компьютеризированной системе, содержат готовые изделия и специализированные аппаратные средства, они должны разрабатываться/оцениваться в соответствии с требованиями, установленными в настоящем стандарте.

10 Установка и ввод в эксплуатацию

10.1 Упаковывание, хранение, транспортирование и распаковывание должны осуществляться так, чтобы не повредить систему.

10.2 Перед извлечением системы из упаковки и ее установкой внешние условия, в которых система будет устанавливаться, следует проверить на соответствие требованиям к внешним условиям размещения аппаратных средств по 5.4.

10.3 Должны быть подготовлены конкретные процедуры и получены необходимые сведения для обеспечения установки, прокладки кабелей и подсоединения системы в соответствии с требованиями проекта и, в частности, с требованиями к заземлению. Упомянутые сведения должны включать в себя описание частей оборудования. Для подготовки этих сведений используется план обеспечения качества. Установку, испытания и ввод в эксплуатацию выполняют в соответствии с конкретными процедурами.

10.4 Нормальная работа системы на месте установки должна быть подтверждена запланированными специальными испытаниями по МЭК 61513.

10.5 Испытания должны проводиться по соответствующим стандартам, например МЭК 61000.

10.6 Уровень жесткости испытаний на электромагнитные помехи выбирают так, чтобы он соответствовал наихудшим условиям, которым может подвергаться система.

10.7 Испытания на электромагнитную совместимость систем классов 1 и 2 проводят за пределами места эксплуатации. Этот тип испытаний систем класса 2 направлен на подтверждение правильности ее функционирования. Для систем класса 1 проводят испытания на месте эксплуатации, если это возможно и эффективно.

10.8 После установки и ввода в эксплуатацию необходимо провести процедуру приемки системы перед ее передачей пользователю.

11 Техническое обслуживание

Техническое обслуживание аппаратных средств включает в себя:

- испытания, проверки и калибровку [которые проводят периодически в пределах максимальных установленных интервалов или после замены, капитального ремонта, ревизии и ремонта компонентов (повторная валидация)];
- техническое сопровождение, необходимое для поддержания аппаратной части компьютера в рабочем состоянии, замену расходных материалов, профилактическую замену изделий, а также тщательный осмотр блоков, частей и компонентов;
- ремонт, восстановление работоспособности поврежденного оборудования, блоков и частей.

11.1 Мероприятия по техобслуживанию (требования к техобслуживанию)

11.1.1 Следует разработать и применять официальную процедуру контроля, относящуюся к выполнению операций по техобслуживанию и к его документированию (см. приложение В).

Процедура контроля должна включать в себя:

- необходимые меры для сокращения потенциальных отказов и предотвращения несчастных случаев;
- организационные мероприятия и подготовку к выполнению операций по техобслуживанию в случае, если они влияют на работу АС или на функции, обеспечивающие безопасность.

11.1.2 Работа по техническому обслуживанию должна проводиться только квалифицированным и уполномоченным персоналом. Работа по техническому обслуживанию должна регистрироваться в соответствии с определенной процедурой контроля. Для каждого задания предусматривается персональное подтверждение ответственным лицом или автоматизированным способом удовлетворительного выполнения задания.

Вся соответствующая информация, например, информация, содержащая сведения о часе, дне, замененных деталях и т. д., также должна регистрироваться.

11.1.3 Отчеты о работе по техобслуживанию подлежат проверке (ревизии).

11.1.4 Для некоторых особо важных компонентов вместо замены при появлении отказа может быть принят профилактический режим технического обслуживания. В этом случае должны применяться устройства управления для того, чтобы гарантировать замену компонентов после промежутка времени, не превышающего срока аттестации (если настоящий стандарт распространяется на вид рассматриваемого компонента, тогда см. МЭК 60780).

11.1.5 Условия хранения запасных частей в эксплуатирующей организации должны соответствовать требованиям к условиям хранения конкретных запасных частей. Сроки хранения запасных частей контролируются и изменяются по мере необходимости с течением времени в соответствии со свойствами старения аппаратных средств. Должны применяться любые действия, необходимые для сохранения состояния готовности запчастей, например, периодическое подключение к источнику напряжения.

11.1.6 Запасные части должны быть аттестованы в соответствии со стандартом, применяемым для аттестации используемых компонентов. Любое сокращение требований к аттестации компонента системы класса 1 или 2 или продление сроков аттестации такого компонента должно рассматриваться и соответственно оцениваться как модификация системы; см. раздел 12 (МЭК 61513 определяет устройства управления, применимые к модификации системы).

11.1.7 Все запчасти оборудования должны подвергаться конфигурационному контролю и должны иметь соответствующие опознавательные знаки или маркировку.

11.1.8 Рекомендуется предоставлять гарантии на поставку запчастей оборудования (например, или через холдинг запчастей с получением гарантий от поставщиков или путем обеспечения возможности их производства).

11.2 Информация об отказах

11.2.1 Сбор данных об отказах во время работы оборудования является основным источником информации, которую можно использовать в целях его совершенствования:

- знаний о надежности компонентов (с учетом реальных рабочих условий окружающей среды);
- оценок надежности оборудования (по определению фактической частоты отказов при эксплуатации и по наблюдению за работоспособностью в рабочих условиях);
- методики технического обслуживания (благодаря оптимизации использования запасных деталей, улучшению программ профилактического технического обслуживания, а также требований к персоналу, проводящему техническое обслуживание).

11.2.2 Данные об отказах при эксплуатации по отчетам о техобслуживании следует передавать в банк данных об отказах.

Отчеты о техобслуживании должны включать в себя (если необходимо и если они известны):

- идентификационные данные о системе с неисправным компонентом;
- обстоятельства отказов и их последствия;
- описание неисправных компонентов;
- данные о местонахождении компонентов в системе;
- описание неполадки, вызвавшей отказ;
- дату обслуживания;
- возраст поврежденных компонентов;
- данные о лице (ах), предоставившем(их) отчет;
- данные о лице (ах), обнаружившем(их) неполадку.

11.2.3 Данные об отказах систем, важных для безопасности, должны подлежать периодическому анализу, гарантирующему, что частота отказов компонента останется в пределах допустимой нормы. Любые статистически существенные отрицательные тенденции в данных должны экстраполироваться с тем, чтобы по возможности гарантировать, что оборудование будет удовлетворительно работать до следующей оценки данных по отказам оборудования или до замены оборудования (кротчайший возможный период).

11.3 Документация по техническому обслуживанию

11.3.1 Указания по техническому обслуживанию должны быть представлены в письменном виде в форме инструкций, руководств и т. д.

11.3.2 Документация по техобслуживанию должна описывать порядок обслуживания применительно к используемому оборудованию, определяя компоненты, требующие регулярного контроля, перекалибровки или замены.

11.3.3 Документы по техническому обслуживанию должны включать в себя описание способов обнаружения отказов и их диагностики для каждого конкретного модуля системы.

11.3.4 В документации по техническому обслуживанию должен быть изложен следующий порядок проведения ремонта:

- методы ремонта или замены различных подсистем, модулей и компонентов;
- ограничения, которые нужно иметь в виду во время ремонта системы, (например, обязательное выключение системы или части системы);
- степень, до которой система должна перепроверяться после ремонта.

Кроме операций планового периодического технического обслуживания следует предусмотреть мероприятия (там, где это необходимо), которые могут использоваться при рассмотрении аномального поведения системы и определять неисправные компоненты.

12 Модификации

Для устранения неисправности, удовлетворения новых или пересмотренных функциональных требований может потребоваться модификация аппаратных средств.

12.1 Процесс, контролирующий изменения в проекте аппаратных средств, должен соответствовать требованиям 6.3.6 МЭК 61513.

12.2 Изменения в проекте аппаратных средств, имеющие последствия не только на одном этапе проекта (т. е. за исключением любых изменений, внесенных проектировщиками в процессе создания проекта), должны вноситься в соответствии с задокументированной процедурой внесения изменений в проект. Эта процедура должна учитывать любые потенциальные последствия для других аспектов проекта системы, например, для аппаратных средств и программного обеспечения.

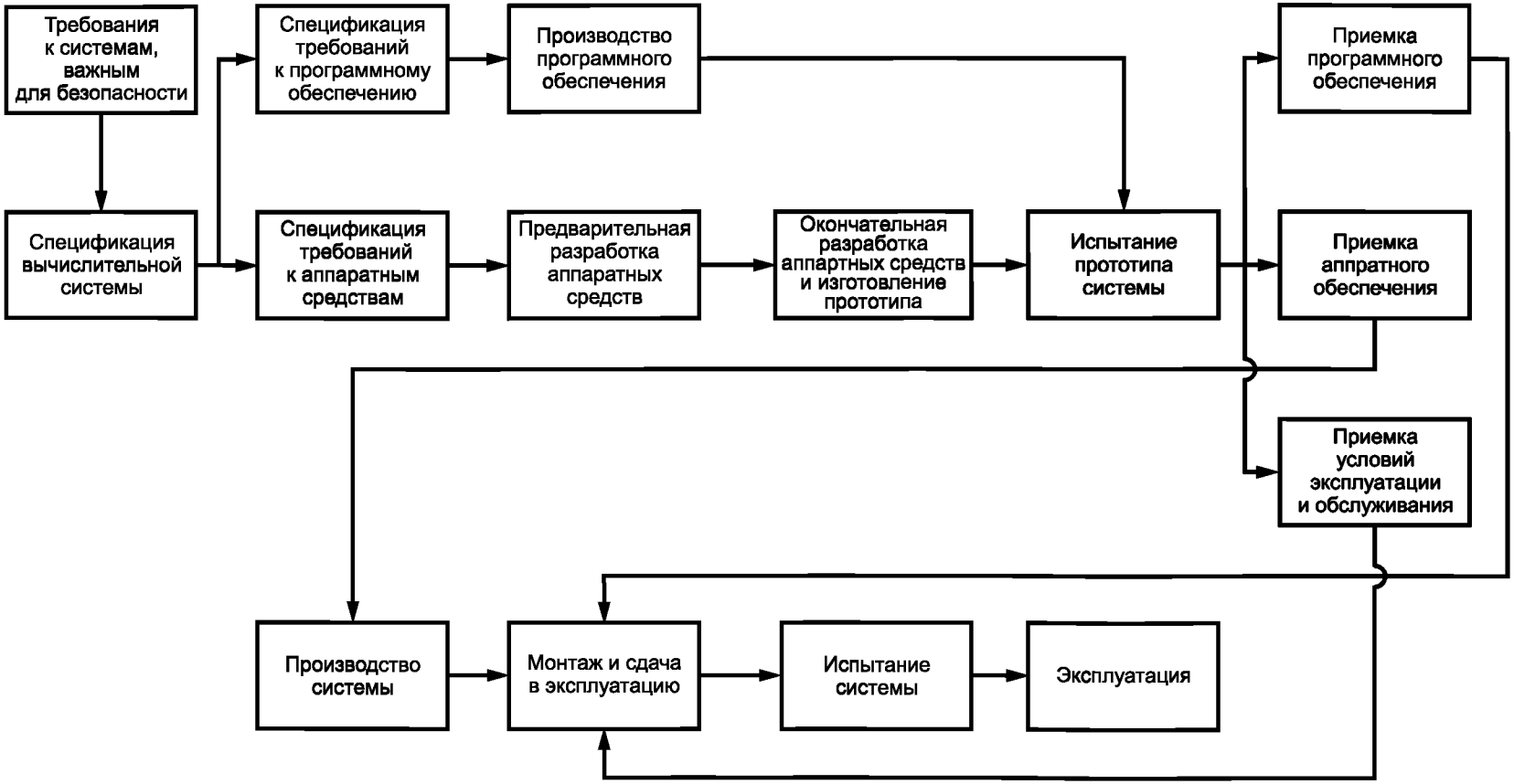
12.3 Процедура внесения изменений в проект должна гарантировать определение воздействия всех изменений на аппаратные средства и процессы верификации, валидации и аттестации, а также выполнение всех требуемых доработок.

13 Эксплуатация

Требования к работе системы изложены в МЭК 61513 (МЭК 60880 и МЭК 62138 содержат дополнительную информацию).

Приложение А
(справочное)

Жизненный цикл системы



Примечание — Для простоты обратные связи не показаны.

Рисунок А.1 — Жизненный цикл системы

Приложение В
(справочное)

Структура квалификации

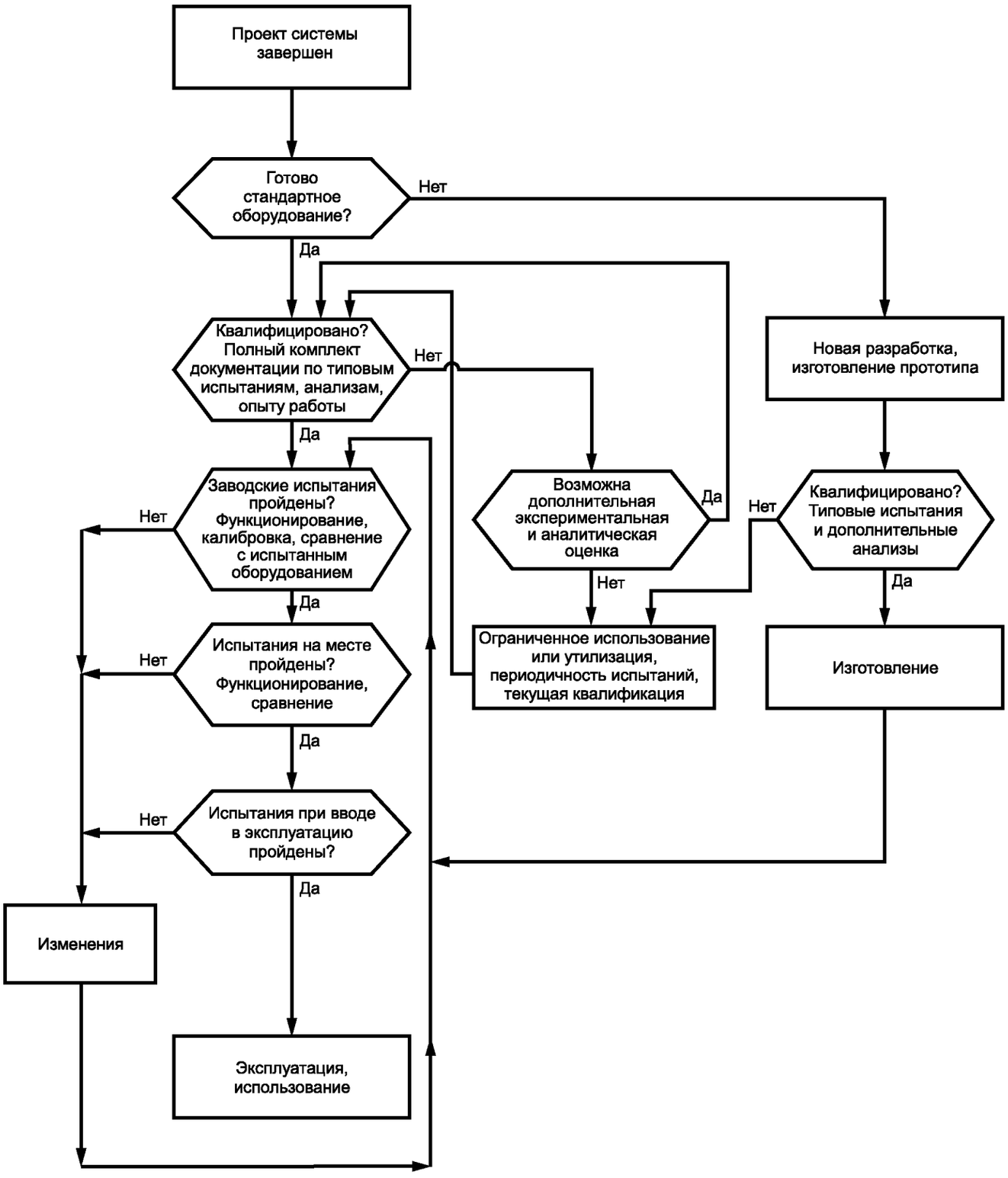


Рисунок В.1 — Структура квалификации

Приложение С
(справочное)

Пример процедур технического обслуживания

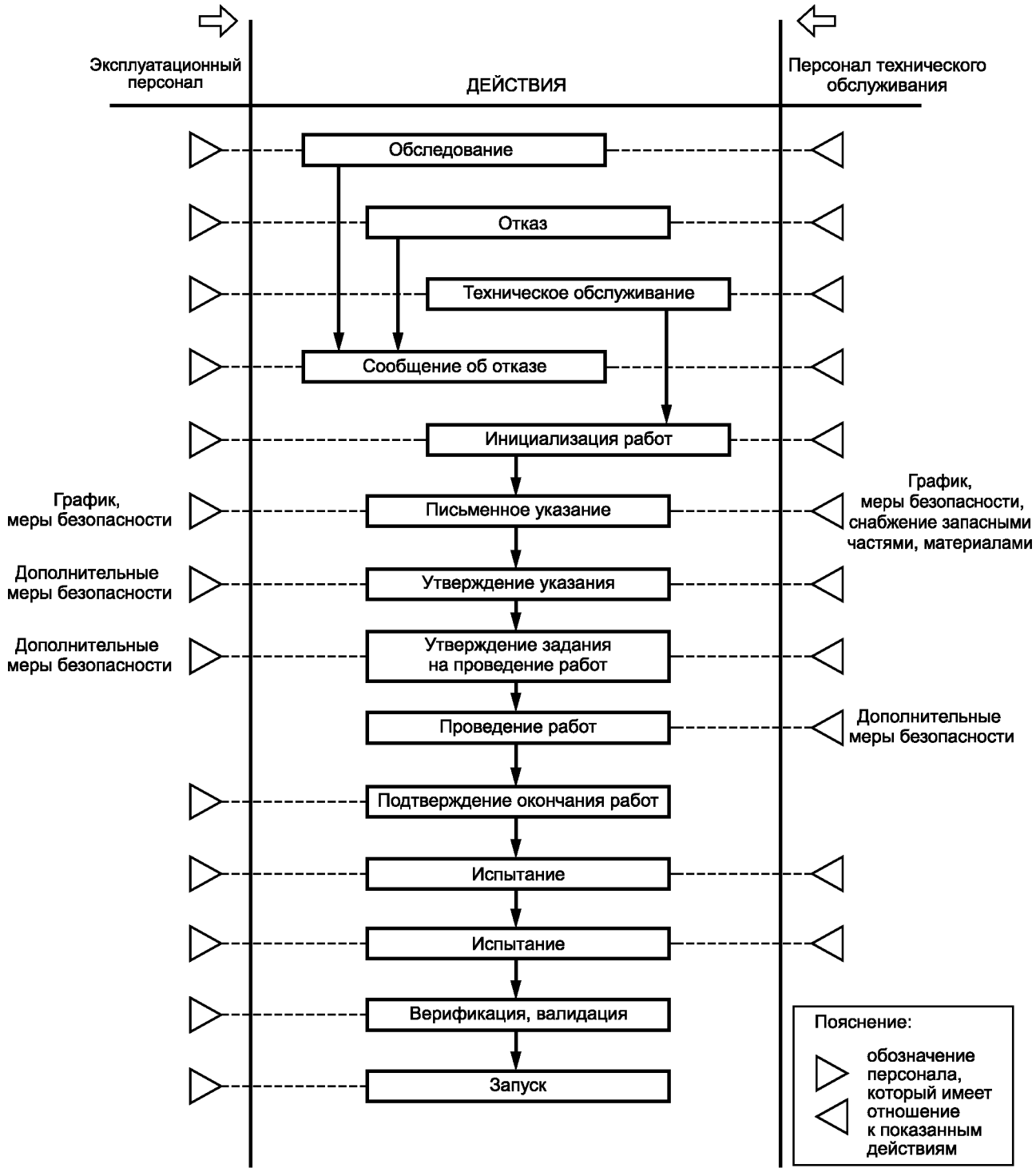


Рисунок С.1 — Пример процедуры технического обслуживания

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60780	—	*
МЭК 60812	—	*
МЭК 60880:2006	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютеризированных систем, выполняющих функции категории А»
МЭК 61000 (все части)	—	*
МЭК 61025	—	*
МЭК 61513:2001	IDT	ГОСТ Р МЭК 61513—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
МЭК 62138	IDT	ГОСТ Р МЭК 62138—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютеризированных систем, выполняющих функции категории В и С»
ИСО 9001	—	*
Руководство МАГАТЭ NS-G 1.3	—	**
Руководство МАГАТЭ 50-C/SG-Q:1996	—	**

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

** Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод текста документа на русский язык, который доступен на http://www.iaea.org/.

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Библиография

[1] IEC 61226 Nuclear power plants — Instrumentation and control systems important to safety — Classification of instrumentation and control functions
[2] ISO 12207 Information technology — Software life cycle process
[3] IAEA Safety Glossary:2006
[4] IAEA NS-R-1:2000 Safety of nuclear power plants: Design

УДК 621.3.049.75:006.354 ОКС 27.120.20

Ключевые слова: атомные станции; системы контроля и управления, важные для безопасности; аппаратное обеспечение; компьютеризированные системы

Редактор *В.Н. Копысов*
Технический редактор *Н.С. Гришанова*
Корректор *И.А. Королева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 09.06.2012. Подписано в печать 26.06.2012. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,85. Тираж 86 экз. Зак. 587.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.