ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 60965 – 2012

АТОМНЫЕ СТАНЦИИ

Пункты управления

Резервные пункты управления для остановки реактора без доступа в блочный пункт управления

IEC 60965:2009

Nuclear power plants –

Control rooms –

Supplementary control points for reactor shutdown without access to the main control room

(IDT)

Настоящий проект стандарта не подлежит применению до его утверждения

Москва

Стандартинформ

2012

Предисловие

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

Сведения о стандарте

1 Подготовлен Открытым акционерным обществом «Всероссийский научно-исследовательский институт атомных электростанций» (ОАО «ВНИИАС») и Автономной некоммерческой организацией «Измерительно-информационные технологии» (АНО «Изинтех»)

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 № - ст

4 Настоящий стандарт идентичен международному стандарту МЭК 60965 «Атомные станции. Пункты управления. Резервные пункты управления для остановки реактора без доступа в блочный пункт управления» (IEC 60965:2009. «Nuclear power plants - Control rooms – Supplementary control points for reactor shutdown without access to the main control room»).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2011

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

Введение

a) Техническая справка, основные вопросы и организация стандарта

Стандарт МЭК 60965:1989 был разработан для обеспечения требованиями, предъявляемыми к проекту резервных пунктов атомных станций, предназначенных для остановки реактора без доступа в блочный пункт управления. Первая редакция стандарта МЭК 60965 весьма интенсивно использовалась в ядерной промышленности. Однако стало очевидным, что стандарт должен отражать современный технический прогресс, особенно в области программного обеспечения. Кроме того, появилась необходимость ясно и четко описать взаимосвязи между стандартом по блочным пунктам управления (т.е. МЭК 60964) и дополняющими его стандартами (т.е. МЭК 61227, МЭК 61771, МЭК 61772, МЭК 61839 и МЭК62241).

Настоящий стандарт МЭК посвящен функциональному проектированию резервных пунктов управления АС. Предполагается, что стандарт будет использоваться разработчиками АС, эксплуатирующими и надзорными организациями.

В конце стадии предварительного рассмотрения настоящей редакции стандарта были выявлены два момента, а именно: а) в стандарт должны быть включены требования, касающиеся регулярных испытаний резервных пунктов управления; б) необходимо выполнить теоретическую оценку времени, имеющегося для перехода из блочного в резервный пункт управления и ввода резервного пункта управления в эксплуатацию, исходя из возможной продолжительности нахождения в безопасном состоянии реактора, оставленного без контроля. Однако, так как эти вопросы не были формально подняты ни одним из национальных комитетов, они сформулированы только в настоящем введении для проработки в следующей редакции.

b) Положение дел с существующими стандартами в серии стандартов подкомитета МЭК ПК 45А

МЭК 60965 является документом третьего уровня подкомитета МЭК ПК 45А, охватывающим вопросы проектирования резервных пунктов управления.

МЭК 60965 необходимо читать в комплексе со стандартом МЭК 60964, описывающим проектирование блочного пункта управления (включая дополняющие его стандарты, упомянутые выше), который является соответствующим документам подкомитета МЭК ПК 45А, содержащими руководства по органам управления оператора, верификации и валидации проекта, применению дисплеев, функциональному анализу и распределению функций, функциям сигнализации и ее представлению.

Более подробная структура серии стандартов подкомитета МЭК ПК 45А приведена в пункте г) настоящего введения.

с) Рекомендации и ограничения применения данного стандарта

Основная цель стандарта состоит в изложении требований к функциональному проектированию, использование которых при проектировании резервных пунктов управления атомных станций необходимо для удовлетворения требований к безопасности.

Предполагается, что настоящий стандарт будет применяться к тем новым резервным пунктам управления, концептуальное проектирование которых начнется после опубликования данного документа. Рекомендации, содержащиеся в данном стандарте, могут быть использованы в ходе переоснащения, усовершенствования и модернизации.

В соответствии с параграфами 6.15-6.30 руководства МАГАТЭ NS-G-1.3, в данном стандарте были приведены особые рекомендации, касающиеся следующих вопросов:

определение предусмотренных проектом станции и блочного пункта управления условий, при которых предполагается использование резервных пунктов управления;

доступ персонала АС в резервные пункты управления в подобных опасных ситуациях;

обеспечение безопасной для персонала АС окружающей среды в резервных пунктах управления во время их использования;

обеспечение резервных пунктов управления информацией о состоянии критических функций реактора;

перевод функций управления и отображения из блочного пункта управления в резервные пункты управления при возникновении опасных ситуаций;

независимость и физическое разделение кабелей, используемых для резервных пунктов управления, от кабелей, используемых для блочного пункта управления;

обеспечение возможности приведения станции в безопасное остановленное состояние из резервных пунктов управления;

средства коммуникации между резервным пунктом управления и руководством станции.

Для того, чтобы данный стандарт оставался актуальным в течение последующих лет, наибольшее внимание в нем уделяется основным принципам, а не конкретным технологиям.

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

Документом верхнего уровня серии стандартов подкомитета МЭК ПК 45А является стандарт МЭК 61513. Он содержит общие требования к системам контроля и управления и к оборудованию, используемому для реализации функций, важных для безопасности АС. МЭК 61513 структурирует серию стандартов подкомитета МЭК ПК 45А.

МЭК 61513 содержит ссылки непосредственно на другие стандарты подкомитета МЭК ПК 45А, раскрывающие основные вопросы, связанные с классификацией функций и систем, их характеристиками, обеспечением независимости систем, защитой от отказов по общей причине, программным и техническим обеспечением автоматизированных систем и проектированием пунктов управления. Упомянутые стандарты, образующие второй уровень, должны рассматриваться совместно с МЭК 61513 в качестве комплекта взаимосогласованных документов.

На третьем уровне стандартов подкомитета МЭК ПК 45А находятся стандарты, непосредственно не упоминаемые в МЭК 61513, т.к. они касаются

конкретного оборудования, технических методик или определенной деятельности. Как правило, эти документы могут использоваться сами по себе, однако по общим вопросам в них содержится ссылка на стандарты второго уровня.

Четвертый уровень серии стандартов подкомитета МЭК ПК 45 образуют технические отчеты, не являющиеся нормативными документами.

В МЭК 61513 был использован тот же формат представления, что и в основном документе по безопасности МЭК 61508, посвященном общей структуре жизненного цикла безопасности и систем. Однако МЭК 61513 трактует общие требования стандартов МЭК 61508-1, МЭК 61508-2 и МЭК 61508-4 применительно к ядерной отрасли. Поэтому согласованность с МЭК 61513 облегчит соответствие требованиям стандарта МЭК 61508 в их толковании для ядерной промышленности. С этой точки зрения МЭК 60880 и МЭК 62138 соответствуют МЭК 61508-3 в части использования для ядерной отрасли.

В МЭК 61513 имеются ссылки на документы ISO и МАГАТЭ 50-C-QA (в настоящее время этот документ заменен на GS-R-3) по вопросам, связанным с обеспечением качества.

Серия стандартов подкомитета МЭК ПК 45А последовательно проводит в жизнь и детализирует принципы и основные аспекты безопасности, изложенные в правилах МАГАТЭ по безопасности АС и в серии руководств по безопасности МАГАТЭ, в частности в NS-R-1, устанавливающим требования по безопасности, закладываемые в проект АС, и в руководство по безопасности NS-G-1.3, касающимся систем контроля и управления, важных для безопасности АС. Термины и определения, используемые в стандартах ПК 45А, согласованы с теми, что используются в документах МАГАТЭ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

АТОМНЫЕ СТАНЦИИ
Пункты управления.
Резервные пункты управления для остановки реактора без доступа в блочный пункт управления

Nuclear power plants.
Control rooms.
Supplementary control points for reactor shutdown
without access to the main control room

Дата введения – 2011 – –

1 Область применения

Настоящий стандарт устанавливает требования к резервным пунктам управления (РПУ), обеспечивающим оперативный персонал атомной станции (АС) возможностью остановить реактор и поддерживать станцию в безопасном остановленном состоянии в случае невозможности дальнейшего управления функциями безопасности с блочного пункта управления (БПУ) или в случае невозможности использования самого БПУ или его оборудования.

Настоящий стандарт также устанавливает требования к определению функций, проектированию и организации человеко-машинного интерфейса и к процедурам, которые должны использоваться в соответствии с системным подходом для верификации и валидации функционального проекта РПУ.

Предполагается, что в процессе нормальной эксплуатации станции в РПУ, предназначенных для выполнения операций остановки за пределами БПУ, персонал отсутствует, за исключением периодических плановых проверок. Требования стандарта основаны на применении положений инженерной психологии в той части, в которой они применимы к человеко-машинному интерфейсу, используемому во время подобных периодических проверок и во время аварийных ситуаций.

Настоящий стандарт не распространяется на специальные центры аварийного реагирования (например, центры технической поддержки) или на установки, предназначенные для обращения с радиоактивными

отходами. Вопросы, связанные с более детальным проектированием, также выходят за рамки данного стандарта.

Настоящий стандарт следует принципам Требований МАГАТЭ NS-R-1 «Безопасность атомных электростанций: проектирование» и Руководства по безопасности МАГАТЭ NS-G-1.3 «Системы контроля и управления, важные для безопасности АС».

Целью данного стандарта является установление требований к функциональному проектированию, использование которых при проектировании РПУ АС необходимо для удовлетворения требований к безопасности.

Предполагается, что настоящий стандарт распространяется на РПУ, концептуальное проектирование которых начнется после его опубликования. При необходимости применения данного стандарта для действующих атомных станций или разработок, начатых до его опубликования, необходимо обратить особое внимание на то, насколько они совместимы с данным стандартом с точки зрения заложенных в них базовых проектных решений. Это касается, например, таких факторов, как совместимость РПУ и БПУ, использованного эргономического подхода, уровня автоматизации и информационных технологий.

2 Нормативные ссылки

Перечисленные ниже документы, на которые имеется ссылка в настоящем стандарте, являются обязательными при использовании настоящего стандарта. Ссылки, содержащие дату, касаются именно той редакции документа, которая соответствует этой дате. При отсутствии даты должна использоваться последняя редакция цитируемого документа (включая любые поправки).

МЭК 60709 Атомные станции. Системы контроля и управления, важные для безопасности. Обеспечение независимости (IEC 60709, Nuclear power plants – Instrumentation and control systems important to safety – Separation)

МЭК 60964 Атомные станции. Пункты управления. Проектирование (IEC 60964, Nuclear power plants – Control rooms – Design)

МЭК 61226 Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и

управления (IEC 61226, Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions)

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

МЭК 61771 Атомные станции. Блочный пункт управления. Верификация и валидация проекта (IEC 61771, Nuclear power plants – Main control room – Verification and validation of design)

МАГАТЭ NS-R-1 «Безопасность атомных электростанций: проектирование (IAEA NS-R-1:2000, Safety of nuclear power plants: Design)

МАГАТЭ NS-G-1.3:2002, Системы контроля и управления, важные для безопасности АС (IAEA NS-G-1.3:2002, Instrumentation and control systems important to safety in nuclear power plants, 2002)

3 Термины и определения

В рамках настоящего документа используются следующие термины и определения (прим. пер.: в порядке алфавита русского языка). Другие термины соответствуют общей терминологии, определенной в МЭК 60964, МЭК 65513, а также в документах программы стандартов по ядерной безопасности МАГАТЭ (NUSS), таких как руководство по безопасности NS-G-1.3 или словарь по безопасности.

3.1 **персонал пункта управления** (control room staff): Группа работников АС, находящихся в пункте управления и несущих ответственность за достижение целей эксплуатации АС, управляя ею с помощью человеко-машинного интерфейса. Обычно персонал пункта управления состоит из операторов, выполняющих супервизорные функции, и операторов, которые фактически контролируют АС и ее состояния и манипулируют органами управления, однако может также включать в себя работников и специалистов, допущенных в БПУ, например, во время длительно развивающихся событий.

[МЭК 60964, 3.3]

3.2 **местные посты (или средства) управления** (local control points (or facilities)): Посты (или средства), размещенные за пределами

основного пункта управления и предназначенные для осуществления управляющих действий местными операторами.

[МЭК 60964, 3.17]

3.3 **местные операторы** (local operators): Оперативный персонал, выполняющий задачи за пределами пункта управления.

[МЭК 60964, 3.18]

3.4 **оперативный персонал** (operating staff): Персонал АС, работающий посменно и осуществляющий эксплуатацию станции. Оперативный персонал состоит из персонала пункта управления, инженеров по эксплуатации и обслуживанию и др.

[МЭК 60964, 3.20]

3.5 **резервный пункт управления** (supplementary control point): Место, с которого может осуществляться ограниченное управление и/или контроль, направленные на обеспечение функций безопасности, определенных в результате анализа безопасности, в случае потери возможности выполнять эти задачи из блочного пункта управления. Резервный пункт управления может быть реализован в виде отдельного пункта управления, однако, во многих случаях он представляет собой набор панелей для управления и средств отображения информации в помещениях с коммутационной аппаратурой или других подобных помещениях.

4 Сокращения

АС Атомная станция

БПУ Блочный пункт управления

РПУ Резервный пункт управления

СКУ Система контроля и управления

5 Принципы проектирования

5.1 Общие положения

Параграф 6.75 руководства МАГАТЭ NS-R-1 устанавливает, что «предпочтительно в одном помещении (помещении резервного пункта управления), физически и электрически отделенном от основного пункта управления, должно быть также размещено достаточное количество

контрольно-измерительных приборов и оборудования для управления, с тем, чтобы можно было остановить реактор и поддерживать его в этом состоянии, отводить остаточное тепло и контролировать важнейшие параметры станции, если будет потеряна возможность осуществлять эти важнейшие функции безопасности из помещения основного пункта управления.

Параграфы 6.15-6.30 руководства МАГАТЭ NS-G-1.3 содержат требования, предъявляемые к резервным пунктам управления (в настоящем стандарте – РПУ), включающие в себя требования к:

– определению в проектных основах станции ситуаций, в которых возникает потребность в использовании РПУ (параграфы 6.17, 6.19, 6.20);

– расположению и конфигурированию РПУ для поддержки быстрого их использования (параграф 6.29);

– подходящему маршруту доступа в РПУ с индикацией опасностей и соответствующими защитными мерами на протяжении этого маршрута (параграфы 6.27, 6.28);

– предотвращению несанкционированного доступа или использования РПУ (параграф 6.21);

– невозможности одновременного влияния одного и того же постулированного исходного события на возможность управления функциями безопасности как с БПУ, так и с РПУ, а также к независимости электрических цепей в РПУ относительно аналогичных цепей в БПУ (параграфы 6.20, 6.23);

– определению приоритета управления между БПУ и РПУ и передаче управления от БПУ к РПУ (параграфы 6.18, 6.20, 6.24);

– ручному управлению с РПУ, выполняемому с помощью простых действий (параграф 6.22);

– максимально возможному использованию в РПУ средств отображения информации и органов управления, похожих на те, что установлены в БПУ (параграф 6.22);

– учету различия в назначении БПУ и РПУ (параграф 6.25);

– наличию соответствующих средств, обеспечивающих обитаемость и рабочее пространство для выполнения задач, в случае, если предусматривается длительное использование РПУ (параграф 6.30).

5.2 Основные цели

РПУ должен быть оснащен средствами, позволяющими остановить реактор, перевести станцию в состояние безопасного останова и поддерживать ее в этом состоянии без доступа в БПУ. Однако РПУ не предназначен для выполнения всех остальных функций контроля и управления станцией, которые обычно выполняются в БПУ. С учетом типа АС и детальных соображений безопасности РПУ может объединять оборудование, позволяющее преодолевать заранее определенный набор постулированных исходных событий.

РПУ необходим тогда, когда внутри БПУ складываются условия, выходящие за пределы проектных требований к его эксплуатации, и, следовательно, приводящие к тому, что БПУ становится больше непригодным. Возможными причинами могут быть пожар в помещении БПУ, чрезмерная задымленность или опасный состав воздуха в БПУ, сильные повреждения БПУ или его кабелей, приводящие к невозможности выполнения функций безопасности, большие повреждения помещения или существенный выход из строя оборудования БПУ.

Должны быть определены предусмотренные проектом постулированные исходные события и цепочки событий, для которых необходимо и запланировано использование РПУ. Для каждого выявленного события необходимо обоснованно оценить предполагаемую длительность использования РПУ.

Поскольку события, приводящие к непригодности БПУ, очень редки, ожидается, что анализ безопасности станции покажет, что частота наложения подобных событий на другие независимые события на станции является приемлемо низкой; в частности предполагается, что первый контур при этом не поврежден. Однако должное внимание необходимо уделять любой неисправности, которая может произойти как следствие остановки реактора, а также любым неисправностям на станции, находящейся в состоянии остановки, которые имеют достаточно высокую частоту наложения на ситуации использования РПУ. В частности, при проектировании РПУ необходимо учитывать возможную длительную непригодность БПУ вследствие пожара или других причин.

Критерии использования РПУ должны быть ясно прописаны в эксплуатационных процедурах.

За пределами БПУ должна иметься возможность определения, находится ли станция в полностью безопасном состоянии. Желательно, чтобы это делалось посредством РПУ.

С точки зрения эксплуатации (например, для упрощения действий или предотвращения ошибочного толкования) желательно иметь только один РПУ. Однако при этом необходимо учесть соблюдение требований безопасности, в частности требования к резервированию и независимости.

РПУ должен обладать способностью полноценного представления информации, включая представление на компьютерных дисплеях и систему сигнализации.

До выполнения требуемых действий должно иметься достаточное для доступа в РПУ время, а также достаточное оборудование для обеспечения необходимой коммуникации между всем оперативным персоналом, участвующим в этих действиях и с помещениями как на самой станции, так и вне нее. Соответствующие требования приводятся в подразделе 7.7.

Компоновка приборов и способ представления в РПУ должны обеспечивать оперативный персонал достаточной информацией для оценки состояния станции и контроля за остановкой (с последующим удержанием остановленного состояния) реактора, длительным процессом расхолаживания активной зоны реактора и удержанием любых радиоактивных веществ.

Состав технологических систем, управляемых с РПУ, может ограничиваться только теми, которые обеспечивают функции безопасности.

Для всего набора постулированных исходных событий и ситуаций, в которых невозможно использование БПУ, РПУ должен в достаточной мере обеспечивать управление функциями безопасности, позволяющими достичь и удерживать состояние безопасной остановки. Контроль и управление, обеспечиваемые в РПУ, должны охватывать состояние релевантных функций безопасности и управление запуском и остановкой их выполнения, а также состояние соответствующих основополагающих функций безопасности (см. МАГАТЭ NS-R-1, параграф 4.6).

Средства контроля за безопасностью в помещении, контроля доступа на станцию и пожарная сигнализация, обычно устанавливаемые в БПУ,

должны также быть предусмотрены и в независимом месте. Этим независимым местом может быть РПУ, либо помещение, не подверженное воздействию того события, которое обусловило причину использования РПУ.

Конструкция РПУ должна быть совместимой с конструкцией БПУ. Процесс выработки требований и проектирования необходимых органов управления и средств индикации для РПУ должен осуществляться в соответствии с требованиями МЭК 60964, кратко изложенными в разделе 6 настоящего стандарта.

5.3 Принципы безопасности

В проекте АС обычно устанавливаются внешние и внутренние опасные события, которые должны приниматься в расчет. Проект должен обеспечивать уверенность в том, что рассматриваемые события не способны одновременно привести к невыполнению или неэффективному выполнению функций БПУ и РПУ (а также местных постов управления), необходимых для безопасной остановки реактора, мониторинга безопасности остановки, контроля и управления критическими функциями безопасности.

Функции РПУ должны классифицироваться в соответствии с МЭК 61226, и при этом должным образом должны быть учтены критерии использования РПУ, описанные в подразделе 5.2.

Оборудование и системы должны проектироваться с глубиной резервирования, соответствующей их классу безопасности. Если системы безопасности, системы, не влияющие на безопасность, и резервированные системы размещены слишком близко друг к другу, то необходимо уделить внимание их физическому и функциональному разделению.

Принимая во внимание постулированные причины, при которых невозможно использовать функциональные возможности БПУ, функции РПУ (это касается и расположения РПУ) должны быть спроектированы так, чтобы даже в опасных аварийных состояниях к РПУ существовал доступ по безопасным маршрутам.

Проект должен обеспечивать персоналу пункта управления достаточное время, чтобы попасть в РПУ после того, как БПУ станет

непригоден. Действия и продолжительность автоматического выполнения функций безопасности без вмешательства человека с момента их запуска в БПУ и до момента ввода в действие РПУ должны быть достаточными для перемещения персонала. Оно должно также включать в себя время на доступ к органам управления и время на оценку состояния станции в РПУ.

Должны быть предусмотрены средства для отключения возможности управления с БПУ и перевода управления в РПУ. Эти средства должны быть отнесены к наивысшему классу безопасности из тех, к которым относятся функции безопасности, управление которыми становится невозможным с БПУ. Они должны быть гарантированно высоконадежными и, при необходимости, гарантированно отвечать критерию единичного отказа.

Средства перевода управления должны заблокировать органы управления БПУ для обеспечения уверенности, что пожар или другие повреждения, воздействующие на БПУ, не могут вызвать непреднамеренные управляющие действия. Эти средства также должны быть такими, чтобы избежать или минимизировать переходные процессы в управляемых параметрах во время перевода управления в любом направлении – как с БПУ в РПУ, так и с РПУ в БПУ.

Средства перевода управления могут находиться между БПУ и РПУ, в РПУ, либо в самом БПУ, если анализ показывает, что это не сможет привести к отказу при выполнении перевода управления или к отказу управления с РПУ. Если эти средства размещаются в БПУ, то должны быть также предусмотрены дополнительные возможности, реализуемые за пределами БПУ.

В РПУ должны иметься возможности определения состояния органов управления РПУ и БПУ.

Системы контроля и управления (СКУ) должны быть спроектированы так, чтобы не допустить одновременного управления технологическими системами с БПУ и РПУ.

СКУ должны быть спроектированы так, чтобы снизить вероятность воздействия ложных сигналов от элементов и систем БПУ на безопасность станции до приемлемого уровня. СКУ должны быть спроектированы так, чтобы снизить вероятность появления ложных сигналов от элементов РПУ, мешающих контролю и управлению станцией

с БПУ в нормальных и аварийных ситуациях до приемлемого уровня. Примером технических решений для достижения этих целей является использование автоматического ввода резерва, кодированных сигналов, оптически изолированных цепей.

Если РПУ введен в работу, то приоритет осуществляемых с него действий должен быть выше любых других действий ручного управления, за исключением случаев, когда управление должно осуществляться с местного поста управления.

В проекте РПУ должны быть предусмотрены меры для предотвращения несанкционированного доступа или использования. Для средств перевода управления также должны быть предусмотрены меры недопущения несанкционированного перевода управления с БПУ в РПУ и наоборот. Доступ в РПУ и любая попытка перевода управления в РПУ должны быть видны в БПУ.

РПУ должны быть спроектированы так, чтобы свести к минимуму ошибки оператора.

Проект должен предусматривать письменные инструкции, хранящиеся на РПУ, для работы:

– с технологическими системами и устройствами управления;

– с информационными и регистрирующими системами;

– с устройствами связи;

– с любым другим оборудованием, работа с которым осуществляется с РПУ.

Эксплуатационные процедуры, определяющие действия, предпринимаемые с РПУ, должны быть простыми и ясными.

Оборудование РПУ должно быть пригодно для работы в условиях окружающей среды, соответствующих тем предусмотренным проектом постулированным исходным событиям и последовательностям событий, для которых необходимо и запланировано использование РПУ.

Проектант должен предусмотреть регулярную проверку и осмотр оборудования РПУ на предмет удовлетворения требованиям проекта.

Проект должен позволять регулярную тренировку и отработку навыков работы с РПУ без нарушения работоспособности станции.

5.4 Принципы инженерной психологии

Для того, чтобы обеспечить оптимальное распределение функций, гарантирующих максимальное использование способностей оператора и системы, и достичь максимальной безопасности станции, в проекте должно быть уделено особое внимание принципам инженерной психологии и психофизиологическим характеристикам персонала в аварийных ситуациях, особенно в условиях, требующих быстрых действий, например, тех, которые должны быть выполнены за очень короткое время сразу после ввода в работу РПУ.

Если анализ безопасности показывает, что пребывание в РПУ может оказаться продолжительным, то должны быть приняты меры, обеспечивающие нормальные характеристики обитаемости (например, вентиляция). Такие меры не обязательно должны соответствовать требованиям, предъявляемым к аналогичным характеристикам БПУ.

Человеко-машинный интерфейс в РПУ должен строиться по аналогичным правилам, что и в БПУ.

При необходимости нескольких РПУ и/или местных постов управления, должно быть разработано четкое руководство по их использованию, укомплектованию персоналом и координации деятельности, охватывающей эти средства. Кроме того, должен быть проведен анализ человеческого фактора для определения того, какие из задач, подлежащих выполнению, могут быть решены надежно и в пределах времени, принятого в ходе анализа безопасности.

В случае, если в соответствии с требованиями избыточности и разделения (например, разделения двух аналогичных каналов капитальным противопожарным барьером) необходимо иметь более одного РПУ, они должны быть надлежащим образом скомпонованы с четкой идентификацией соответствующего им оборудования станции и не должны иметь зеркальную компоновку (см. МЭК 60964).

6 Процесс проектирования

Разработка технических требований к РПУ должна вестись на основе системного подхода. Данный процесс должен осуществляться параллельно с процессом проектирования БПУ и должен использовать аналогичные процедуры, критерии и методы. В частности, процесс

проектирования РПУ и документирования целей и правил должен содержать следующие стадии:

a) определение предусмотренных проектом сценариев, их целей и критериев отказа (см. подраздел 5.2);

b) разработка специфических для данной конкретной станции функций РПУ, согласующихся с общим проектом;

c) назначение основных функций оперативному персоналу и СКУ и распределение их по местам, с которых осуществляется управление;

d) классификация функций РПУ в соответствии с их важностью для безопасности и разработка соответствующих проектных и технических требований;

e) проектирование специфического для данной станции РПУ в соответствии с основными принципами, изложенными в разделе 5 МЭК 60964;

f) проведение верификации проекта (т.е. персонала, процедур и программы тренировки персонала РПУ) и валидации системы в целом (см. раздел 8);

g) разработка спецификации (технического задания) проекта на основе результатов предыдущих стадий (см. раздел 7);

h) выполнение детального проектирования и проведение окончательной верификации и валидации на станции после завершения (см. раздел 8).

Примечание – В ходе описанного выше процесса необходимо определить перечень систем, которые должны управляться с РПУ, их конфигурацию, а также перечень технологических параметров, которые должны контролироваться с РПУ.

7 Функциональное проектирование

7.1 Общие положения

Вследствие достаточно редкого использования и ограниченного числа задач, которые необходимо выполнять в РПУ, проект должен быть ориентирован на минимизацию количества оборудования, высокую

надежность выполнения функций и конфигурацию, доступную для легкого и быстрого понимания.

7.2 Человеческий фактор

Антропометрические данные, стереотипы населения, громкость звуковых сигналов, углы обзора и взгляда, а также выбор предпочтения между аналоговыми или цифровыми индикаторами должны быть согласованы с аналогичными решениями для БПУ.

Во избежание утомления при длительной работе и для обеспечения достаточной для выполнения задач видимости должен быть предусмотрен соответствующий уровень освещения.

Уровень шума не должен препятствовать отчетливому голосовому взаимодействию.

Если рабочие зоны предназначены для длительного использования, то должны быть предусмотрены соответствующие возможности для сидячей работы, ведения записей и размещения документации.

Если используется компьютеризованный способ представления информации или управления, то система должна работать в определенной степени, а лучше абсолютно так же, как и аналогичные средства управления и отображения информации в БПУ. Требования к надежности и условия окружающей среды могут потребовать использования другого оборудования, однако последовательности операций при этом должны быть похожими и совместимыми с аналогичным в БПУ.

7.3 Расположение и маршрут доступа

Выбор места расположения РПУ и проектирование его защиты должны быть выполнены таким образом, чтобы ни одна последовательность любых постулированных исходных событий не могла одновременно воздействовать на работоспособность РПУ и БПУ. Должны учитываться не только события, несущие непосредственную угрозу пунктам управления, но и события, которые могут воздействовать на обслуживающие системы, обеспечивающие работу РПУ и БПУ, соответственно.

Важной угрозой, при возникновении которой может потребоваться использование РПУ, является пожар. Должна быть выполнена оценка противопожарной защиты РПУ и маршрутов перемещения к ним людей, которая позволит убедиться в возможности доступа к месту расположения РПУ. Аналогичные оценки для всех обслуживающих систем, особенно систем обогрева, вентиляции и кондиционирования воздуха, маршрутов доступа и кабельных трасс должны быть сделаны и для других проектных ситуаций, в которых планируется использование РПУ. Оценка кабельных трасс должна показать независимость кабелей РПУ и БПУ.

Должна существовать возможность добраться до РПУ легко, безопасно и за отведенное время, несмотря на необходимость управления доступом. Эта должно быть возможно как из БПУ при его эвакуации, так и другими маршрутами в обход БПУ и других помещений, потенциально находящихся под воздействием угроз, вызвавших использование РПУ.

По маршруту следования от БПУ к РПУ должна быть обеспечена индикация потенциальных опасностей (например, пожара) и оборудование для соответствующих контрмер (например, дыхательные аппараты). Перед тем, как войти в РПУ оперативный персонал должен иметь возможность убедиться, что доступ к оборудованию безопасен.

Для уведомления остального оперативного персонала, особенно тех, кто во время покидания персоналом БПУ находился вне площадки АС или блока, должна быть предусмотрена четкая индикация того факта, что БПУ недоступен и непригоден для управления, вплоть до момента его возврата к работе.

7.4 Окружающая среда в РПУ

Условия окружающей среды в РПУ должны удовлетворять требованиям, вытекающим из анализа безопасности для нормальных или аварийных ситуаций, а также должны соответствовать государственным нормативам, включая план ликвидации чрезвычайных ситуаций.

Для предусмотренных проектом ситуаций, требующих использование РПУ, условия окружающей среды, определенные в результате анализа безопасности для того места, где будет размещен РПУ, не должны выходить за рамки тех, в которых возможно нормальное пребывание

человека без защитных приспособлений. Если потребность в РПУ может возникнуть в процессе запроектных или тяжелых аварий, включая действия по плану ликвидации чрезвычайных ситуаций, то для таких ситуаций также должно быть продемонстрировано, что место, в котором находится РПУ, пригодно для нормального пребывания человека.

Электрическая батарея, питающая системы аварийного освещения, должна быть постоянно работоспособной даже при отказе штатной системы питания. Аварийная система должна обеспечивать достаточное для выполнения задачи освещение в течение определенного промежутка времени, который должен отвечать требованиям плана ликвидации чрезвычайных ситуаций на станции.

7.5 Пространство и компоновка

РПУ должны иметь достаточное пространство для:

– размещения всего необходимого информационного и управляющего оборудования в хорошо структурированной компоновке;

– ведения и размещения на рабочих местах записей и процедур;

– хранения документации и инструкций;

– оборудования связи.

Для развития и модернизации в помещении РПУ должно быть предусмотрено резервное пространство.

Компоновка РПУ должна позволять немедленно начать его использование сразу по прибытии оперативного персонала в РПУ.

7.6 Информационное и управляющее оборудование

Для минимизации возможности ошибок человека вся информация, средства отображения информации, регистрирующее и управляющее оборудование должны быть организованы и структурированы в соответствии со своими функциями и приоритетом и должны работать так же, как и соответствующая часть интерфейса БПУ.

С целью более наглядного представления информации могут быть использованы мнемосхемы.

Принципы группирования, кодирование и маркировка оборудования РПУ должны подчиняться правилам, установленным для БПУ.

Как было указано в разд. 5.2, для функций безопасности должны быть предусмотрены средства отображения информации и органы управления. Глубина их резервирования должна выбираться в соответствии с их классом безопасности и проектными техническими требованиями.

Если единственный РПУ не обеспечивает необходимого резервирования внутри самого себя и это резервирование не достигается альтернативным РПУ, то для обеспечения необходимой индикации и управления в некоторых проектах АС возможно использование местных постов управления, что позволит смягчить последствия отказа и потери функциональности РПУ. В исключительных ситуациях, если это требуется по соображениям безопасности, такое инженерное решение может рассматриваться как альтернатива расширению средств РПУ. Для подобных исключительных ситуаций необходимо убедиться, что доступность соответствующего местного поста управления и время доступа к нему находятся в приемлемых пределах.

7.7 Системы связи

В РПУ должна быть обеспечена связь с руководством АС и центром технической поддержки при его наличии. В качестве связи должна использоваться обычная внутренняя телефонная связь и другие средства связи, такие как пейджинговая связь, определяемые в соответствии с требованиями станционного плана ликвидации чрезвычайных ситуаций. Надежные средства должны также обеспечивать связь РПУ с местными постами управления. В случае необходимости нескольких РПУ, между ними должна быть предусмотрена связь.

Должно быть предусмотрено резервное коммуникационное оборудование, использующее другие линии передачи данных и пригодное для решения эксплуатационных задач, управления процессами остановки и связи с кризисными центрами и другими службами аварийного реагирования. Подобное резервирование оборудования должно быть выполнено и для связи между РПУ и/или местными постами управления.

Штатное станционное оборудование связи может быть использовано для связи с БПУ в целях обучения, испытаний и др.

7.8 Прочее оборудование

Оборудование, которое должно быть размещено в РПУ или в непосредственной близости от него, включает в себя:

– медицинское оборудование для оказания первой медицинской помощи;

– оборудование, которое должно использоваться при локальных опасных ситуациях в соответствии со станционным планом ликвидации чрезвычайных ситуаций;

– документация по станционному плану ликвидации чрезвычайных ситуаций;

– портативные светильники, приборы радиационного контроля и противопожарное оборудование;

– защитная одежда и комплекты дыхательных аппаратов.

Эксплуатирующая организация должна разработать правила эксплуатации, которых необходимо придерживаться в случае возникновения в БПУ ситуаций, требующих использования РПУ. Эти правила должны охватывать управление доступом, безопасность помещения и действия в случае пожара. Средства для выполнения этих функций должны быть включены в конструкцию РПУ, если они не предусмотрены где-то еще, и должны быть доступны в течение всего периода, в течение которого БПУ остается непригодным для использования.

8 Верификация и валидация системы

Процесс верификации и валидации системы РПУ тесно связан с процессом верификации и валидации БПУ. Распределение функций между человеком и машиной для РПУ и БПУ должно выполняться параллельно.

Вследствие требований к упрощению задач и, следовательно, информации и действий, верификация и валидация РПУ могут быть упрощены по сравнению с БПУ. Верификация и валидация РПУ должны планироваться с использованием соответствующих критериев на основе требований МЭК 90964 и МЭК 61771.

В ходе окончательной оценки необходимо убедиться, что события, которые могут привести к потере управления функциями безопасности с БПУ, не повлияют на РПУ и его функциональные возможности. Во время испытаний на месте при вводе в эксплуатацию должна быть проверена надежность и работоспособность РПУ.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Т а б л и ц а ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
МЭК 60709	IDT	ГОСТ Р МЭК 60709-2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Разделение»
МЭК 60964	IDT	ГОСТ Р МЭК 60964-2011 «Атомные станции. Пункты управления. Проектирование
МЭК 61226	IDT	ГОСТ Р МЭК 61226-2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Классификация функций контроля и управления»
МЭК 61513	IDT	ГОСТ Р МЭК 61513-2011 «Атомные станции. Системы контроля и управления, важные для безопасности. Общие требования к системам»
МЭК 61771	IDT	ГОСТ Р МЭК 61771 «Атомные станции. Блочный пункт управления. Верификация и валидация проекта»
МАГАТЭ NS-R-1	–	*
МАГАТЭ NS-G-1.3:2002	–	*

* Текст документа на русском языке доступен на http://www.iaea.org/.

П р и м е ч а н и е – В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

– IDT – идентичные стандарты.

Библиография

[1] МЭК 60780 (IEC 60780) Атомные станции. Электрооборудование систем безопасности. Технические требования (Nuclear power plants – Electrical equipment of the safety system – Qualification)

[2] МЭК 60980 (IEC 60980) Рекомендуемые правила обеспечения сейсмической устойчивости электрооборудования систем безопасности атомных станций (Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations)

[3] МЭК 61227 (IEC 61227) Атомные станции. Пункты управления. Органы управления оператора (Nuclear power plants – Control rooms – Operator controls)

[4] МЭК 61772 (IEC 61772) Атомные станции. Блочный пункт управления. Применение дисплеев [Nuclear power plants – Main control room – Application of visual display units (VDU])

[5] МЭК 61839 (IEC 61839) Атомные станции. Проектирование пунктов управления. Функциональный анализ и распределение функций (Nuclear power plants – Design of control rooms – Functional analysis and assignments)

[6] МЭК 62241 (IEC 62241) Атомные станции. Блочный пункт управления. Функции и представление сигнализации (Nuclear power plants – Main control room – Alarm functions and presentation)

[7] ИСО 11064 (все части) (ISO 11064) Эргономическое проектирование центров управления (Ergonomic design of control centres)

УДК 621.311.25 ОКС 27.120.20

Ключевые слова: атомная станция; безопасность, контроль, управление, система, функция безопасности, блочный пункт управления, резервный пункт управления, остановка реактора

Председатель ЦГ1/ПК4/ТК322,
Руководитель Центра АСУТП
ОАО «ВНИИАЭС» Дурнев В.Н.

Секретарь ЦГ1/ПК4/ТК322,
Президент АНО "ИЗИНТЕХ" К.Н. Стась