ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 62646— 2019

Атомные станции

ПУНКТЫ УПРАВЛЕНИЯ

Компьютерно-ориентированные процедуры

(IEC 62646:2016, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Государственной корпорацией по атомной энергии «Росатом» на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

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 16 мая 2019 г. № 197-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 62646:2016 «Атомные станции. Пункты управления. Компьютерно-ориентированные процедуры» (IEC 62646:2016 «Nuclear power plants — Control rooms — Computer-based procedures», IDT).

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

5 Положения настоящего стандарта действуют в целом в отношении сооружаемых по российским проектам атомных станций за пределами Российской Федерации, а также в отношении сооружаемых на территории Российской Федерации атомных станций в части, не противоречащей требованиям Федеральных норм и правил в области использования атомной энергии

6 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
1.1 Объект настоящего стандарта 1
1.2 Причины разработки и применения КОП 1
1.3 Обзор КОП 1
1.4 Использование настоящего стандарта совместно со связанными стандартами 2
1.5 Организация стандарта 2
2 Нормативные ссылки 3
3 Термины и определения 4
4 Обозначения и сокращения 5
5 Политика КОП и концептуальные требования 5
5.1 Общие требования 5
5.2 Политика компьютеризации 6
5.3 Семейства КОП 8
5.4 Обзор особенностей компьютеризации 9
5.5 Выходная документация 11
5.6 Запроектные условия 11
6 Применение КОП 11
6.1 Общие положения 11
6.2 Применение КОП в производственных условиях 11
6.3 Формы поддержки деятельности оператора с помощью КОП 13
6.4 Поддержка координации оператора 13
6.5 Выходная документация 14
7 Компьютерно-ориентированные процедуры и функциональные требования 14
7.1 Общие положения 14
7.2 Требования безопасности 14
7.3 Особенности человеко-машинного интерфейса 15
7.4 Интеграция системы КОП в ЦСО 16
7.5 Система КОП, внедренная в ЦСО 16
7.6 Отказы системы КОП 17
7.7 Выходная документация 18
8 Требования к детальному проектированию 18
8.1 Общие положения 18
8.2 Основные характеристики КОП 18
8.3 Выходная информация КОП 19
8.4 Навигация 20
8.5 Рекомендации КОП 21
8.6 Процедурно-ориентированная автоматизация 22
8.7 Другие объекты КОП 24
8.8 Выходная документация 24
9 Жизненный цикл КОП 24
9.1 Общие положения 24
9.2 Организация проектирования 24
9.3 Проектная группа 25

9.4 Детальное проектирование КОП и обеспечение качества выполнения 25
9.5 Программа верификации и валидации 25
9.6 Верификация и валидация КОП 26
9.7 Внедрение КОП на АС 28
9.8 Выходная документация 28
9.9 Обучение оперативного персонала 29
9.10 Техническое обслуживание КОП и систем КОП 29
9.11 Обратная связь 29
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 30
Библиография 31

Введение

a) Технические положения, основные вопросы и организация стандарта

В данном стандарте МЭК основное внимание уделяется компьютеризации процедур, используемых оперативным персоналом. Эти процедуры всегда в значительной степени способствовали высокой безопасности и работоспособности атомных станций (АС), а применение в настоящее время компьютерных технологий для обеспечения совершенства рекомендаций операторам АС растет и становится актуальной практикой. Настоящий стандарт также дает указания относительно решения о том, в какой степени эти процедуры следует компьютеризировать.

Предполагается, что стандарт будет использоваться проектировщиками АС, обслуживающим персоналом, системными экспертами и инспекторами надзорных органов.

В июне 2013 года на совещании ПК 45А МЭК, состоявшемся в Москве, было принято решение пересмотреть МЭК 62646 в связи с уроками, извлеченными из аварии на «Tokyo Electric Power Company (TEPCO) Fukushima Daiichi», и последними комментариями от национального комитета Канады. Настоящий стандарт содержит изменения по результатам этого пересмотра.

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

МЭК 62646 — это документ третьего уровня в структуре серии стандартов ПК 45А МЭК, посвященный общим решениям проблем, связанных с компьютеризированными процедурами.

МЭК 62646 следует рассматривать вместе с МЭК 60964 и МЭК 61839. МЭК 60964, поддерживаемый МЭК 61227, МЭК 61771 и МЭК 61772, является документом ПК 45А МЭК, содержащим указания по применению органов управления оператора, верификации и валидации проекта, применению устройств визуального отображения в пункте управления, в то время как МЭК 61839 устанавливает требования к функциональному анализу и назначению при подготовке рекомендаций по распределению функций между операторами и системами.

Более подробная информация о структуре серии стандартов ПК 45А МЭК приведена в пункте d) введения.

c) Рекомендации и ограничения в отношении применения настоящего стандарта

Важно отметить, что настоящий стандарт не устанавливает дополнительных функциональных требований для систем безопасности.

Настоящий стандарт касается технических требований и эргономического проектирования, связанных с компьютерно-ориентированными процедурами (КОП). Однако, он не дает подробных рекомендаций по эргономическому проектированию центров управления, поскольку эти рекомендации рассматриваются в стандартах серии ИСО 11064, а также подробных рекомендаций о распределении задач между человеком и системой, рассмотренных в ИСО 61839, и подробных рекомендаций по кибербезопасности, приведенных в ИСО 62645. Настоящий стандарт также не включает требования к организации обслуживания процедур.

Аспекты, для которых в настоящем стандарте предусмотрены требования и рекомендации:

- вначале рассматриваются создание политики компьютеризации процедур (особенно тех типов процедур, которые следует компьютеризировать) и степень их компьютеризации. Затем определяются различные семейства КОП, нацеленные на связанные функции. Наконец, рассматриваются аспекты безопасности КОП;
- использование КОП внутри и вне блочного пункта управления (БПУ) с учетом возможной связи КОП с бумажно-ориентированными процедурами, а также содействие КОП оперативной деятельности, включая координацию работы пользователей;
- проектные требования к безопасности и небезопасности для цифровой системы обработки КОП, и соображения о том, какие действия должны быть предприняты в случае отказа этой системы;
- подробные требования и рекомендации, обусловленные функциональными особенностями КОП (начиная с основных и заканчивая самыми сложными), затрагивающие управление АС, информацию, навигацию и руководство;
- жизненный цикл КОП, от настройки до эксплуатации КОП, включающий подготовку операторов при проектировании и внедрении.

Чтобы гарантировать, что данный стандарт будет и впредь оставаться актуальным, основное внимание в нем уделяется принципиальным вопросам, а не конкретным технологиям.

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

МЭК 61513 и МЭК 63046 являются документами верхнего уровня серии стандартов ПК 45А МЭК. МЭК 61513 содержит общие требования по безопасности к системам контроля и управления (СКУ) и к оборудованию, используемым при выполнении функций, важных для безопасности АС. МЭК 63046 содержит общие требования к энергосистемам АС, он охватывает системы электроснабжения, включая системы питания СКУ. МЭК 61513 и МЭК 63046 должны рассматриваться совместно и на одном уровне. МЭК 61513 и МЭК 63046 включены в состав серии стандартов ПК 45А МЭК и образуют полную структуру, устанавливающую общие требования к приборам, системам управления и электрическим системам АС.

МЭК 61513 и МЭК 63046 относятся непосредственно к другим стандартам ПК 45А МЭК по общим темам, связанным с категоризацией функций и классификацией систем, аттестацией, разделением систем, защитой от сбоев по общей причине, проектированием пунктов управления, электромагнитной совместимостью, кибербезопасностью, программными и аппаратными аспектами для цифровых программируемых систем, согласованием требований безопасности и защищенности, а также с управлением процессом старения. Стандарты, указанные непосредственно на этом втором уровне, следует рассматривать вместе с МЭК 61513 и МЭК 63046 как согласованный набор документов.

На третьем уровне в серии стандартов ПК 45А МЭК представлены стандарты, не имеющие прямого отношения к МЭК 61513 или МЭК 63046 и являющиеся стандартами, относящимися к конкретному оборудованию, техническим методам или конкретным видам деятельности. Обычно эти документы, ссылающиеся по общим темам на документы второго уровня, могут использоваться самостоятельно.

Четвертый уровень, расширяющий серию стандартов ПК 45А МЭК, соответствует техническим отчетам, которые не являются нормативными документами.

Серия стандартов ПК 45А МЭК последовательно реализует и детализирует принципы безопасности и защищенности и основные аспекты, предусмотренные в соответствующих стандартах безопасности МАГАТЭ и в соответствующих документах серии стандартов по ядерной безопасности МАГАТЭ. В частности, эти принципы и аспекты изложены в документах: «Требование МАГАТЭ SSR-2/1» (требования безопасности, связанные с проектированием АС), «Руководство по безопасности МАГАТЭ SSG 30» (классификация безопасности конструкций, систем и компонентов на АС), «Руководство по безопасности МАГАТЭ SSG 39» (проектирование систем контроля и управления для АС), «Руководство по безопасности МАГАТЭ SSG-34» (проектирование систем электроснабжения АС) и «Руководство по внедрению NSS17» (вопросы обеспечения компьютерной защищенности на ядерных объектах). Терминология и определения безопасности и защищенности, используемые в стандартах ПК 45А, соответствуют тем, которые используются МАГАТЭ.

В МЭК 61513 и МЭК 63046 принят формат представления из базовой публикации по безопасности МЭК 61508 в части общей структуры жизненного цикла и структуры жизненного цикла системы. Что касается ядерной безопасности, МЭК 61513 и МЭК 63046 обеспечивают интерпретацию общих требований МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 для сектора ядерных приложений. В этой структуре МЭК 60880, МЭК 62138 и МЭК 62566 соответствуют МЭК 61508-3 для сектора ядерных приложений. МЭК 61513 и МЭК 63046 относятся к стандартам международной организации по стандартизации (ИСО [ISO — International Organization for Standardization]), а также к стандартам МАГАТЭ GS-R-3, GS-G-3.1 и GS G 3.5 по темам, связанным с обеспечением качества (ОК). На втором уровне, касающемся ядерной безопасности, МЭК 62645 является исходным документом для стандартов по безопасности ПК 45А МЭК. МЭК 62645 основывается на действующих принципах высокого уровня и основных концепциях общих стандартов безопасности, в частности ИСО/МЭК 27001 и ИСО/МЭК 27002, адаптирует и дополняет их в соответствии с ядерным контекстом, а также связывает их с серией стандартов МЭК 62443. На втором уровне, касающемся пунктов управления, МЭК 60964 является исходным документом для стандартов ПК 45А МЭК, а МЭК 62342 является исходным документом для стандартов ПК 45А МЭК по управлению старением.

Примечания

1 Предполагается, что при проектировании для АС СКУ, реализующих обычные функции безопасности (например, для обеспечения безопасности работников, защиты имущества, защиты от химических опасностей и опасностей, связанных с технологической энергией), будут применяться международные или национальные стандарты.

2 Домен ПК 45А МЭК был расширен в 2013 году для покрытия электрических систем. В 2014 г. и 2015 г. в ПК 45А МЭК были проведены обсуждения, с целью решения, как и где должны быть рассмотрены общие требования к проектированию электрических систем. Эксперты ПК 45А МЭК рекомендовали разработать независимый стандарт на том же уровне, что и МЭК 61513 для установления общих требований к электрическим системам. Для решения этой задачи теперь начата подготовка МЭК 63046. После публикации МЭК 63046 примечание 2 о введении стандартов ПК 45А МЭК будет исключено.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Атомные станции

ПУНКТЫ УПРАВЛЕНИЯ

Компьютерно-ориентированные процедуры

Nuclear power plants. Control rooms. Computer-based procedures

Дата введения —2019—08—01

1 Область применения

1.1 Объект настоящего стандарта

Настоящий стандарт устанавливает требования для всего жизненного цикла эксплуатационных процедур, которые проектировщик желает компьютеризировать. В нем также содержатся рекомендации для принятия решений о том, какие типы процедур следует компьютеризировать и в какой степени. После компьютеризации процедуры обозначаются как «компьютерно-ориентированные процедуры» (КОП).

1.2 Причины разработки и применения КОП

Усиление безопасности, облегчение работы операторов и улучшение эксплуатационных характеристик АС всегда были важными целями, достижение которых во время эксплуатации АС в значительной степени зависит от действий обслуживающего персонала и от эксплуатационных процедур. Применение цифровых технологий не только способствует реализации эффективных способов автоматизации ключевых функций, но также улучшает оборудование, управление и человеко-машинный интерфейс АС.

Кроме того, использование компьютерной технологии, обеспечивающей форматы эксплуатационных процедур для операторов АС в диалоговом режиме и в режиме реального времени, растет и становится актуальной практикой. Эти технологии могут применяться как при нормальной эксплуатации, так и в качестве консультационных форматов, используемых в условиях нарушений нормальной эксплуатации. Такие эксплуатационные процедуры, при надлежащем их внедрении и поддержании их в актуальном состоянии, могут обеспечить расширенную поддержку, обеспечивающую повышение безопасности и эффективности действий оператора по сравнению с бумажно-ориентированными процедурами. Подготовка указанных эксплуатационных процедур требует большой осторожности и тесного взаимодействия с операторами и проектировщиками АС, а также тесного сотрудничества с проектировщиками средств измерения и управления.

КОП имеют много общего с бумажно-ориентированными процедурами. Требования настоящего стандарт концентрируются только на том, что характерно для КОП.

1.3 Обзор КОП

Процедуры предоставляют операторам два типа элементов верхнего уровня:

- информация, то есть пояснения или данные, отображаемые для того, чтобы позволить оператору контролировать процесс, оценивать ситуацию на АС, понимать рабочий план действий и принимать соответствующие решения;

Издание официальное

- рекомендации, то есть набор упорядоченных шагов, которые подсказывают оператору порядок действий и помогают ему контролировать процессы, системы, оборудование АС и управлять ими.

Информация и рекомендации комбинируются для минимизации ошибок оператора и оптимизации эффективности работы АС.

Информация и рекомендации могут иметь разный уровень детализации в зависимости от правил процедуры, призванной учитывать опыт оператора и существующие принципы управления.

Компьютеризация процедур согласно с принятой методикой проектирования может обеспечивать:

- расширение информации о процессах и оборудовании АС;
- расширение рекомендаций оператору;
- дополнительные функции для запуска и управления автоматизированным циклом.

Настоящий стандарт содержит рекомендации и обзор правил, философии и концептуальных требований по внедрению КОП, включая цели проектирования, допущения, подходы, исходные данные, объем, типы семейств КОП, ключевые особенности КОП и выходную документацию.

1.4 Использование настоящего стандарта совместно со связанными стандартами

Настоящий стандарт предназначен для рассмотрения аспектов, которые:

- являются специфичными для КОП, то есть не являются общими с бумажно-ориентированными процедурами. Например, применение функциональных сценариев для проверки процедур не является специфическим для КОП;
- еще не рассматривались в действующих стандартах, то есть инженерия человеческих факторов, жизненный цикл систем безопасности, распределение задач между человеком и машинами.

Некоторые важные положения, необходимые для правильного и эффективного проектирования КОП на стадии его концептуального проектирования, рассматриваются в следующих взаимосвязанных стандартах:

a) требования по функциональному анализу и назначению, приведенные в МЭК 61839, определяют процедуры функционального анализа и назначения, дают правила разработки критериев для назначения функций либо операторам, либо системам;

b) руководящие принципы учета человеческого фактора при проектировании приведены в МЭК 61772:2009, разделы 4 и 5 данного стандарта содержат рекомендации по учету человеческого фактора при физической реализации устройств визуального отображения (УВО) (см. 4.1), при подготовке форматов отображения (см. 4.4) и при реализации блочного пункта управления (см. раздел 5). Стандарты серии ИСО 11064 обеспечивают руководство по проектам, ориентированным на человека, на протяжении всего жизненного цикла компьютерно-ориентированной интерактивной системы.

Кроме того, МЭК 60964 и МЭК 60965, которые обеспечивают требования и рекомендации для блочных пунктов управления и резервных пунктов управления, а также МЭК 61772, содержащий требования и рекомендации по внедрению УВО в пунктах управления, применяют при внедрении КОП на новых АС. Дополнительные рекомендации по внедрению КОП в случае модернизации блочного пункта управления приведены в 6.2.3.

Настоящий стандарт предполагает одновременное рассмотрение требований к:

1) компьютерной защищенности, которая необходима для защищенности всего жизненного цикла КОП, но не ограничивается компьютеризацией процедур. Вместе с тем эту тему следует учитывать при компьютеризации рабочих средств (требования по кибербезопасности приведены в МЭК 62645);

2) внедрению функций программного и аппаратного обеспечения компьютерных систем КОП, которые согласно МЭК 60880, МЭК 61226, МЭК 62138 и МЭК 61513 следует реализовывать в соответствии с классом безопасности этих систем;

3) проектированию сценариев (включая предполагаемые рабочие события, такие как переходные процессы на АС, нарушения режима работы АС или исходные события) валидации КОП;

4) организации функциональной поддержки процедур.

1.5 Организация стандарта

В разделе 2 перечислены стандарты, на которые приведены ссылки в настоящем стандарте.

В разделе 3 приведены определения, относящиеся к настоящему стандарту.

В разделе 4 перечислены аббревиатуры, используемые в настоящем стандарте.

В разделе 5 представлен обзор КОП. В нем приведены рекомендации для разработки политики компьютеризации процедур на основе типа процедуры, которую необходимо реализовать. Описаны три

универсальных разновидности (называемых семействами), для которых приведены общие и конкретные рекомендации. Также представлено руководство, связанное с требованиями безопасности систем КОП.

В разделе 6 приведены требования по использованию КОП в различных ситуациях [включая модернизацию блочного пункта управления (БПУ) и различные условия как внутри, так и вне БПУ] по возможности в сочетании с бумажно-ориентированными процедурами. Затем в разделе 6 рассматривается поддержка и координация деятельности оператора.

Раздел 7 касается цифровой системы, обрабатывающей КОП. Сначала в этом разделе рассмотрены требования, связанные и не связанные с безопасностью, а затем приведены требования по обработке сбоев в работе этой системы.

В разделе 8 основное внимание уделяется подробным требованиям и рекомендациям, обусловленным функциональными особенностями КОП (начиная с основных и заканчивая самыми сложными) и затрагивающим руководство и управление АС, информацию и навигацию. Также приведены различные варианты, которые могут облегчить использование КОП.

В разделе 9 рассматривается жизненный цикл КОП, от разработки проекта до обслуживания КОП при эксплуатации, включая подготовку операторов при проектировании и внедрении.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

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 компьютерно-ориентированных систем, выполняющих функции категории А)

IEC 60964:2009, Nuclear power plants — Control rooms — Design (Атомные электростанции. Пункты управления. Проектирование)

IEC 60965:2016, Nuclear power plants — Control rooms — Supplementary control room for reactor shutdown without access to the main control room (Атомные электростанции. Пункты управления. Резервный пункт управления для остановки реактора без доступа к блочному пункту управления)

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

IEC 61772:2009, Nuclear power plants — Control rooms — Application of visual display units (VDUs) (Атомные электростанции. Пункты управления. Применение устройств визуального отображения (УВО))

IEC 61839, Nuclear power plants — Design of control rooms — Functional analysis and assignment (Атомные электростанции. Проектирование пунктов управления. Функциональный анализ и назначение)

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

IEC 62241:2004, Nuclear power plants — Main control room — Alarm functions and presentation (Атомные электростанции. Блочный пункт управления. Сигнализация и представление)

ISO 11064 (all parts), Ergonomic design of control centres (Эргономическое проектирование центров управления)

ISO 11064-1, Ergonomic design of control centres — Part 1: Principles for the design of control centres (Эргономическое проектирование центров управления. Часть 1. Принципы проектирования центров управления)

ISO 11064-3, Ergonomic design of control centres — Part 3: Control room layout (Эргономическое проектирование центров управления. Часть 3. Компоновка пункта управления)

ISO 11064-4, Ergonomic design of control centres — Part 4: Layout and dimensions of workstations (Эргономическое проектирование центров управления. Часть 4. Компоновка и габариты рабочих станций)

ISO 11064-5, Ergonomic design of control centres — Part 5: Displays and controls (Эргономическое проектирование центров управления. Часть 5. Средства отображения и органы управления)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **резервная система** (back-up system): Альтернативное оборудование для мониторинга и управления АС, предназначенное для использования в случае отказа обычно применяемой системы человеко-машинного интерфейса (ЧМИ).

Примечание — Резервная система может стать недоступной в случае возникновения запроектной аварии.

3.2 **компьютерно-ориентированная процедура** (computer-based procedures): Интерактивное компьютерное приложение, используемое для представления рекомендаций операторам АС по процедурам, которое может дополнительно содержать динамическую информацию процесса, включая доступ к органам управления оператора.

Примечание — В отличие от бумажно-ориентированных процедур, которые являются статическими документами, КОП предполагают опции считывания динамической информации. Эти опции позволяют оператору «перемещаться» с одного шага на другие различными способами, размещать закладки и использовать параллельные представления.

3.3 **система КОП** (CBP system): Цифровая система, реализующая КОП.

Примечание — КОП может быть реализована в системе ЧМИ вместе с другими функциями управления АС или на автономном компьютере КОП.

3.4 **цифровая система отображения** (digital plant display system): Система цифровых компьютерных форматов (форматов отображения), предназначенных для контроля и управления АС, например, блок-схемы, отображаемые на УВО.

3.5 **формат (формат отображения)** (format [display format]): Графическое представление информации на УВО в виде текстового сообщения, цифрового представления, условных обозначений, мнемосхем, гистограмм, графиков, указателей, многоугольного образа.

[МЭК 60964:2009, пункт 3.7]

3.6 **абстрактное мышление** (high-level mental processing): Акт обработки и/или интерпретации информации человеком в целях получения краткой абстрактной информации.

[МЭК 60964:2009, пункт 3.12]

3.7 **человеко-машинный интерфейс** (human machine interface), ЧМИ: Интерфейс между оперативным персоналом, СКУ и информационно-вычислительными системами, обеспечивающими связь с АС. Данный интерфейс включает в себя средства отображения информации, органы управления и интерфейс системы поддержки оператора.

[МЭК 60964:2009, пункт 3.13]

3.8 **навигация** (navigation): Функция, которая поддерживает операторов в определении местоположения желаемой информации на УВО информационной системы, а также в управлении выбором отображений.

[МЭК 62241:2004, пункт 3.29]

3.9 **эксплуатационные процедуры** (operating procedures): Набор документов, определяющий оперативные задачи, которые необходимо выполнить для достижения функциональных целей.

3.10 **рабочая стратегия** (operating strategy): Формализованный подход, направленный на руководство разработкой эксплуатационных процедур и устанавливающий подходы к разрешению ситуаций высокой степени сложности, например, связанных с сохранением блока или возврата его в безопасное состояние после разгерметизации или нарушения охлаждения первого контура реактора.

3.11 **бумажно-ориентированные процедуры** (paper-based procedures): Эксплуатационные процедуры (см. пункт 3.9), напечатанные на бумажных листах.

3.12 **постулируемое исходное событие** (postulated initiating event): Событие, определяемое на стадии проектирования, как способное привести к ожидаемым эксплуатационным событиям или аварийным условиям.

[Глоссарий МАГАТЭ, 2007]

3.13 **последовательность** (sequence), **последовательность процедуры** (procedure sequence): Набор элементарных шагов в процедуре, которые должны быть полностью выполнены для достижения функциональной цели.

Примечания

1 Частичное выполнение последовательности может привести либо к неисправности, либо к отказам цепей или оборудования, либо поставить под угрозу выполнение функции.

2 Как правило, процедура включает в себя несколько последовательностей для достижения своей глобальной функциональной цели.

3 Последовательность может состоять из одного шага.

3.14 **шаг** (step): Единственная проверка параметров, единственное действие на компоненте АС, простое решение или устное сообщение между операторами, которые должны быть сделаны при выполнении процедуры.

3.15 **резервный пункт управлени**я (supplementary control room): Место, из которого может осуществляться ограниченное управление АС и (или) ее контроль для выполнения функций безопасности, определенных анализом безопасности, как это требуется в случае потери возможности выполнять эти функции из БПУ.

Примечание — Для существующих АС резервный пункт управления может быть специальным (отдельным) пунктом управления, но во многих случаях он включает в себя комплекты панелей управления и дисплеи в помещениях распределительных устройств или аналогичных местах. В последнем случае для таких панелей управления и дисплеев в этом стандарте используется термин «резервный пост управления».

[МЭК 60965:2016, пункт 3.6]

3.16 **устройство визуального отображения;** УВО [Visual Display Unit (VDU)]: Средство отображения информации, включающее в себя экран, на который выводится изображение, формируемое компьютером.

Примечание — Это примечание относится только к французскому языку.

[МЭК 60964:2009, пункт 3.31]

4 Обозначения и сокращения

В настоящем стандарте применяют следующие обозначения и сокращения:

АС (NPP) — атомная станция;

БПУ (MCR) — блочный пункт управления;

ВиВ (V&V) — верификация и валидация;

ИЧФ (HFE) — инженерия человеческих факторов;

КОП (CBP) — компьютерно-ориентированная процедура;

МАГАТЭ (IAEA) — международное агентство по атомной энергии;

ОВКВ (HVAC) — отопление, вентиляция, кондиционирование воздуха;

ЧМИ (HMI) — человеко-машинный интерфейс;

ПИС (PIE) — постулируемое исходное событие;

РПУ (SCR) — резервный пункт управления;

СКУ (I&C) — система контроля и управления;

УВО (VDU) — устройство визуального отображения;

ЦСО (DPDS) — цифровая система отображения;

ЭП (OP) — эксплуатационные процедуры.

5 Политика КОП и концептуальные требования

5.1 Общие требования

Раздел 5 содержит рекомендации по определению:

- четкой политики в отношении объема процедур, уровня рекомендаций и возможностей непосредственного управления процессом, например, с учетом опыта эксплуатации АС и человеческих возможностей, а также организационных и технологических вопросов;
- разновидностей семейств КОП;
- ключевых особенностей КОП;
- выходной документации.

5.2 Политика компьютеризации

5.2.1 Общие положения

Разработка политики компьютеризации должна быть частью определения концепции пункта управления, общей архитектуры средств измерения и управления, определения политики человеческих факторов и полезных принципов работы (см. МЭК 60964:2009, раздел 5).

Данную разработку следует поддерживать результатами анализа опыта эксплуатации, результатами концептуальных исследований, а также по возможности, некоторыми прототипами, используемыми при проектировании либо разработанными на раннем этапе проектирования.

Проектировщик должен определить типы процедур, подлежащих компьютеризации, и степень этой компьютеризации.

В руководящем плане проекта должны быть указаны причины компьютеризации процедур, поскольку они сильно влияют на то, какие процедуры будут компьютеризированы и в какой степени.

Внедрение КОП не обязательно решит проблемы рабочей стратегии или проблемы персонала, но проектное исследование для КОП может помочь прояснить характер этих проблем и помочь определить пути решения проблем на ранней стадии процесса проектирования.

Примечание — Возможные последствия для структуры оперативного персонала, компоновки блочного пункта управления, рабочих стратегий, состава процедур, проектирования и разработки автоматики и т.д. выходят за рамки настоящего стандарта.

В состав процедур, которые могут быть компьютеризированы, входят процедуры следующих типов:

- процедуры, регулирующие нормальную работу АС в нормальных условиях, например пуск АС, или процедуры, решающие элементарные задачи, а именно передачи тепла через трубопровод или снижение нагрузки и возврат к нормальной мощности;
- аварийные процедуры;
- процедуры реагирования на аварийную сигнализацию;
- процедуры пожаротушения;
- процедуры реагирования на потерю электропитания и любые виды процедур для непроектных условий;
- процедуры периодических испытаний, разработанные в соответствии с требованиями МЭК 60671, например, предназначенные для калибровки потока или для отключения реактора, или любые другие процедуры периодических испытаний.

Другие документы, которые также могут быть компьютеризированы:

- технические спецификации;
- таблицы технических компонентов, обеспечивающие легкий доступ к конкретным данным через устройство отображения ЧМИ.

5.2.2 Обоснование необходимости внедрения КОП

В дополнение к рассмотренным в других стандартах МЭК, перечисленных в разделе 2, проблемам по анализу задач, функциональному анализу и назначению, а также рекомендациям по проектированию учета человеческого фактора, при планировании проекта и на ранних этапах проектирования должны быть учтены следующие технические аспекты:

a) национальные нормативные аспекты;

b) рабочие стратегии: это функциональная проблема, которую следует рассматривать независимо от компьютеризации, например, если в случае аварии необходимо сделать выбор между стратегиями, основанными на состояниях или событиях;

c) организация эксплуатационного персонала:

при строительстве новой АС или модернизации существующей АС проект КОП может стать неотъемлемой частью общего проекта или проекта реконструкции пункта управления, что делает необходимым применение общепринятых методов инженерии человеческих факторов;

d) учет опыта эксплуатационного персонала:

1) следует учесть уроки, извлеченные из существующих КОП или бумажно-ориентированных решений;

2) кроме того, проектировщик может учесть, что следует компьютеризировать только рабочую стратегию или, наоборот, только детализированную часть процедур;

e) обучение операторов;

f) данные, полученные от средств контроля АС.

Примечание — Уровень рекомендаций КОП зависит от имеющихся измерительных приборов;

g) преимущества и недостатки обработки КОП и других рабочих функций в одной и той же системе следует тщательно взвесить в отношении ИЧФ, системных цифровых мощностей и компоновки БПУ. В частности, следует рассмотреть вопрос о возможной недоступности как КОП, так и других эксплуатационных функций, требующихся одновременно. Согласно МЭК 61513 необходимо рассмотреть всю архитектуру, включающую систему КОП, а также саму систему КОП.

Примечание — Система КОП может взаимодействовать с множеством систем, так что возможные состояния отказа и реакция оператора могут быть весьма важными.

Исходя из приведенных соображений, следует предварительно определить политику КОП и виды процедур, которые могут быть компьютеризированы.

5.2.3 Область применения КОП

Для идентификации функций, которые должны быть назначены операторам, в первую очередь должен применяться МЭК 61839.

Для того чтобы принять окончательное решение о видах компьютеризированных процедур и о степени или форме компьютеризации, которые должны быть реализованы (т.е. см. семейства КОП в 5.3), следует учитывать изложенное в МЭК 61772:2009, разделы 4 и 5, а также следующие вопросы, которые должны быть рассмотрены в концептуальном проекте:

- определение видов процедур, которые могут быть обработаны одновременно (то есть несколькими операторами) при нормальной работе, в случае пожара, в случае потери электропитания, в случае периодического испытания, в случае ПИС;
- определение уровня безопасности рекомендаций оператору предоставляемых КОП и времени реагирования оператора, а также степени их соответствия принятым или требуемым значениям;
- оценка количества форматов отображения и количества УВО, необходимых для этих процедур;
- оценка максимального количества процедур, которые могут быть обработаны параллельно одним оператором или всем эксплуатационным персоналом при работе в случае возникновения наихудшей проектной комбинации событий;
- оценка максимального количества окон, которые могут отображаться параллельно в наихудших случаях на одной рабочей станции или на всех рабочих станциях пункта управления;
- распределение задач эксплуатационного персонала между КОП и бумажно-ориентированными процедурами согласованным образом (например, для исключения ошибок оператора).

Вышеуказанную оценку следует выполнять с учетом концепции пункта управления. При этом необходимо учитывать следующие вопросы:

a) набор рабочих станций и рабочих мест, в которых предполагается использовать КОП, в блочном пункте управления и во всех других постах управления;

b) тот факт, что процедура может быть временно приостановлена, например в случае возникновения тревоги;

c) максимальный объем информации, отображаемой в формате;

d) производительность системы КОП, в частности, в отношении отображений, емкости памяти и навигации;

e) достаточные дополнительные поля, чтобы облегчить будущие изменения.

Кроме того, системный класс системы КОП (см. МЭК 61513), который может быть достигнут, следует рассматривать на ранней стадии процесса проектирования, когда принимаются решения о функциональном распределении. Системный класс системы КОП, который может быть достигнут, будет часто определяться возможностью реализации аттестации различных элементов общей архитектуры, в которой реализуется система КОП. Эти элементы обычно включают в себя: проект КОП, систему КОП, ЦСО и системы управления, через которые КОП взаимодействует с АС и базовыми сетями, обеспечивающими связь между этими элементами.

Приведенные положения могут оспаривать аспекты политики внедрения КОП, предлагаемого проекта системы КОП, ее возможностей и ее эксплуатации или связанных с ними затрат и выгод, а также изменения структуры или рабочих стратегий.

Следует определить содержание и границы человеческих факторов, а также провести организационные исследования для:

1) определения человеческих ресурсов, необходимых для реализации проекта, то есть специалистов, которые должны быть интегрированы в команду проекта, специалистов для верификации и валидации, организации обслуживания КОП;

2) использования конечного продукта, включая средства технического обслуживания.

Для принятия решения может использоваться изложенное в МЭК 60964, МЭК 61772, МЭК 61839, МЭК 62241, ИСО 11064 и, особенно, в ИСО 11064-1, ИСО 11064-3, ИСО 11064-4 и ИСО 11064-5. Изложенное в МЭК 60965 может использоваться в случае, когда некоторые КОП должны быть реализованы в резервном пункте управления.

5.3 Семейства КОП

Несмотря на то, что в соответствии с политикой проектирования процедуры могут быть компьютеризированы по-разному, их реализацию следует рассматривать в рамках одного из трех общих семейств КОП, как показано в таблице 1. Эти три семейства основаны на рассмотрении:

- предполагаемого уровня рекомендаций оператору;
- требуемых входов и выходов процесса.

Таблица 1 — Семейства КОП

Определение семейства КОП		Уровень поддержки оператора		
		Нет шагов отслеживания/ручной ход	Автоматическое отслеживание шагов	Управление возможностью
Тип сигнала КОП интерфейса	**Нет ввода** информации процесса	1	Невозможно	Невозможно
	Ручной ввод информация процесса	1	Невозможно	2
	Автоматический ввод информации процесса	2	2	2 или 3
	Действия по процессу	3	3	3

Строки таблицы соответствуют разным уровням связи с системой КОП — от информации процесса до действий по процессу. В столбцах представлены различные уровни компьютеризации и связанный с ними интеллект. На самом продвинутом уровне поддержки оператора система может предоставить помощь оператору; эта особенность называется возможностью руководства (см. 8.5).

Пересечения строк и столбцов содержат возможные варианты семейства КОП.

Эти три семейства КОП характеризуются следующим образом:

- семейство 1: КОП, которые являются по существу автономными заменами бумажных процедур, представляя связанные страницы статической информации и этапов работы. Оператор может иметь возможность вводить некоторые данные вручную, чтобы облегчить понимание процедуры.

КОП этого семейства не получает никакой информации о процессе автоматически и не обладает возможностями управления АС;

- семейство 2: КОП, которые могут давать рекомендации оператору на основе информации, полученной системой КОП. Каждый элемент информации может быть интегрирован в представленные форматы отображения. Если необходимы расширенные рекомендации, например в форме помощи по решению (см. 8.5.4), тогда соответствующую КОП следует отнести к семейству 3;

- семейство 3: КОП, предоставляющая информацию и рабочие шаги при полной интеграции с оперативной информацией об АС, состояниях и значениях параметров для того, чтобы оператор мог управлять исполнительным механизмом с устройства отображения КОП, при этом функции автоматического управления могут быть доступны через устройство отображения КОП, а автоматический запуск последовательности действий может быть инициирован оператором с устройства отображения КОП.

Распределение КОП по семействам и связанная с ним аргументация должны быть документированы.

Все семейства могут включать отдельные объекты, указанные в 8.7.

Примечание — Ручной ввод применяется для передачи ограниченного объема информации, иначе задача ввода информации будет слишком сложной для оператора.

Для каждого типа процедур, перечисленных в 5.2.1, может быть выбрано другое семейство КОП, поскольку необходимо поддерживать простой и понятный инженерный подход.

Выбор типа семейства КОП, проект КОП и общая архитектура, в которой реализуется КОП, влияют на распределение (или разделение) каждой функции КОП между человеком-оператором, другими аппаратными или компьютеризованными ЧМИ БПУ, системой КОП и другими различными элементами общей архитектуры. Функциональное распределение определяет надежность безопасности (то есть зависимость для безопасности, включая необходимые требования к отказоустойчивости или обнаружению отказов), которая будет распределена в системе КОП и различных элементах общей архитектуры, которые реализуют или способствуют реализации каждой из различных функций КОП. Поэтому полученный требуемый системный класс будет прямым результатом проектирования КОП, включая тип семейства КОП, и функциональное распределение в общей архитектуре КОП.

Примечание — В зависимости от архитектуры средств измерения и управления АС, особенно во время их модернизации, может оказаться невозможным внедрение систем КОП семейства 2 и семейства 3.

5.4 Обзор особенностей компьютеризации

5.4.1 Общие положения

Компьютеризация основана на общих правилах и требованиях, а также на вопросах, связанных с рекомендациями оператору и управлением АС.

5.4.2 Общие требования к компьютеризации

Для процедур, относящихся ко всем семействам:

- КОП на постоянной основе либо по запросу оператора должна предоставлять возможность отображения главной цели процедуры и обзора последовательностей ее выполнения. КОП по запросу оператора должна отображать дополнительную информацию о таких шагах или последовательностях, как предварительные действия, процессы и ожидаемые реакции устройства;
- проектировщик должен убедиться, что набор процедур и соответствующие им требования к производительности системы обработки соответствуют потенциальным возможностям системы КОП.

В отношении КОП, принадлежащих к семейству 1, процедуре компьютеризации следует:

a) быть интуитивно понятной и максимально простой;

b) давать четкое представление о функциональной цели;

c) обеспечивать легкое понимание оператором действующей стратегии;

d) обеспечить, чтобы контекст последовательности КОП не был потерян для оператора;

e) оставлять полную ответственность за операторами;

f) облегчать продвижение внутри процедур и ограничивать вызовы между процедурами.

Для КОП, принадлежащих к семействам 2 и 3, процедуре компьютеризации следует:

1) соблюдать рекомендации, установленные для КОП, принадлежащих к семейству 1;

2) предоставлять оператору возможность оставлять без завершения шаги и последовательности, которые не имеют отношения к достижению цели процедуры более высокого уровня;

3) обеспечивать надлежащие проверки (предпочтительно автоматические) и блокировки безопасности состояния АС или оборудования, гарантирующие возможность и безопасность выполнения в текущее время запрошенной последовательности или информирующие оператора в противном случае;

4) исключать возможность выполнения переопределений условий безопасности из системы КОП (то есть не следует допускать такие переопределения);

5) поддерживать соответствующие подтверждения оператора перед выполнением автоматических последовательностей;

6) предоставлять адекватную и согласованную информацию и форматы отображения для членов команды операторов, которые могут работать на независимых устройствах отображения КОП, и обеспечивать обнаружение и четкое указание оператору любых несоответствий, которые могут возникать на независимых устройствах отображения КОП из-за внутренних сбоев системы КОП;

7) применять одинаково ко всем процедурам данного типа, например, ко всем аварийным процедурам или ко всем процедурам управления пожаром;

8) быть согласованной для различных типов процедур, которые могут обрабатываться параллельно.

5.4.3 Представление рекомендаций оператору

Рекомендации, представляемые КОП, должны напоминать операторам о функциональных задачах и детализировать информацию о надлежащей последовательности шагов эксплуатационных процедур, а также предоставлять информацию и рекомендации, направленные на успешное выполнение каждого шага и общих целей.

В дополнение к предоставлению оператору элементарной информации о процессе, расширенная информация о процессе может предоставляться посредством доступа к КОП, диагностики или руководства по принятию решений.

Диагностика или руководство по принятию решений могут быть:

- автоматизированные: оператору предлагается диагностика или решение, затем он может запросить подробную информацию об этом;
- поддерживаемые: КОП, отображающие блок-схемы, которые помогают оператору установить диагноз или решение. При этом осуществляется легкий поиск информации, необходимой оператору для выполнения простого выбора, или информация включена в блок-схемы так, чтобы оператор мог последовательно подтверждать каждый шаг.

При разработке руководства КОП следует уделять должное внимание:

a) состоянию АС, при котором будет применяться КОП;

b) частоте событий или ситуаций. Например, для редких событий следует предусмотреть расширенное руководство по сравнению с применяемыми в повседневной работе;

c) эксплуатационной политике. Например, стремление к высокой доступности АС может привести к увеличению компьютеризации и автоматизации;

d) действиям оператора, когда они необходимы или когда эти действия требуются только в течение определенного срока (т. е. с учетом соответствующих аварийных сигналов или уведомлений оператору, которые могут потребоваться, или с учетом осторожных безопасных действий, необходимых в случае неспособности оператора действовать);

e) отзывам и требованиям персонала.

Разработчик руководства должен учитывать характеристики системы КОП, то есть производительность, внешнее оформление.

Возможности оператора по запросу элементарной информации могут быть расширены для расчетов, приводящих к обобщенной информации высокого уровня.

КОП предоставляет оператору синтезированную информацию и, возможно, некоторую помощь, как описано в 8.7.

5.4.4 Предоставление автоматизированной процедуры

КОП может помочь оператору в управлении АС:

- автоматически предоставляя сообщения оператору при выполнении заданных условий;
- автоматически выполняя последовательности, которые были инициированы оператором.

Что касается бумажно-ориентированных процедур, КОП следует разрабатывать с учетом:

- распределения функций между оператором и системой КОП, системой автоматизации АС или ЦСО;
- того, что процедура, установленная для резервной системы, не зависит от ЦСО и системы КОП;
- простоты понимания оператором, особенно в аномальных условиях.

Дополнительные соображения, которые необходимо учитывать:

a) следует избегать дублирования функций между оператором и системой, за исключением случаев, когда они спроектированы как резервное средство, и следует искать проектные решения, в которых система КОП и оператор выполняют взаимодополняющие функции;

b) форматы отображения КОП могут включать в себя возможности команд или могут перенаправлять операционные действия для управления форматами отображения ЦСО. Другой вариант может заключаться в том, чтобы разрешить команды КОП, разрешив их из ЦСО.

Понимание обстановки оператором должно быть улучшено за счет:

1) отображения адекватной информации, чтобы оператор был полностью информирован об изменении состояния АС:

важные решения не следует автоматизировать, завершение автоматических последовательностей следует сопровождать оповещением, следует оповещать о любых проблемах, возникающих во время автоматической последовательности, а также о значениях параметров процесса, достигших предопределенного порога;

2) предоставления оператору возможности в любой момент взять КОП под контроль.

Примечание — В некоторых ситуациях может потребоваться прекращение действия КОП, в то время как для других ситуаций может потребоваться от оператора взять под контроль ограниченное количество шагов;

3) координации действий оперативной группы:

последовательности, запущенные двумя операторами, могут иметь разные времена выполнения и не должны приводить к противоречивым или конкурирующим действиям.

5.5 Выходная документация

Логические обоснования и предположения о внедрении КОП (как описано в 5.1—5.4) должны быть задокументированы на раннем этапе проекта и включают:

- политику, концептуальные требования и философию реализации КОП;
- типы КОП, их цели и объем;
- подход и предположения по внедрению КОП, включая соображения ЦСО;
- варианты руководства КОП, включая описание исходных данных проекта и другую необходимую информацию;
- варианты процедурно-ориентированной автоматизации;
- политику обучения операторов.

5.6 Запроектные условия

В случае возникновения запроектных условий система КОП должна считаться недоступной (см. примечание). Набор бумажно-ориентированных процедур, предназначенных для работы в запроектных условиях, должен применяться для управления АС из БПУ, то есть КОП не следует проектировать для работы в таких условиях.

Примечание — Так как система КОП не предназначена для работы в запроектных условиях, то предполагается, что система КОП может стать недоступной или ненадежной в любое время.

Обновление комплектов КОП и бумажно-ориентированных процедур должно быть скоординировано и согласовано с процедурами резервного копирования.

Оперативный персонал должен быть обучен использованию этих комплектов процедур, упражнения по их применению должны выполняться периодически.

6 Применение КОП

6.1 Общие положения

Раздел 6 устанавливает требования к различным условиям применения КОП. В нем рассматриваются различные условия использования КОП применительно к БПУ и в возможной связи с бумажно-ориентированными процедурами. Раздел 6 учитывает требования возможных различных форм помощи и координации деятельности оператора. Он завершается описанием состава выходной документации.

6.2 Применение КОП в производственных условиях

6.2.1 Общие положения

В 6.2 рассматриваются различные условия, в которых КОП может использоваться либо в новых компьютеризированных пунктах управления, либо в частично модернизированных обычных пунктах управления в сочетании с бумажно-ориентированными процедурами, либо при локальной эксплуатации оператором вне пункта управления.

Общая интеграция КОП в БПУ и в других постах управления должна быть выполнена на основе МЭК 60964, МЭК 60965 и МЭК 61513. Применение УВО должно соответствовать МЭК 61772. Функции и представление сигнализации должны соответствовать МЭК 62241. Программное обеспечение должно соответствовать МЭК 60880 или МЭК 62138 в соответствии с категорией безопасности.

6.2.2 Применение КОП в компьютеризированных пунктах управления

Должна быть предусмотрена возможность раздельного управления форматами отображения системы КОП и другими форматами отображения ЦСО.

Совместимость форматов КОП и рабочих форматов ЦСО следует обеспечивать:

- проектированием совместимых макетов ЧМИ и деталей для форматов отображения, то есть аббревиатур, символов, цветов и т. д.;
- предотвращением несоответствий в том случае, когда рабочие форматы и форматы КОП относятся к одному объекту, цепи или оборудованию;
- обновлением форматов ЦСО и КОП, при их одновременном отображении, без существенной разницы во времени, связанной с форматами.

6.2.3 Применение КОП в обычном или гибридном блочном пункте управления

«Обычный пункт управления» — это такой пункт, который был спроектирован без какого-либо цифрового оборудования. «Гибридный пункт управления» — это пункт, который включает в себя циф-

ровые устройства для контроля и управления частью АС, но не всей АС. Обычные пункты управления могут быть преобразованы в гибридные пункты управления. Степень компьютеризации гибридного пункта управления, исключая все другие элементы управления АС, может сильно варьироваться в зависимости от практических целей.

Для реализации КОП в обычном или гибридном пункте управления в дополнение к требованиям, приведенным в 5.2.3, должны рассматриваться ограничения существующего БПУ, то есть в основном наличие свободного пространства и свободных рабочих областей оператора. Применение устройств для отображения КОП в обычном БПУ может потребовать замены существующих элементов, индикаторов, кнопок и т. д., чтобы освободить место для установки наборов УВО и соответствующего оборудования, такого как клавиатуры, планшеты, шаровые манипуляторы и т. д.

Примечание — Также рассматриваются возможности таких служб, как ОВКВ (отопление, вентиляция и кондиционирование воздуха).

В качестве конкретной задачи для обычных и гибридных пунктов управления следует изучить одновременное использование КОП с обособленным оборудованием, таким как индикаторы, регистраторы, кнопки, автоматические ручные станции управления и т.д. Кроме того, необходимо предположить и проанализировать параллельное использование КОП и бумажно-ориентированных процедур.

Принимая во внимание, что компьютеризация управления АС ограничена, КОП следует спроектировать для предоставления информации и рекомендаций, то есть их следует отнести к семейству 1 или семейству 2 и привести в соответствие требованиям для этих семейств.

Кроме того, следует предусмотреть конкретные положения:

- спроектировать КОП ЧМИ, чтобы в случае отображения информации УВО оператор не путал КОП с любыми другими отображаемыми форматами, особенно в условиях аварии. Если нет других форматов цифрового отображения, ИСО 11064-1, ИСО 11064-3, ИСО 11064-4 и ИСО 11064-5 и МЭК 61772:2009, особенно раздел 4, следует использовать для определения любых требуемых отображаемых форматов;
- позволить операторам считывать КОП из своих рабочих областей, либо находясь перед УВО, либо на некотором расстоянии от УВО.

6.2.4 Применение КОП в сочетании с бумажно-ориентированными процедурами

КОП допускается использовать вместе с бумажно-ориентированными процедурами либо по причинам, изложенным в проекте, либо по временным причинам в зависимости от вариантов, определенных в соответствии с 5.2.3.

Примеры

1 Детальная работа остается бумажно-ориентированной, тогда как рабочая стратегия компьютеризирована.

2 Конкретные наборы бумажно-ориентированных процедур используются, например, во время отключений, реализуемых при обнаружении ошибки в компьютеризированной процедуре, до тех пор, пока не будет подготовлена правильная новая компьютеризованная версия.

Совместное применение процедур должно быть спроектировано таким образом, чтобы:

- между КОП и бумажно-ориентированными процедурами отсутствовал разрыв;
- возможное перекрытие между КОП и бумажно-ориентированными процедурами было функционально обосновано;
- ссылки и наименования КОП и бумажно-ориентированных процедур были согласованы и не приводили к ошибкам человека;
- переадресация между КОП и бумажно-ориентированными процедурами была ясна;
- обеспечивалась возможность отслеживания действий, выполняемых как с помощью КОП, так и с помощью бумажно-ориентированных процедур;
- ситуация оставалась легкой для объяснения во время смены персонала.

6.2.5 Применение КОП вне блочного пункта управления

Если некоторые локальные пункты управления, например РПУ, компьютеризированы и работают с КОП, то последние должны быть адаптированы под задачи оператора.

Операции с местных постов управления, если они компьютеризированы, или с любых типов переносных устройств должны учитывать требования, изложенные в 6.4.

6.3 Формы поддержки деятельности оператора с помощью КОП

6.3.1 Общие положения

КОП должны быть спроектированы таким образом, чтобы обеспечить операторам возможность реагировать на обстоятельства, принимая во внимание реальную ситуацию на АС, отслеживая процесс и обнаруживая события.

Процедуры предназначены для оказания помощи оператору, предлагая рабочие стратегии и готовя возможные действия относительно состояния АС. Тем не менее могут возникнуть непредвиденные ситуации, в которых оператор должен иметь возможность достичь цели высшего уровня, установленной процедурой, даже если некоторые части этой процедуры стали неактуальными.

Для целей настоящего стандарта функции КОП разделены на основные функции (например, предоставление информации оператору) и второстепенные функции (например, управление окнами и навигацией в пределах необходимой информации).

6.3.2 Поддержка основной деятельности оператора

На этапе проектирования КОП должны быть рассмотрены следующие концепции с документированным обоснованием проектных решений по каждой концепции:

- совместимость с представлением оператора.

Аспекты ЧМИ совместимы с абстрактным мышлением оператора, то есть с пониманием, опытом и ожиданиями оператора относительно состояния и эволюции АС и способа осуществления функции КОП;

- представление ситуации.

Отображаемая информация легко идентифицируема и понятна, точность воспроизводимых значений согласована с точностью измеренных значений, так что она помогает абстрактному мышлению и продвижению оператора к функциональной цели процедуры. Следует отображать степень достоверности данных;

- структура ЧМИ.

Аспекты ЧМИ основаны на логических и согласованных правилах. Основными аспектами ЧМИ являются представление информации, иерархия последовательностей в рамках процедуры, терминология, фразеология помощи, структура списков и т. д.;

- совместимость с деятельностью.

Отображаемая информация имеет отношение к состоянию АС;

- возможности оператора.

Объем отображаемой информации позволяет оператору понять ее содержание, и оператору достаточно времени, чтобы принять правильные решения.

Контекстная информация может отображаться для усиления обоснованности информации и для содействия пониманию оператора.

6.3.3 Поддержка второстепенной деятельности оператора

Для того чтобы упростить оператору выполнение обязанностей и позволить ему сосредоточиться на основных задачах, во время проектирования следует учитывать следующие аспекты. Основные проектные решения по каждому аспекту следует задокументировать, включая их обоснование:

- интеллектуальная нагрузка оператора.

Сводится к минимуму запоминание предметов, таких как списки кодов, коды команд, информация для запоминания, переходящая с одной страницы на другую;

- действия оператора.

Действия выполняют легко, избегают лишних действий.

Второстепенная деятельность оператора касательно КОП должна быть простой и должна выполняться надежным способом, так чтобы не ухудшалось выполнение основных видов деятельности.

6.4 Поддержка координации оператора

КОП следует четко указывать связи в отношении последовательностей, назначенных отдельному представителю оперативного персонала, то есть сообщений, необходимых для обмена информацией между операторами и руководителем. Такая координация может быть реализована путем удержания в процедурах, запроса устных диалогов и компьютеризированных подтверждений.

Следует обратить внимание на то, что, например, когда руководитель является единственным пользователем КОП и затем координирует других операторов, или как руководитель, так и первичный и вторичный операторы снабжены КОП, процедура должна указывать, какая связь необходима между ними.

Если несколько операторов могут одновременно обращаться к одной и той же КОП, должны быть указаны правила управления одновременным доступом к одной процедуре. Должны быть определены следующие вопросы:

- кто может получить доступ к КОП, в соответствии с уровнем полномочий;
- какой вид доступа разрешен: только для чтения или для полного использования;
- как осуществляется доступ к выполняемой в настоящее время КОП;
- как предотвратить повторение или прекращение действия процедуры, запущенной другим оператором, особенно когда эта КОП предназначена для управления АС. Это может быть достигнуто путем резервирования процедур, что гарантирует, использование КОП для управления АС только одним оператором, тогда как все остальные операторы имеют доступ только для чтения.

Резервирование процедур требует определения политики относительно возможных вызовов другой процедуры или подпроцедуры;

- какие сигналы КОП предоставляются, то есть сигналы, предупреждающие о том, что КОП в настоящее время используется, или сигналы, указывающие на то, что КОП зарезервирована в течение длительного времени без использования.

Все специфические процедуры могут быть назначены только определенным рабочим станциям.

КОП должна обеспечивать координацию операторов для параллельного использования КОП в блочном пункте управления и в местных постах управления. Возможные отказы цифровой связи не должны снижать надежность и доступность КОП в БПУ и в местных постах управления. Во избежание несогласованного управления процессом следует оповещать о значительной разнице между операциями, использующими один и тот же набор КОП.

6.5 Выходная документация

Все условия, определенные в соответствии с 6.3 и 6.4, следует задокументировать в соответствующих документах:

- краткие варианты представления и обоснования фаз проектирования, разработки, проверки и лицензирования;
- сводка для операторов, которой следует быть памяткой, простой в использовании в аномальных ситуациях на АС;
- подробный документ, применимый в качестве ориентира для проектирования и технического обслуживания КОП.

Указанная документация должна обновляться вместе с дальнейшими изменениями КОП для обеспечения целостности.

7 Компьютерно-ориентированные процедуры и функциональные требования

7.1 Общие положения

Раздел 7 касается цифровой системы обработки КОП, будь она интегрирована в управляющую АС ЦСО или независима от нее. Рассмотрены требования безопасности и небезопасности.

Затем в разделе 7 изложены требования к обработке отказов системы КОП. Этот раздел заканчивается требованием к выходной документации.

Независимо от решения экранные заставки не должны использоваться.

7.2 Требования безопасности

Необходимо внимательно рассмотреть фундаментальную роль безопасности КОП, когда она играет какую-либо роль в безопасности вообще или является частью стратегии глубоко эшелонированной защиты АС в целом. Система КОП не должна дискредитировать защиту СКУ АС.

Бумажно-ориентированные и компьютерно-ориентированные процедуры, независимо от их уровня управления, предназначены для использования оператором, и они не должны управлять процессом без участия оператора (т.е. запуск процедуры и наблюдение выполняет оператор). Ожидается, что оператор будет действовать разумно, а не применять процедуры автоматически, и будет нести полную ответственность за их надлежащее использование.

В соответствии с МЭК 61513 классификация безопасности системы КОП может быть проведена на соответствие классам 1, 2 и 3 или КОП может быть вообще не классифицирована. Класс КОП должен быть установлен с учетом:

a) функционального охвата КОП;

b) типа семейства КОП.

Примечание — Различные типы семейств КОП перечислены в 5.3;

c) возможного воздействия на безопасность в случае:

1) потери КОП,

2) ошибочного указания операторам или ложного сигнала управления.

Пример — Возможные и приемлемые режимы отказа каждой КОП, воздействия на информированность оператора и его способность реагировать на события, произошедшие на АС, вероятность ошибки оператора (например, из-за зависимости от времени, сложности и важности безопасности принятия решений и т.д.) и наличие резервных средств восстановления после отказа;

d) доступности разнообразной информации, предоставляемой оператору, что позволяет подтверждать информацию, отображаемую КОП. Оператору следует пройти обучение для проведения сравнений информации (см. 9.9).

Примечание — Хотя согласно МЭК 61226:2009 (подпункт 7.3.2.1) существует возможность выполнять ручные функции категории А путем взаимодействия системы КОП с системой класса 1, внимание проектировщика обращается на тот факт, что это требует значительного анализа в поддержке доказательств безопасности, особенно вытекающих из аспектов инженерной психологии.

КОП может быть реализована в виде нескольких подсистем с различными классами безопасности.

Требования и рекомендации, приведенные в МЭК 61513, МЭК 60880 и МЭК 62138, следует применять при проектировании и внедрении общей архитектуры средств измерения и управления, входящих в состав системы КОП, а также для самой системы КОП. Уровень избыточности системы КОП должен соответствовать классу безопасности системы КОП. Требования, определенные в МЭК 61772:2009 (пункт 4.3), должны выполняться.

Примечание — Требуемый системный класс безопасности может ограничить возможные варианты с точки зрения подхода к проектированию КОП, включая то, какие типы семейств КОП могут быть реализованы. Если необходимый системный класс не может быть достигнут и аттестован, должен быть рассмотрен альтернативный подход. Это может потребовать изменения типа семейства КОП, подхода к проектированию и функциональных распределений. Это может также потребовать изменения выбора платформы КОП, изменения механизмов связи или изменения ее общей архитектуры. Неспособность рассмотреть такие проблемы на раннем этапе проекта внедрения системы КОП может привести к дорогостоящим задержкам и необходимости перепроектирования.

В случае если для системы КОП не определен класс безопасности, требования, соизмеримые с возможными эксплуатационными воздействиями, следует определить на основе стандартов МЭК, перечисленных в предыдущем абзаце.

Надлежащая проверка последовательностей, запущенных КОП, должна осуществляться в системах управления АС. Проверка должна включать контроль любых блокировок, необходимых для обеспечения безопасности.

Особое внимание должно быть уделено этапам разработки и верификации, чтобы гарантировать, что потенциальные неисправности или сбои системы КОП не смогут отключать, блокировать или запускать ручные и автоматические функции. Следует исследовать функциональные последствия ошибочных или несинхронизированных данных, полученных от других систем, в частности, систем автоматизации. Исследования безопасности должны учитывать общую архитектуру средств измерения и управления, входящих в состав системы КОП, а также саму систему КОП.

7.3 Особенности человеко-машинного интерфейса

Требования к ЧМИ указаны в стандартах: МЭК 61772:2009 (в частности, разделы 4 и 5), ИСО 11064, ИСО 11064-1, ИСО 11064-3, ИСО 11064-4 и ИСО 11064-5.

Для ЧМИ в части форматов отображения КОП возможны только три случая:

1) цифровая система ЦСО уже используется для управления АС в то время, когда проектируются КОП и система КОП: ЧМИ этих двух систем должен быть совместимым;

2) цифровая система ЦСО разрабатывается параллельно с КОП и системой КОП: ЧМИ двух систем должен быть совместимым. Для проектирования форматов отображения обеих систем следует использовать МЭК 61772 и ИСО 11064;

3) нет другой цифровой системы, отображающей информацию на экране для управления АС. МЭК 61772 и ИСО 11064 должны использоваться при проектировании форматов отображения КОП.

7.4 Интеграция системы КОП в ЦСО

Чтобы интегрировать КОП в состав ЦСО, должно быть подтверждено, что:

- класс безопасности ЦСО согласуется с классом безопасности КОП, как предусмотрено в соответствии с изложенным в 7.2;
- характеристики ЦСО соответствуют требованиям 5.2.3;
- для КОП, принадлежащих к семейству 3 и реализующих функции категории В, как система отображения на АС, так и линии связи с ней отвечают требованиям МЭК 61513 и МЭК 62138 для класса 2;
- характеристики ЦСО соответствуют требованиям раздела 8.

Требования и рекомендации МЭК 61772 должны применяться.

7.5 Система КОП, внедренная в ЦСО

7.5.1 Общие положения

Подраздел 7.5 дополняет требования безопасности, указанные в 7.2, и касается соединений между системой КОП и ЦСО.

Для принадлежащих к семействам 2 и 3 КОП, которые взаимодействуют с АС через ЦСО, систему КОП и ЦСО следует отнести к совместимым классам безопасности и требованиям, если иное не предусмотрено четким обоснованием.

Для КОП, принадлежащих к семейству 3, распределение задач между системой КОП и системами управления АС должно быть следующим:

- инициирование автоматических последовательностей оператором должно быть на уровне отображения компьютера, а также в режиме удержания;
- запускаемые КОП автоматические последовательности, возможно, использующие вводы АС и обратные связи исполнительных механизмов, должны обрабатываться системами управления АС.

7.5.2 Требования к оценке размеров и общей надежности

В дополнение к требованиям безопасности необходимо учитывать:

- система КОП должна соответствовать требованиям 5.2.3;
- требования к надежности и эксплуатационной готовности должны быть совместимы для системы КОП и ЦСО;
- должна быть предусмотрена самодиагностика системы КОП;
- для обеспечения возможности последующего расширения системы следует точно определить ее необходимую резервную мощность с учетом таких элементов, как память, производительность процессора, емкость хранилища данных, пропускная способность сети и количество подключаемых рабочих станций.

7.5.3 Соединения между системой КОП и системой обработки и отображения данных

Архитектура и системные аспекты должны соответствовать МЭК 61513.

Должны быть реализованы меры предосторожности во избежание расхождений между командами, отправленными системой КОП и ЦСО, или, по крайней мере, о таких расхождениях оператор должен быть оповещен.

Учитывая, что некоторые значения параметров, полученные от процесса или оборудования, могут использоваться как системой КОП, так и ЦСО при реализации различных функций и, возможно, отображаться в разных форматах, тогда:

- обе системы следует анализировать вместе в отношении режимов отказов, а также резервного процесса в случае отказа и периодического тестирования;
- система КОП не должна подвергаться опасности из-за возможных отказов ЦСО и наоборот;
- отказ системы КОП должен сигнализироваться ЦСО, а частичные или полные отказы ЦСО должны сигнализироваться независимым сигналом тревоги;
- отказ интерфейса между двумя системами должен сигнализироваться хотя бы одной из двух систем;

- отправка сигналов от обеих систем к одному и тому же исполнительному механизму должна сигнализироваться либо одновременно, либо в течение нескольких минут. Противоречивые приказы должны сигнализироваться определенным образом;

- следует принять меры для минимизации разницы во времени при обновлении динамических частей отображений одного и того же объекта. Значение в диапазоне до 2 с может считаться приемлемым, большие различия следует указывать.

7.5.4 Согласованное обслуживание системы КОП и ЦСО

Техническое обслуживание с точки зрения аппаратного обеспечения, программного обеспечения, конфигурации и приложений следует учитывать для обеих систем, включая процесс переаттестации.

7.6 Отказы системы КОП

Общие положения относительно отказов УВО приведены в МЭК 61772:2009 (пункты 4.3 и 4.4).

Операторы должны быть обучены, чтобы отслеживать эффективность КОП. В обеспечение поддержки операторов в системе КОП должны быть реализованы условия самоконтроля и самопроверки для обнаружения и сигнализации отказа. Учитывая возможные последствия ошибочных действий операторов, их охват самоконтролем следует сделать как можно более высоким. Для КОП, принадлежащих к семейству 3, следует предусмотреть надлежащие отказоустойчивые механизмы, где это возможно. Чтобы обеспечить обнаружение неисправностей КОП, часть оперативного персонала может использовать бумажно-ориентированные процедуры.

Примечание — Основными способами обнаружения неисправностей в настоящее время являются самоконтроль, осуществляемый в соответствии с МЭК 60671, а также независимые механизмы выполняемых персоналом контроля и периодического наблюдения.

Если оператор подозревает наличие в КОП неисправности, которая не была обнаружена или не опознана системой, например неожиданные отклонения параметров, система КОП, ее части или подсистемы средств измерения и управления могут считаться неработоспособными.

В случае отказа КОП, важных для безопасности, или отказа системы КОП, реализующих функции безопасности (например, категории В или С), должны быть использованы разнообразные резервные средства и адаптированный набор процедур. Этот набор резервных процедур должен быть совместим с ЦСО, если эта система все еще работоспособна и используется для управления АС.

Примечание — Степень резервирования средств и связанных с ними процедур обычно ограничивается набором функций, необходимых для перевода АС в безопасное состояние и поддержания ее в этом состоянии, а также для сведения к минимуму воздействия на работу АС до восстановления системы КОП или ЦСО.

Разнообразный набор средств, предназначенных для резервирования системы КОП (например, таких как ручные бумажно-ориентированные процедуры), должен учитывать, что ситуация отказа является редкой и напряженной, и должен быть направлен на то, чтобы избежать недоразумений или ошибок операторов, а для этого необходимо:

- быть независимым от системы КОП, как с технической, так и с функциональной точки зрения, то есть не иметь ссылок на информацию, существующую только в системе КОП;
- опираться на рабочие стратегии, аналогичные стратегиям КОП;
- предназначаться для одного и того же оперативного персонала;
- использовать, по возможности, совместимые с представлением КОП словарные и графические элементы, а также представления процедур.

Резервный набор процедур и любая связанная резервная система должны быть легкодоступны.

Резервная система и набор резервных процедур, если они компьютеризированы, должны быть спроектированы, разработаны и испытаны в соответствии с их классом безопасности и должны соответствовать требованиям раздела 9.

Примечание — Выбор второго набора КОП в качестве резервного представляет собой большую проблему, поскольку это подразумевает использование различных систем КОП с обнаружением неисправностей, более сложным обслуживанием и обучением операторов. По этой причине обычно предпочтительны бумажно-ориентированные процедуры. Для принятия такого решения также рассматриваются экономические аспекты.

Если КОП реализуются как отдельная от ЦСО система, то применяют следующие правила:

- ЦСО следует контролировать систему КОП и сигнализировать обнаруженные неисправности персоналу пункта управления;
- ЦСО не следует блокировать в случае отказа системы КОП.

7.7 Выходная документация

Системные и функциональные требования, соответствующее обоснование проекта (варианты и решения) общей архитектуры и подхода к системе КОП должны быть задокументированы в соответствии с требованиями МЭК 61513 (и соответствующими стандартами того же уровня, что и МЭК 62138) и в соответствии с классом безопасности системы.

8 Требования к детальному проектированию

8.1 Общие положения

В разделе 8 приведены рекомендации и установлены требования к детальному проектированию характеристик КОП (начиная с основных и заканчивая самыми сложными), например, таких как управление АС, информация, навигация и рекомендации по управлению. Также даны различные варианты, которые могут облегчить использование КОП.

8.2 Основные характеристики КОП

8.2.1 Общие положения

Для координации развития КОП, чтобы избежать неправильной интерпретации при их использовании и облегчить их обслуживание, основные характеристики КОП должны быть определены в самом начале проекта и должны использоваться в течение всего жизненного цикла КОП. Эти основные характеристики должны использоваться при проектировании, разработке и обслуживании набора КОП.

Примечание — Специалисты, модернизирующие КОП, могут не быть ее разработчиками.

Указанную деятельность следует выполнять интегрированной командой, представленной в 9.3. Следует принять во внимание опыт, основанный на использовании бумажно-ориентированных процедур и других известных случаях использования КОП.

Любое дальнейшее изменение характеристик КОП, определенных в соответствии с разделом 8, следует обосновывать, официально утверждать и документировать.

8.2.2 Основные характеристики, необходимые для КОП

Следующие основные характеристики КОП следует определить точным и недвусмысленным образом:

- все технические термины, символы и графические элементы;
- глоссарий, определяющий смысл и использование каждого элемента формата;
- символы или рисунки, представляющие элементарные шаги КОП, а также ссылки между ними;
- правила обработки содержимого шагов КОП;
- правила распределения имен для вычисленных или внутренних переменных.

Примечание — Имена переменных помогают оператору понять тип и использование рассчитанной переменной;

- правила навигации между КОП, элементарными шагами, страницами или последовательностями КОП.

Элементы, такие как «шаги», «индикаторы», «блоки принятия решений», а также их комбинации, которые предназначены для общего использования, следует определить как повторно используемые элементы с набором параметров, которые необходимо указать.

Для процедур, которые были прерваны и повторно запущены, следует предусмотреть подтверждение того, что условия и допущения все еще действительны для продолжения выполнения.

8.2.3 Правила представления

Чтобы минимизировать интеллектуальную нагрузку на оператора и соответствовать общим требованиям, приведенным в 5.4.2, представление КОП следует спроектировать таким образом, чтобы:

- были четко определены местные действия;
- оператору предоставлялся обзор прерванных и выполняемых в настоящее время процедур;
- представление процедуры было согласовано со всеми КОП и соответствовало модели представления ЦСО;
- была минимизирована возможность ошибок оператора с использованием для управления АС как КОП, так и ЦСО;

- информация, необходимая для выполнения процедуры, считывалась с рабочей позиции оператора;
- всегда был представлен последний утвержденный и выпущенный вариант процедуры.

Исключения из приведенных требований должны быть обоснованы.

Чтобы свести к минимуму ошибки оператора, содержимое формата следует:

a) отображать идентификацию текущей процедуры и текущей последовательности в рамках этой процедуры;

b) четко определять выполненные шаги, активные шаги и возможные последующие шаги;

c) минимизировать количество обособленных действий для доступа к отображению требуемого формата;

d) облегчать взаимодействие между оператором и процедурой.

8.2.4 Компоновка формата отображения КОП

Компоновку формата отображения КОП следует проектировать так, чтобы:

- идентификация процедуры, то есть ее название и функциональное кодирование, а также цели функциональной процедуры были постоянно видны, как часть формата процедуры, и имели постоянное место в формате;
- распределение информации осуществлялось по одному и тому же методу во всех процедурах;
- разделение процедуры на последовательности выполнялось в соответствии с согласованными правилами;
- важность шагов отображалась наглядным образом;
- предупреждения, предостережения и другая информация, связанная с одним шагом, были видны всякий раз, когда отображается этот шаг.

Любые такие предупреждения, предостережения и информация должны быть представлены таким образом, чтобы их нужно было прочесть, например, используя всплывающие меню, которые должны быть подтверждены оператором, прежде чем оператор сможет начать выполнение определенного шага. Используемые для отображения, закрытия или запоминания информации, всплывающие окна в зависимости от контекста должны появляться в предопределенных частях форматов, они не должны скрывать слишком большую часть формата и должны быть легко переместимы из одного места в другое. Они не должны нарушать использование КОП, например путем пропуска или маскировки, или дублирования шагов или последовательностей, или путем блокировки форматов на экранах.

8.2.5 Требования к представлению отдельных элементов отображения

Правила представления отдельных элементов отображения заключаются в следующем:

- информацию и шаги действий следует представлять по-разному;
- диапазон принятия решений с их соответствующими выборами (например, «да» или «нет») следует представлять однородным вне зависимости от процедуры;
- если требуется ответ оператора, автоматические действия не следует продолжать без получения ответа оператора.

Всякий раз, когда форматы процедур содержат повторяющиеся информационные элементы, такие как набор компонентов АС, набор подобных действий и т. д., эти информационные элементы следует представлять в виде списков. Конструкция списков должна обеспечивать:

a) выделение списка из других частей процедуры;

b) четкое обозначение приоритетов пунктов;

c) наличие для всех списков заголовков;

d) привлечение к списку внимания оператора.

8.3 Выходная информация КОП

8.3.1 Общие положения

Информацию о системе КОП следует сделать доступной оператору, например, обозначение, версия, дата выпуска, номер страницы. Такую информацию следует отображать систематически либо по запросу оператора.

Все семейства КОП должны предоставлять указанную информацию для того, чтобы:

- оператор мог правильно использовать рекомендации КОП;
- оператор был полностью информирован об изменении состояния АС.

Сигнализация и сообщения, генерируемые процессом или происшествием на оборудовании, должны быть адаптированы к рабочей фазе процедуры, в которой они могут отображаться, и не должны вводить в заблуждение оператора или заставлять его сомневаться.

Сигнализация, генерируемая КОП, должна отображаться так же, как сигнализация, генерируемая событиями процесса или оборудования. При проектировании следует применять МЭК 62241.

8.3.2 Информация КОП, принадлежащей к семейству 1

КОП, принадлежащие к семейству 1, аналогичны бумажно-ориентированным процедурам, поскольку они указывают на контролируемые параметры процесса и оборудования, но не отображают никакой динамической информации о состоянии АС.

8.3.3 Информация КОП, принадлежащей к семейству 2

Чтобы обеспечить адекватное понимание операций, информация КОП, принадлежащих к семейству 2, должна включать представление состояния всех индикаторов и входов процесса и оборудования, которые:

- необходимы для понимания и выполнения рабочих стратегий;
- необходимы для понимания ситуации, состояния АС и отображаемых сообщений, относящихся к процедуре.

Качество информации КОП следует обеспечивать:

a) частотой обновления параметров, адаптированных к потребностям процедуры;

b) незамедлительным отображением информации о возможном конфликте между введенными оператором данными и полученными или вычисленными значениями параметров.

Информацию о перекрестных ссылках КОП следует сделать легкодоступной оператору. Шаги бумажно-ориентированной процедуры, связанные с перекрестной проверкой данных, следует переносить на решения по КОП.

Информацию о пригодности следует показывать пользователю. В более общем плане информацию о статусе следует сделать доступной, например: «доступен», «запрещен для тестирования», «запрещен для эксплуатации», «недоступен», «несовместим с другими входами».

Применение политики проектирования приведет к принятию решений по отображению:

1) обобщенной информации;

2) информации, относящейся к состоянию АС;

3) информации, выбранной оператором.

Примечание — Для отображения указанных видов информации может потребоваться, чтобы системой КОП вычислялись дополнительные значения на основе входных данных или других дополнительных значений. Это может также привести к необходимости дополнять исходную информацию указанием степени ее достоверности, которая, например, может являться результатом перекрестной проверки различных значений.

Дополнительные расчетные значения следует сделать:

- доступными операторам (как и любые другие значения полученных сигналов);
- легко идентифицируемыми при отображении на УВО, например, с помощью специальной кодировки или определенного цвета.

Информационные характеристики КОП могут различаться в зависимости от типов процедур, перечисленных в 5.2, при условии, что форматы ЧМИ остаются согласованными.

Политика предоставления рекомендаций может требовать выявления возможных расхождений между действиями операторов и предлагаемым решением.

8.3.4 Информация КОП, принадлежащей к семейству 3

Для автоматического управления АС или обеспечения надлежащей возможности предоставления рекомендаций все виды информации из КОП, принадлежащих к семейству 2, обязательные и дополнительные, должны предоставляться КОП, принадлежащих к семейству 3.

8.4 Навигация

8.4.1 Общие положения

Возможности навигации следует реализовать в соответствии с политикой ЧМИ, предусмотренной для ЦСО и КОП.

8.4.2 Навигация в КОП семейства 1

В навигацию для КОП семейства 1 следует включить варианты, обеспечивающие переход непосредственно на страницы, просмотр страниц и поиск терминов на страницах.

Расширенные возможности могут быть реализованы:

- для получения страниц или последовательностей, таких как закладки, индексы, оглавления;
- отображения контекстной информации, такой как всплывающие окна или миниатюры;

- стандартизации подпрограмм, например, отражающих процессы теплопередачи по трубопроводам или процессы вывода стержней.

Могут быть предоставлены ссылки на соответствующие процедуры, например, процедуры технической спецификации или процедуры реагирования на сигнализацию. Эти процедуры не следует путать с отдельными шагами.

Если несколько процедур одновременно активны, следует предоставить оператору возможность перехода из одной процедуры в другую, даже если последняя в настоящее время не отображается.

8.4.3 Навигация в компьютерно-ориентированной процедуре семейства 2 или 3

Особенности навигации для КОП, принадлежащих к семейству 2 или 3, расширяются по сравнению с особенностями навигации для КОП, принадлежащих к семейству 1, применительно к последовательностям и отдельным шагам внутри процедуры.

Кроме того, процедуры могут быть исследованы в соответствии с типами шагов, например, чтобы найти следующее решение, касающееся давления первого контура.

Следует предоставить возможность отслеживать путь, по которому следовал оператор до достижения текущей ситуации. В отслеживаемый путь следует включать все процедуры, которые взаимодействовали между собой. Как правило, такому отслеживанию следует запускаться автоматически для КОП, связанных с работой в аварийных условиях. Форматы, содержащие историю действий оператора, не следует путать с форматами, связанными с текущей ситуацией.

8.5 Рекомендации КОП

8.5.1 Общие положения

Рекомендации КОП опираются на те же положения, что и бумажно-ориентированные процедуры, но распространяются на политику компьютеризации. Эти рекомендации варьируются от предоставления элементарной информации о процессе до предоставления расширенной помощи:

- для выбора, определения доступности и возможности исполнения КОП;
- диагностики;
- принятия решения.

Примечание — Детали рекомендаций различаются, частично из-за характера процедур, например, процедуры аварийного реагирования предоставляют больше указаний, чем обычные эксплуатационных процедуры, и частично из-за ожидаемой осведомленности оператора, которая основывается на политике обучения.

8.5.2 Выбор КОП, доступность и исполнение

КОП, как и бумажно-ориентированной процедуре, следует быть отсортированной и доступной в зависимости от ее характера, а именно:

- если намерение заключается в изменении состояния АС, например, при запуске, отключениях;
- в ответ на сигнализацию, сигналы процесса или сигналы оборудования;
- периодически, например, как процедуры наблюдения, которые вводятся при каждой передаче смены.

Учитывая применение КОП, события на АС или периодические события могут автоматически сигнализировать о том, к какому типу КОП необходимо получить доступ. Специальная процедура может быть рекомендована или автоматически выбрана.

Доступ к необходимой процедуре следует сделать как можно более простым, т. е. следует избегать слишком сложного пути выбора.

КОП также может позволить оператору автоматически контролировать параметры процесса или оборудования и определять пороговые значения этих параметров. Когда параметром достигнуто пороговое значение, может быть отправлен сигнал, и при условии, что ни необходимая информация, ни необходимые условия и предостережения не будут исключены, соответствующий шаг КОП может быть напрямую доступен и отображен.

Следует оставлять КОП доступной вручную, а инициирующее событие следует отображать по запросу оператора.

8.5.3 Помощь при диагностике

Особые ситуации на АС, четко определенные проектировщиком, например авария или любое событие, обозначенное отклонениями параметров безопасности, могут быть идентифицированы во время работы и сигнализированы. Диагностику состояния АС следует представлять в КОП, как набор шагов и решений по контролю, которые приведут к возможным дальнейшим расследованиям и рекомендациям по корректирующим действиям.

Оператор должен нести ответственность за результаты диагностики и доступ к предлагаемой процедуре.

Подробную информацию о диагнозе следует отображать по запросу оператора.

8.5.4 Помощь при принятии решений

Помощь в решении следует ограничить шагами, требующимися для принятия решения. Информация, такая как входные данные, сигнализация, трендовые кривые, вычисленные значения параметров и т. д., которые затем могут быть необходимы, должна быть доступна и легко отображаться.

Оператор должен нести ответственность за любое принятое решение.

Для усиления помощи в принятии решений КОП следует сигнализировать о том, что:

- предлагаемая процедура была начата;
- каждый шаг был подтвержден оператором;
- каждый шаг получил положительный сигнал обратной связи;
- выбор оператора соответствует предложению в случае диапазона решений;
- достигнуты цели рассматриваемой процедуры.

Сигналы обратной связи от исполнительных механизмов и датчиков могут использоваться, например, в сложных ситуациях, чтобы убедиться, что действия оператора соответствуют шагам КОП. Если выбран этот вариант, то должны быть сообщены несоответствия, но не должны существовать препятствия действиям оператора.

Примечание — Основными типами обратных связей являются:

- обратная связь от контроллера для подтверждения состояния АС или оборудования;
- обратная связь для подтверждения состояния контроллера, особенно блокировок безопасности;
- обратная связь для подтверждения состояния аппаратного переключателя панели или аварийного состояния;
- обратная связь для подтверждения статуса других индикаций или соответствующих разрешающих функций, доступных оператору;
- обратная связь для подтверждения внутренних состояний КОП, контроллера, аварийного состояния, других систем отображения и т. д.

8.5.5 Компьютеризация рекомендаций КОП

Каким бы ни был тип и уровень рекомендаций, КОП должны быть компьютеризированы так, чтобы:

- они отображали все необходимые элементы, позволяющие оператору понимать и контролировать АС в любой ситуации;
- они обеспечивали обоснованный и уместный уровень информации для того, чтобы оператор мог ее усвоить, а не отвлекаться или озадачиваться из-за недостатка поддержки;
- они оставляли оператора ответственным за свои действия, либо попросив оператора подтвердить предложения, либо попросив его выбрать курс действий, отличный от предлагаемых действий;
- они предоставляли по запросу оператора отображение обоснований предложений;
- они различали предложения и шаги или информацию;
- они не скрывали важную часть отображаемого формата менее важной информацией;
- блокировали обновления информации, например из-за сбоя оборудования, для облегчения ее обнаружения.

Помощь следует отображать по запросу оператора, и оператору следует дать возможность отключать ее в любое время.

Операторам следует предоставлять возможность временно отключать отображение предупреждающих сообщений, которые могут быть выданы с помощью вспомогательных функций. Должна отсутствовать возможность блокировать процессы сигнализации.

Может быть предложено использование других процедур, и могут быть предоставлены ссылки на них.

8.6 Процедурно-ориентированная автоматизация

8.6.1 Общие положения

КОП может быть спроектирована таким образом, чтобы автоматически выполнять некоторые рабочие задачи под контролем оператора.

8.6.2 Взаимодействие между операторами и процедурно-ориентированной автоматизацией

Распределение задач между операторами и цифровыми системами должно быть основано на МЭК 61839 и, возможно, обосновано критериями, относящимися к конкретному проекту. КОП должна быть спроектирована так, чтобы:

- информировать оператора о важности для безопасности выполняемой последовательности;
- постоянно информировать оператора о том, что выполняется;
- позволять оператору осуществлять переход на ручное управление в любое время;
- поддерживать оператора соответствующими подтверждениями, например, путем проверки значений параметров, до выполнения автоматических последовательностей;
- обеспечить адекватную автоматическую проверку (или потребовать ручную проверку оператором) состояния АС или оборудования, чтобы обеспечить то, что запрошенные последовательности разрешены и безопасны в это время и в текущем состоянии АС;
- информировать оператора о его действиях, зависящих от времени, например, с помощью таймеров задач;
- информировать оператора о состоянии КОП, например, «только чтение», «ручное выполнение», «автоматическое выполнение» и т. д.;
- включить после надлежащей проверки оператором значений параметров автоматическое выполнение последовательности после ее ручного прерывания;
- предупредить оператора о случайном событии, которое может помешать правильной обработке процедуры. Следует предоставить оператору способы показать причину появления такого предупреждения.

Следует изучить дополнительные возможности системы, например, КОП может позволять операторам выбирать части КОП, которые по желанию операторов могут выполняться автоматически.

8.6.3 Проектирование КОП для управления атомной станцией

КОП, предназначенная для управления АС в целом, должна быть спроектирована с учетом того, что:

- эта КОП проектируется только в случае, если существуют переопределенные оператором автоматические последовательности, которые не начинаются и не заканчиваются в рамках одной и той же процедуры;
- приоритет между управляющими действиями, запущенными из КОП, и управляющими действиями, запущенными вручную или из ЦСО, устанавливается в соответствии с правилами приоритета для ручных и автоматических функций;
- последовательности заданы и фиксированы. Они могут включать в себя точки удержания, требующие подтверждения оператора;
- вначале проверяется доступность оборудования или схемы, когда это требуется для обработки шага;
- автоматические действия и ручные команды операторов записываются с отметкой времени и архивируются.

Для последовательностей, важных для безопасности, следует предоставлять соответствующие подтверждения обратной связи (или, альтернативно, запрос на подтверждение оператора вручную) соответствующего состояния оборудования или АС до начала выполнения автоматизированных управляющих последовательностей, а также для подтверждения успешного завершения управляющих воздействий. Отклонения следует регистрировать и сигнализацию о них (при необходимости) направлять оператору.

Если некоторые процедуры не могут быть отображены УВО, либо потому, что их слишком много, либо из-за ограниченной емкости экрана УВО, следует предусмотреть положения, позволяющие им:

a) подавать сигнал или отправлять сигнализацию для значимых событий;

b) давать периодические признаки жизни, чтобы показать, что процедуры все еще обрабатываются. С другой стороны, некоторые процедуры могут быть автоматически остановлены или заморожены в зависимости от спецификации проектировщика;

c) отображаться по запросу оператора.

На этапе проектирования следует проводить анализ для доказательства того, что работа не подвергается риску, даже если некоторые находящиеся в работе процедуры не отображаются постоянно на УВО.

Если функция автоматизации КОП, принадлежащей к семейству 3, доступна из более чем одного ЧМИ, то следует реализовать соответствующие предупреждения, блокировки и передачи обслуживания, чтобы предотвратить возможность отображения этой КОП, имеющей активное управление одной и той же последовательностью (или, возможно, интерферирующей последовательностью), на нескольких УВО одновременно.

Примечание — Это минимизирует количество и сложность возможных режимов отказа между УВО КОП и другими УВО и (или) контроллерами. Это также уменьшает вероятность ошибки координации оператора при таких обстоятельствах.

8.7 Другие объекты КОП

Для каждого типа процедуры следует учитывать различные варианты:

- может быть предусмотрен вариант включения заметок оператора в КОП. Это соответствует тому, что операторы используют для бумажных процедур. Данные примечания могут использоваться, например, для указания необходимости временного отклонения от КОП в конкретных условиях, которые должны быть детализированы;
- оператору может быть предоставлена возможность выбора соответствующих параметров процесса, подлежащих контролю;
- могут предоставляться возможности отслеживания и архивирования. В случае редких ситуаций на АС может быть принято решение регистрации и архивирования управления ситуацией с помощью КОП, чтобы проанализировать эту ситуацию позже;
- регистрация действий. Следует организовать автоматическую запись действий, предпринятых в ответ на шаги КОП;
- может быть предусмотрен вариант адаптации рекомендаций к ситуации, чтобы позволить операторам выбирать уровень рекомендаций, адаптированный к их навыкам в отношении конкретных КОП или последовательностей.

8.8 Выходная документация

Детальный проект должен быть документирован в соответствии с требованиями МЭК 61513, МЭК 60880 и МЭК 62138, если это применимо, а также в соответствии с категорией безопасности функций, выполняемых КОП.

Все варианты, определенные в соответствии с разделом 8, следует задокументировать в соответствующих документах, в том числе:

- краткое изложение вариантов и обоснований для фаз проектирования, разработки, проверки или лицензирования;
- резюме для операторов, которое следует понимать как напоминание, легко используемое при нарушении нормальной эксплуатации АС;
- подробный документ, который будет использоваться в качестве ориентира при проектировании и обслуживании КОП.

Указанная документация должна обновляться вместе с дальнейшими изменениями в КОП для обеспечения ее соответствия.

9 Жизненный цикл КОП

9.1 Общие положения

Раздел 9 устанавливает требования и рекомендации для всего жизненного цикла КОП от организации проектирования до эксплуатации КОП и обучения операторов, при этом особое внимание уделяется верификации и валидации КОП.

9.2 Организация проектирования

Проект компьютеризации процедур объединяет ЧМИ, рабочие стратегии и аспекты программной инженерии. Организационные аспекты ЧМИ и рабочие стратегии такие же, как и для бумажно-ориентированных процедур. Если система КОП важна для безопасности, то программные аспекты следует устанавливать на основе МЭК 61513, с учетом того, что система КОП похожа на любую другую разработку программного обеспечения и относится к классифицированным по безопасности КОП или к КОП, не классифицированным по безопасности.

Первая задача состоит в том, чтобы организовать команду проекта со всеми необходимыми компетенциями и определить комитет по принятию решений.

Основываясь на политике КОП, команде проекта следует взять на себя ответственность:

- за проектирование процедур;

- разработку процедур;
- верификацию и валидацию процедур;
- рассмотрение и утверждение процедур;
- пересмотр процедур.

Инжиниринговые инструментальные средства следует использовать для обеспечения качества и прослеживаемости разработки в течение типичных этапов жизненного цикла процедуры. На всех этапах разработки проекта компьютеризация имеет потенциальную выгоду и может облегчить работу, которая должна быть выполнена, особенно при отслеживании разработки и архивировании различных версий.

Следует организовывать официальные обзоры, разнообразные адресные рекомендации и архивирование выводов.

9.3 Проектная группа

Для того чтобы проектировать, разрабатывать, тестировать и особенно проверять КОП, следует объединить различные группы участников:

- проектировщики процедур;
- специалисты по человеческому фактору;
- компьютерные специалисты, когда это необходимо;
- все категории конечных пользователей, то есть руководители, операторы и, возможно, местные операторы.

Опыт и потребности операторов, а также гибкость и емкость МВО следует учитывать при проектировании внешнего вида КОП, чтобы сделать КОП более легко усваиваемой оператором.

Этих экспертов следует интегрировать в команду, экспертам следует работать вместе с самого начала проекта.

9.4 Детальное проектирование КОП и обеспечение качества выполнения

В зависимости от класса безопасности системы КОП должны применяться подробные требования к проектированию и внедрению, изложенные в МЭК 61513, МЭК 60880, МЭК 62138 и МЭК 61772. В случае если система КОП не относится к категории безопасности, могут использоваться требования к системам третьего класса безопасности.

Каким бы ни был его класс безопасности, система обработки КОП должна быть самоконтролируемая, а обнаруженные сбои должны сигнализироваться.

Программа обеспечения качества, с учетом классификации безопасности КОП, должна быть разработана для проверки того, что:

- требования разделов 6—8 учтены правильно;
- прослеживаемость разработки гарантирована;
- регулярно выполняется архивирование разрабатываемого программного обеспечения, а резервные файлы доступны и надежны;
- охват тестами является оптимальным, обеспечиваются прослеживаемость и архивирование результатов испытаний;
- версии КОП управляются правильно.

9.5 Программа верификации и валидации

Требования к программе верификации и валидации, приведенные в МЭК 61513, МЭК 60880, МЭК 62138 и МЭК 61772, должны применяться в зависимости от класса безопасности системы КОП. В случае если система КОП не относится к категории безопасности, могут использоваться требования к системам третьего класса безопасности.

Верификация и валидация (ВиВ) КОП состоит:

- из ВиВ системы КОП, ее аппаратной части и программного обеспечения, в соответствии с ее классификацией безопасности;
- технической или статической верификации КОП (см. 9.6.2).

Верификация КОП должна учитывать как соответствие форматов визуального отображения спецификациям ЧМИ, так и технические аспекты анимации процедур;

- функциональной и эргономической валидации КОП с использованием полномасштабного тренажера и участием операторов (см. 9.6.3).

Первые два мероприятия могут быть запланированы на всем этапе разработки, тогда как последнее следует выполнять с использованием комплексных и когерентных подмножеств КОП или с использованием полного набора КОП.

В начале проектирования должна быть создана программа верификации и валидации для обеспечения того, чтобы на протяжении всего этапа разработки выполнялись требования разделов 6—8, чтобы определить необходимые ресурсы, то есть человеческие и цифровые средства, и подготовить окончательную верификацию и валидацию готового продукта. Также следует подготовить надлежащие положения о документировании.

9.6 Верификация и валидация КОП

9.6.1 Общие положения

В 9.6 рассматривается системная верификация и валидация технических и эргономических аспектов КОП, предполагая, что уже выполнена верификация детального проекта в соответствии с требованиями безопасности и качества, включая программные аспекты модулей КОП и тестирование на уровне модулей.

Организация качества должна гарантировать, что любой обнаруженный отказ будет исправлен надлежащим образом и соответствующая документация будет соответствующим образом откорректирована.

Четкость представления и простоту использования реализации вариантов, определенных в разделе 6, следует оценивать на раннем этапе проекта, чтобы не подвергаться сомнению при разработке КОП.

Функциональные сценарии должны быть спроектированы для представления значительных событий процесса или рабочих ситуаций.

Эквивалентность КОП и бумажных процедур должна быть подтверждена.

Примечания

1 Функциональные сценарии являются генеральными планами по валидации бумажно-ориентированных или компьютерно-ориентированных процедур. К сожалению, невозможно продемонстрировать, что они исчерпывающе описывают все ситуации на АС и что они тщательно спроектированы.

2 Рассмотрение дополнительных типов сценариев валидации будет необходимо для КОП (т. е. в дополнение к бумажно-ориентированным процедурам) для проверки событий, возникающих из-за недостатков (и последующих отказов) в рамках реализации КОП.

9.6.2 Техническая верификация КОП

Верификацию КОП следует направить на обнаружение ошибочного применения характеристик, описанных в 8.2, таких как:

- использование неопределенных символов, слов, графиков и т. д.;
- несоответствия между именами переменных и отображаемой информацией;
- несоответствия между текстом шага и рекомендациями;
- несоответствия между текстом шага и связанной с ним командой.

Верификацию следует направить на обнаружение ошибок в проекте или программировании процедур, которые могут препятствовать достижению цели безопасности или эксплуатации, например:

a) циклы процедур;

b) взаимоблокировки: процедура А ожидает информацию из процедуры В, в то время как процедура В ожидает информацию из процедуры А;

c) открытые или неправильные ссылки на страницы или шаги.

Положения по верификации следует принимать таким образом, чтобы техническая верификация КОП:

1) являлась столь же исчерпывающей, насколько это технически возможно и разумно;

2) опиралась на методы и инструменты, которые сводят к минимуму неоднозначные интерпретации операторов;

3) публиковала результаты аудита;

4) прослеживалась и легко анализировалась;

5) облегчала регрессионные тесты.

Чтобы обнаружить как возможные ошибки программирования, так и операционные ошибки, следует рассмотреть возможность автоматической обработки всех или выбранных процедур для прогнозирования заранее определенных сценариев, вычисленных симулятором процесса. Эти сценарии, в том

числе учитывающие аномальные ситуации на АС, предусмотрены для того, чтобы активизировать как можно больше функций КОП.

9.6.3 Функциональная и эргономическая валидация

Валидацию КОП следует выполнять так же, как и для бумажно-ориентированных процедур. Валидацию следует завершить в учебном БПУ, являющемся представлением реального БПУ, с применением реальных КОП и ЦСО, а также с возможностью адекватного подражания условиям и сценариям АС, включая условия нарушений, аварийные ситуации и условия аварии, в случае необходимости, для стимулирования и подтверждения реакции тестируемой КОП.

Операторам БПУ, имеющим соответствующую квалификацию и опыт работы, следует участвовать в обзоре и принятии плана тестирования для любых КОП, связанных с безопасностью.

Операторы БПУ, имеющие соответствующую квалификацию и опыт работы, должны участвовать в проведении фактического теста на проверку безопасности КОП, связанной с безопасностью.

Функциональную и эргономическую валидацию следует направить на то, чтобы:

- функциональное распределение задач между операторами и машинами было правильным и эффективным;
- оператор мог правильно понимать и применять КОП;
- КОП помогала оператору достичь ожидаемых целей, даже в случае аномальных ситуаций;
- ошибки рабочей стратегии не остались необнаруженными;
- КОП повышала надежность действий оператора и снижала риск того, что оператор не будет соблюдать технические спецификации;
- у операторов в любое время было хорошее представление о процессе и его прогрессировании в процедурах;
- была правильная координация команды операторов;
- операторы могли отслеживать и обнаруживать любые отказы в системе КОП;
- операторы могли переключаться от КОП и системы КОП до набора резервных процедур и обратно;
- внешний вид КОП был совместим с внешним видом, реализованным в ЦСО.

Конкретные проблемы компьютеризации, которые могут возникнуть во время валидации, должны оцениваться следующим образом:

a) навигация между страницами.

Операторы могут с трудом понять, какую часть стратегии они применяют, и планировать свои последующие действия путем «листания» компьютеризированных страниц;

b) «туннельный эффект».

Оператор может стать неспособным думать самостоятельно, независимо от причины. Например, оператор, возможно, потерял понимание стратегии и применяет КОП механически, или для правильного использования КОП требуется слишком большая концентрация внимания, чтобы оператор понимал ее содержимое;

c) абстрактное мышление оператора.

Оператор должен полностью и легко понимать состояние АС и последствия действий, предложенных КОП;

d) связь между членами оперативного персонала и, возможно, с сотрудниками, не входящими в состав оперативного персонала.

Поведение КОП семейства 2 или 3 следует регистрировать во время работы сценария и анализировать функциональной группой специалистов на предмет согласованности между ожидаемыми действиями и действиями, выработанными имитатором КОП.

Примечание — Запись поведения КОП позволяет сравнивать различные рабочие стратегии, чтобы выбрать лучшую. Также полезно создать ссылочный файл, который можно будет использовать при тестировании будущих версий КОП.

9.6.4 Выходная документация

Требования и результаты системы ВиВ должны быть документированы в соответствии с требованиями МЭК 61513, МЭК 60880 и МЭК 62138, если это применимо, и в соответствии с категорией безопасности функций, реализуемых КОП.

Они, как правило, потребуются для обеспечения выдачи или продления лицензии на эксплуатацию.

9.7 Внедрение КОП на АС

КОП обычно реализуется как прикладное программное обеспечение, выполняемое в виде приложения, независимого от системного программного обеспечения. Следующие инструкции относятся к развертыванию этого прикладного программного обеспечения. Модификация системного программного обеспечения системы КОП обычно подразумевает дополнительные ограничения, которые здесь не представлены.

КОП должен быть развернут в когерентных и хорошо идентифицированных комплектах. Комплект может охватывать несколько типов процедур, которые являются взаимозависимыми.

Каждый комплект должен быть развернут в интерактивном режиме одним пакетом и без воздействия на работу АС. Процесс развертывания следует выполнить высокоавтоматизированным.

Для развертывания новой версии КОП должны быть выполнены следующие условия:

- были учтены результаты ВиВ;
- операторы были надлежащим образом подготовлены и проинформированы;
- при необходимости можно было восстановить старую версию КОП.

Чтобы упростить управление КОП на месте, следует указать некоторые конкретные соображения на этапах проектирования и разработки КОП, а именно:

a) применение средства управления в интерактивном режиме;

b) изменение версии КОП, которая должна:

1) легко развертываться;

2) не требовать изменения состояния АС;

3) не влиять на работу АС;

4) не влиять на ЦСО, если таковые имеются;

5) не влиять на операционную систему системы КОП;

c) архивирование старой версии КОП.

Для каждого развертывания должно быть обеспечено надлежащее качество, то есть подробная обработка и прослеживаемость. Следует избегать слишком частого развертывания недавно разработанной или пересмотренной КОП.

Перед развертыванием новой версии КОП все рабочие смены должны быть обучены ее использованию.

Неисправности системы КОП и ошибки КОП следует регистрировать и немедленно передавать организации, выполняющей сопровождение КОП.

9.8 Выходная документация

В качестве общего требования различные выходные данные, описанные в разделе 9, должны быть задокументированы в соответствии с требованиями МЭК 61513, МЭК 60880 и МЭК 62138, если это применимо, в соответствии с категорией безопасности функций, выполняемых КОП.

Требования МЭК 61513, МЭК 60880 и МЭК 62138 также следует использовать в соответствующих случаях для выпуска соответствующей документации в отношении:

- организации, созданной для проектирования, разработки и проверки КОП, а также организации одноразового обслуживания при эксплуатации КОП на основе требований 9.3 и 9.5;
- всех документов по программному обеспечению, а также документов, приведенных в 9.4 и 9.5;
- результатов ВиВ КОП (см. 9.6);
- документации, которую следует автоматизировать для облегчения тестов без регрессии в случае обновления КОП;
- развертывания КОП (см. 9.7).

Для обеспечения полноты и согласованности должен быть проведен обзор готовой документации, выпущенной согласно разделам 5—9.

Важно признать, что КОП необходимо будет модифицировать, поддерживать и, возможно, обновлять или заменять в будущем. Знания в области проектирования потребуются в разное время в течение жизненного цикла системы КОП. Важно документировать окончательные требования к проекту, включая критерии проектирования, ключевые допущения, обоснования и ограничения.

9.9 Обучение оперативного персонала

Основные цели и организация обучения КОП должны быть такими же, как и для бумажно-ориентированных процедур. Операторам, которые принимали участие в работе на этапах проверки КОП, следует оказать помощь в разработке учебной программы.

Обучение должно дополнительно научить оператора:

- эксплуатировать АС с применением КОП, независимо от того, для какой части АС они не были реализованы;
- периодически обеспечивать правильное функционирование системы КОП и выявлять потенциальные сбои;
- переходить к резервной системе процедур и резервным процедурам и управлять АС с их применением.

В случае использования бумажно-ориентированных процедур в качестве резерва обучение должно компенсировать отсутствие опыта их применения.

Следует принять меры для сбора отзывов об опыте и использования их в дальнейшем, например для обновления КОП и улучшения подготовки операторов. Накопление отзывов об опыте следует проводить с самого начала реализации проекта. Особое внимание следует обратить на первые месяцы работы с КОП.

9.10 Техническое обслуживание КОП и систем КОП

Для тестов, ремонта, установки запасных частей и переаттестации КОП и систем КОП должны быть предусмотрены инструкции по техническому обслуживанию аппаратной части, конфигурации и сопровождению программного обеспечения. Использование специальных инструментов должно быть задокументировано. МЭК 61513, МЭК 60880 и МЭК 62138 применяются в том случае, если система КОП классифицирована по безопасности.

Должны быть определены условия для соблюдения указанного времени ремонта.

Программа ВиВ, подробно описанная в 9.5, должна быть разработана и исполнена надлежащим образом при любом техническом обслуживании КОП или системы КОП. Оценку влияния изменений следует проводить для определения соответствующего охвата области проверки, включая регрессионные тесты, выполненные каждый раз для полной проверки изменений. Также требуется обучение операторов перед установкой и вводом в эксплуатацию изменений.

Обновление КОП должно быть подготовлено в автономном режиме, обновление КОП следует планировать так же, как и для бумажно-ориентированных процедур.

Для каждой реализации основных изменений следует предусмотреть качественные положения для раннего выявления ошибок. Операторы могут участвовать в верификации процедур.

Система КОП должна предоставлять в своем составе системное программное обеспечение, которое должно позволять загружать версии КОП без лишних изменений в работе самой системы КОП.

Хронологическая документация, необходимая для работы, ремонта и технического обслуживания системы КОП, если она автономна, должна регулярно заполняться. Записи операций и отчеты должны оцениваться с определенной периодичностью, чтобы идентифицировать и инициировать любые действия по техническому обслуживанию или модификации, которые могут потребоваться. Если КОП функционирует как часть ЦСО, то обслуживание последней должно выполняться с учетом наличия и надежности КОП.

Примечание — Точные требования к документации зависят от конкретной эксплуатирующей организации.

9.11 Обратная связь

Опыт применения КОП следует интегрировать в состав опыта эксплуатации АС, особенно для нового проекта или модификации существующего.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 60880	IDT	ГОСТ Р МЭК 60880—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категории А»
IEC 60964:2009	IDT	ГОСТ Р МЭК 60964—2012 «Атомные станции. Пункты управления. Проектирование»
IEC 60965:2016	—	*
IEC 61513	IDT	ГОСТ Р МЭК 61513—2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования»
IEC 61772:2009	—	*
IEC 61839	—	*
IEC 62138	IDT	ГОСТ Р МЭК 62138—2010 «Атомные электростанции. Системы контроля и управления, важные для безопасности. Программное обеспечение компьютерных систем, выполняющих функции категорий В и С»
IEC 62241:2004	—	*
ISO 11064 (all parts)	IDT	ГОСТ Р ИСО 11064 (все части) «Эргономическое проектирование центров управления»
ISO 11064-1	IDT	ГОСТ Р ИСО 11064-1—2015 «Эргономическое проектирование центров управления. Часть 1. Принципы проектирования центров управления»
ISO 11064-3	IDT	ГОСТ Р ИСО 11064-3—2015 «Эргономическое проектирование центров управления. Часть 3. Расположение зала управления»
ISO 11064-4	IDT	ГОСТ Р ИСО 11064-4—2015 «Эргономическое проектирование центров управления. Часть 4. Расположение и размеры рабочих мест»
ISO 11064-5	IDT	ГОСТ Р ИСО 11064-5—2015 «Эргономическое проектирование центров управления. Часть 5. Дисплеи и элементы управления»

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Государственной корпорации по атомной энергии «Росатом».

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

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 61226:2009, Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions (Атомные электростанции. Приборы и средства управления, важные для безопасности. Классификация приборов и функций управления)

IEC 61227, Nuclear power plants — Control rooms — Operator controls (Атомные электростанции. Пункты управления. Органы управления оператора)

IAEA Safety Guide SSG-39, Design of instrumentation and control systems for nuclear power plants (Проектирование систем контроля и управления для атомных электростанций)

IAEA SSR 2/1, Safety of Nuclear Power Plants: Design (Безопасность атомных электростанций: проектирование)

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 61226:2009, Nuclear power plants — Instrumentation and control important to safety — Classification of instrumentation and control functions (Атомные электростанции. Приборы и средства управления, важные для безопасности. Классификация приборов и функций управления)

IEC 61227, Nuclear power plants — Control rooms — Operator controls (Атомные электростанции. Пункты управления. Органы управления оператора)

УДК 621.311.49:006.354 ОКС 27.120

Ключевые слова: атомные станции, процедуры, компьютерно-ориентированные процедуры, управление, оператор

БЗ 5—2019/102

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 17.05.2019. Подписано в печать 29.05.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,21.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru