Акционерное общество «Научно-технический центр «Диапром»

Утвержден
приказом 14/осн от 24 января 2020

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

ПРИКЛАДНОЕ ПРОГРАМНОЕ ОБЕСПЕЧЕНИЕ «DIAPROM PREDICT»

Стандарт предприятия

Жизненный цикл программного обеспечения

ДКНБ. ЖЦ-СТО-01

Количество листов – 22

Москва 2020

СОДЕРЖАНИЕ

1. Назначение и область применения

1.1 Назначение

1.2.1 Настоящая процедура вводится в целях:

– установления системы в организации и проведении работ по созданию программного обеспечения (ПО) автоматизированных систем (АС), разрабатываемых и выпускаемых Акционерным обществом «Научно-технический центр «Диапром» (АО "НТЦД", далее по тексту документа – Предприятие);

– разграничения полномочий и ответственности участников создания ПО АС;

– внедрения на Предприятии единых подходов к созданию ПО АС;

– повышения ответственности исполнителей за качество и сроки на той или иной стадии создания АС.

1.2.2 Данный стандарт распространяется на все ПО Предприятия находящееся на стадиях:

- анализа требований;
- проектирования;
- кодирования;
- тестирования;
- сопровождения.

1.2 Область применения

Настоящая процедура распространяется на подразделения, непосредственно участвующие в создании АС, как поставляемых Предприятием в рамках исполнения контрактных (договорных) отношений, так и вновь разрабатываемых в рамках работ по НИР (ОКР).

Положения, приведенные в данном документе, могут в последующем изменяться при проведении корректировок по результатам проверок или анализа со стороны руководства Предприятия, либо в связи с выходом новых нормативных документов.

Основанием для разработки настоящей процедуры качества являются:

- требования к производству продукции (раздел 8 стандарта ГОСТ Р ИСО 9001-2015);
- рекомендации, изложенные в документе МАГАТЭ GS-R-3.

2. Термины, определения, сокращения и условные обозначения

2.1 Термины и определения

Термин	Определение
автоматизированная система	система, реализующая информационную технологию выполнения установленных функций с помощью персонала и комплекса средств автоматизации
валидация программного обеспечения	тестирование и оценка интегрированной системы на соответствие спецификациям функциональных, эксплуатационных характеристик и интерфейсов, содержащихся в требованиях к АС
верификация	подтверждение экспертизой и предоставлением объективного свидетельства того, что результаты функционирования соответствуют целям и требованиям, определенным для такого функционирования
дефект	неисправность или ошибка в компоненте технического обеспечения, программного обеспечения или системы Дефекты подразделяются на случайные и систематические. Случайные дефекты возникают в результате деградации технического обеспечения и вызывают отказы в непредвиденные моменты времени. Систематические неисправности возникают вследствие ошибок в проекте (например, ошибок в программном обеспечении) и при одинаковых условиях систематически ведут к одинаковым отказам. Дефект (особенно дефект, связанный с проектированием) может оставаться незамеченным до тех пор, пока сохраняются условия, при которых он не отражается на выполнении функции, т.е. пока не произойдет отказ
защищенность	свойство компьютерной системы, обеспечивающее необходимую уверенность в том, что неуполномоченные лица и системы не смогут модифицировать программное обеспечение и его данные и не будут иметь доступ к функциям системы при том, что такая возможность будет обеспечена для уполномоченных лиц и систем
изделие	любой предмет или набор предметов производства, подлежащих изготовлению на предприятии, включая программное обеспечение
интеграция	последовательная сборка компонентов (оборудования и программного обеспечения) и их проверка внутри завершенной автоматизированной системы
качество	совокупность свойств изделия, определяющих степень его пригодности для использования по назначению. Требования по качеству определяется стандартами, техническим заданием и т.д.
комплекс оборудования	набор приборных и программных компонентов, которые могут работать совместно в одной или более определенных структурах (конфигурациях). Разработка специальной конфигурации для конкретного объекта и соответствующего программного обеспечения может поддерживаться программными средствами; обеспечивает набор стандартных операций (библиотеку прикладных функций), которые могут быть объединены, образуя специальное программное обеспечение. Комплекс оборудования может быть изделием определенного изготовителя или набором изделий, соединенных и настроенных поставщиком
компонент программного обеспечения	один из элементов, составляющих часть программного обеспечения

Термин	Определение
модификация программного обеспечения	изменение в уже согласованном документе (документах), ведущее к изменению программы. Модификация программного обеспечения может происходить на начальной стадии разработки (например, для устранения ошибок, найденных на более поздних стадиях разработки) либо уже после введения программного обеспечения в эксплуатацию
оборудование автоматизированной системы	изделия, составляющие измерительный канал автоматизированной системы или измерительную систему (датчики, согласующие устройства, преобразователи, регистраторы, блоки питания, и т.п.) или любая совокупность их
отказ	отклонение реального функционирования от запланированного
параметр	элемент данных, управляющий поведением автоматизированной системы и/или ее программного обеспечения, который может быть изменен операторами во время функционирования автоматизированной системы
погрешность	разность между рассчитанным, наблюдаемым или измеренным значением величины или параметра и истинным, установленным или теоретическим значением величины или параметра
программа	написанный человеком документ, который преобразуется в рабочую программу автоматизированными инструментальными программами. К программам можно причислить традиционные программы, написанные с помощью универсальных языков программирования
прикладная функция	функция автоматизированной системы по выполнению задачи, связанной с контролируемым процессом, а не с функционированием самой автоматизированной системы
прикладное программное обеспечение	часть программного обеспечения автоматизированной системы, которая обеспечивает выполнение прикладных функций
программное обеспечение	программы (т.е. наборы упорядоченных команд), данные, правила и любая связанная с этим документация, имеющая отношение к работе автоматизированной системы
программа и методика испытаний	документ, содержащий технические данные, подлежащие проверке при испытании изделия, а также порядок и методы их контроля
разработка программного обеспечения	этап жизненного цикла программного обеспечения, который осуществляется для создания программного обеспечения или программного продукта. Разработка охватывает все действия - от создания спецификации требований к программному обеспечению до его валидации и установки на объекте
режим функционирования	функциональное состояние элемента программы, которое обеспечивает определенный рабочий режим. К таким режимам могут относиться инициализация, нормальный (штатный) режим функционирования, режим неполного функционирования в случае частичного отказа технических средств системы или потери связи с внешними системами
системное программное обеспечение	часть программного обеспечения автоматизированной системы, созданная для конкретного компьютера или семейства оборудования
сложность	степень трудности понимания и верификации проекта, реализации или поведения системы или компонента
статический анализ	процесс оценки системы или компонента, базирующийся на ее (его) форме, структуре, содержании или документации

Термин	Определение
тестовое программное обеспечение	часть программного обеспечения автоматизированной системы, предназначенная для проверок функционирования автоматизированной системы или ее частей (прикладного программного обеспечения, оборудования) путем имитации реальных воздействий или входных данных
технические средства автоматизированной системы	см. оборудование автоматизированной системы
управление конфигурацией	порядок применения технической и административной директив и контроля с целью определения и документирования функциональных и физических характеристик сложного устройства, управления их изменением, ведения записей и отчетов об изменении в работе и настройке, а также проверки соответствия конкретным требованиям
эксплуатационные документы	документы, предназначенные для использования при эксплуатации программного обеспечения

2.2 Перечень принятых сокращений

АС – автоматизированная система
СУБД – система управления базами данных
КБД – конфигурационная база данных
ПО – программное обеспечение
СПО – системное программное обеспечение
ТПО – тестовое программное обеспечение
ППО – прикладное программное обеспечение
ОРД – организационно-распорядительная документация
СМК – система менеджмента качества
РД – руководящий документ
ТУ – технические условия
ТЗ – техническое задание
НИР – научно-исследовательские работы
ОКР – опытно-конструкторские работы
ПМ – программа и методика
ЕСКД – единая система конструкторской документации
ЕСПД – единая система программной документации
ЖЦ – жизненный цикл

3. Общие положения

3.1 ПО АС включает в себя (в общем случае) следующие типы ПО:

- системное ПО (СПО);
- прикладное ПО (ППО);
- конфигурационную базу данных (КБД);
- тестовое ПО (ТПО).

3.2 Разработка ПО проводится на основе технических требований, поступающих от Заказчика (как правило, в виде технического задания на АС) или, в случае внедрения в ПО новых функций, по решению руководства Предприятия.

3.3 В разработке СПО, ППО, КБД и ТПО участвуют отделы разработки программного обеспечения (РПО), отдел комплексной диагностики (КД) и системной инженерии (СИ).

3.4 Результаты разработки ПО находятся под контролем версий в репозитории Предприятия.

3.5 Каждый тип ПО находится в отдельном репозитории для обеспечения возможности более гибкого изменения комплектов ПО, поставляемых на конкретный объект внедрения (например, в случаях, когда требуется изменение только одного компонента ПО, независимого от других компонентов).

3.6 При поставке на объект внедрения каждый тип ПО, входящий в поставляемый комплект, оформляется в виде дистрибутивного носителя.

4. Обеспечение качества

4.1 Деятельность на этапах ЖЦ АС

Рисунок 1 иллюстрирует типовую схему деятельности подразделений Предприятия, осуществляемой на этапах жизненного цикла АС в применении к разработке ПО (включая валидацию ПО или АС в целом).

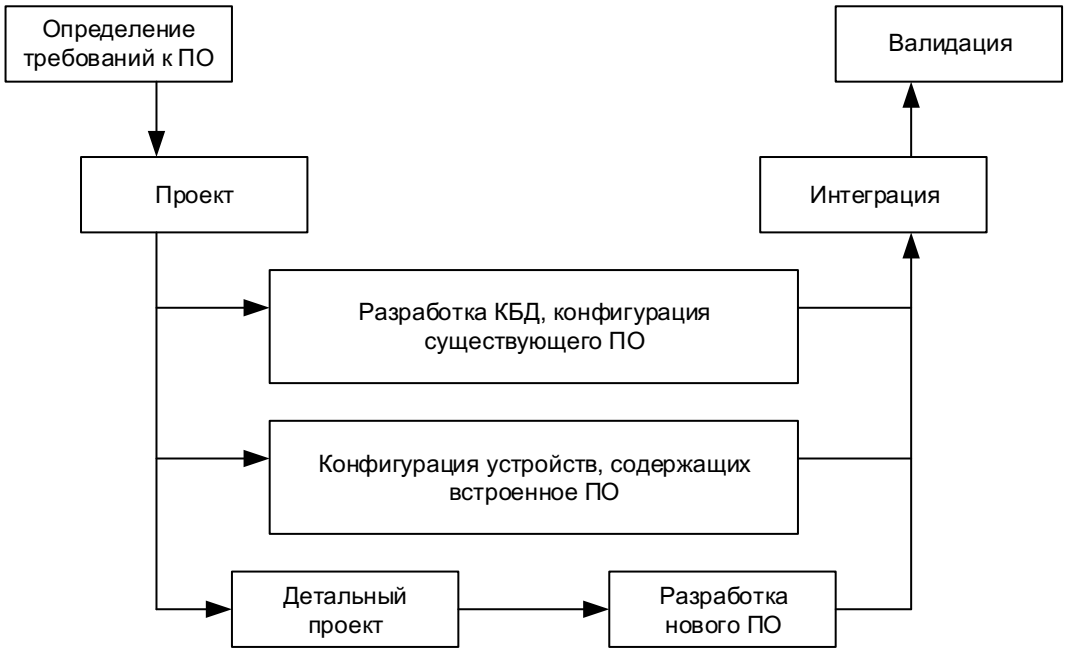

Рисунок 1 – Типовая схема деятельности, осуществляемой на этапах ЖЦ АС

4.2 Определение требований к ПО

4.2.1 При определении требований к ПО должны быть определены:

– прикладные функции АС, которые должны быть реализованы с использованием ПО;

– интерфейсы и взаимодействие ПО с его окружающей средой (например, операторами, остальной частью АС, другими системами и оборудованием). Должны быть описаны, в частности, типы и форматы данных, диапазоны и ограничения по входам и выходам;

– режимы работы ПО и соответствующие условия переходов из одного режима в другой;

– параметры ПО, изменение которых доступно оператору во время эксплуатации, а также проверки, осуществляемые ПО при изменении указанных параметров;

– требования к защищенности ПО;

– временные и количественные характеристики реализации функций;

– требования к метрологическому обеспечению ПО (в обоснованных случаях, см. раздел 0 настоящего документа);

– ограничения, требования или допущения, устанавливаемые ПО к его окружению.

4.2.2. Требования к ПО там, где это уместно, должны устанавливать условия, создаваемые для ПО окружающей средой (например, сетевой трафик, условия функционирования смежных систем) с рассмотрением предельных случаев. В качестве предельных случаев должны рассматриваться:

– отказы связи с одной или несколькими смежными системами;

– лавина данных;

– нарушение целостности принимаемых данных;

– отказы сетевой инфраструктуры.

4.2.3 Требования к ПО должны определять режимы его работы при обнаружении ошибок или отказов. При разработке требований к ПО должно учитываться его поведение при возможных ошибках операторов и отказов других систем или оборудования, с которыми взаимодействует ПО.

4.2.4 Требования к ПО должны определять задачи по своевременному информированию оператора об ошибках или отказах функций ПО. Информация, предоставляемая оператору, должна позволять ему предпринимать соответствующее действие для устранения последствий ошибок или отказов.

4.2.5 В обоснованных случаях должны быть сформулированы требования к защищенности ПО (в части защиты, конфиденциальности и целостности данных и функций, см. ГОСТ Р МЭК 61513-2011, раздел 5). При определении требований рассматриваются следующие аспекты:

– идентификация ключевых данных и функций;

– идентификация и подтверждение прав доступа пользователей и программных модулей;

– управление доступом к ключевым данным и функциям;

– контроль целостности ключевых данных и функций;

– контроль действий персонала, связанных с защищенностью.

4.2.6 Входными данными для определения перечисленных выше требований являются (в общем случае):

– требования контракта (договора);

– требования ТЗ на систему;

– требования к межсистемным интерфейсам, предоставляемые разработчиками смежных систем (в случаях, когда это уместно);

– исходные данные организаций Генерального конструктора и Генерального проектировщика;

– государственные и отраслевые нормативные требования

– другие требования, применимые для конкретного объекта внедрения АС.

4.2.7 Выходные данные должны быть документированы в виде ТЗ на ПО. ТЗ оформляется в соответствии с требованиями ЕСПД.

4.2.8 Подготовка ТЗ осуществляется отделами КД и СИ, ТЗ согласовывается с отделом РПО и передается в работу.

4.3 Проект

4.3.1 Проект ПО должен включать в себя следующие данные:

– данные об организации ПО;

– данные по распределению функций и характеристик ПО по определенным для него задачам;

– данные, идентифицирующие ранее разработанное ПО;

– данные об интерфейсах взаимодействия между задачами ПО, протоколах связи и информационных потоках;

– данные по распределению ресурсов, компонентов и задач ПО по подсистемам (в обоснованных случаях).

4.3.2 Входными данными для проекта ПО являются выходные данные, формируемые на предыдущем этапе.

4.3.3 Выходные данные должны быть документированы в виде пояснительной записки.

4.3.4 Выходные данные должны, в частности, содержать информацию о необходимости разработки нового ПО.

4.3.5 Подготовка выходных данных осуществляется отделом РПО. Документ согласуется с отделом СИ.

4.3.6 При использовании в АС только ранее разработанного ПО допускается ссылаться на существующие проектные и эксплуатационные документы АС, находящихся на более поздних стадиях ЖЦ.

4.4 Разработка КБД, конфигурация существующего ПО

4.4.1 Разработка КБД, как правило, основывается на следующих входных данных:

– данных, предоставляемых Заказчиком в виде ТЗ;

– исходных данных организаций Генерального конструктора и Генерального проектировщика в применении к конкретному объекту внедрения АС;

– знаниях технологических особенностей объекта внедрения АС;

– правилах, определенных для конфигурирования ПО, разрабатываемого на Предприятии.

4.4.2 КБД включает в себя:

– описание внутренних и внешних интерфейсов АС;

– описание взаимодействия модулей ПО;

– описание собственных сигналов АС и конфигурации технических средств АС (измерительных каналов, интерфейсных модулей и т.д.);

– описание внутренних, входных и выходных данных АС, включая:

- имена переменных, их коды в системе кодирования, принятой на объекте внедрения, типы, пределы изменения и единицы измерения;
- граничные условия и уставки;
- форматы отображения данных.

4.4.3 Использование ранее разработанного ПО в совокупности с разрабатываемой КБД должно быть верифицировано на соответствие эксплуатационным документам и ограничениям, установленным проектом ПО.

4.4.4 Выходными данными при разработке КБД является набор файлов (установочных скриптов и настроечных файлов), применимых только в конкретной АС на конкретном объекте внедрения.

4.4.5 Особенностью КБД является ее волатильность в процессе разработки и внедрения, обусловленная неполнотой проектных данных на стадии разработки и конфигурирования ПО АС (особенно для объектов внедрения, реализуемых по новым проектам).

4.4.6 Ответственность за разработку КБД возлагается на отдел СИ. Изменения в КБД вносятся по согласованию с отделом СИ.

4.4.7 Все изменения КБД на всех этапах ЖЦ должны отражаться в системе контроля версий, принятой на Предприятии. Внесение изменений в общесистемную документацию осуществляются в соответствии с правилами, установленными на Предприятии.

4.4.8 К применению в АС, поставляемой на объект внедрения или уже находящейся на нем, допускается только последняя учтенная версия КБД (т.е. версия, хранящаяся в репозитории).

4.5 Конфигурация устройств, содержащих встроенное ПО

4.5.1 Встроенное ПО отдельных устройств АС можно рассматривать как часть системного ПО АС. В соответствии с этим встроенное ПО подчиняется тем же правилам учета и модификации, что и СПО.

4.5.2 Ответственность за учет и модификацию встроенного ПО несет ведущий по проекту конкретной АС.

4.6 Разработка нового ПО

4.6.1 Разработка нового ПО может быть инициирована руководящим лицом Предприятия на основе выходных данных проекта ПО

4.6.2 Входными данными для разработки нового ПО могут являться:

– новые алгоритмы, разработанные на Предприятии и документально оформленные в соответствии с требованиями государственных и отраслевых нормативных документов;

– модифицированные алгоритмы, ранее разработанные на Предприятии;

– общеизвестные алгоритмы в случае их применимости для решения поставленной задачи;

– изменения требований к системному ПО АС, предназначенных для нового объекта внедрения, по отношению к ранее внедренным АС.

4.6.3 Выходными данными процесса разработки нового ПО являются:

– программные модули, помещаемые в репозиторий Предприятия;

– сопроводительная документация в объеме требований ТЗ, а также государственных и отраслевых нормативных документов.

Выходные данные процесса разработки нового ПО являются входными данными для разработки или корректировки общесистемной документации на конкретную АС.

Разработка, постановка на учет и внесение изменений в сопроводительную документацию на ПО и общесистемную документацию осуществляются в соответствии с правилами, установленными на Предприятии.

4.6.4 Ответственным за подготовку входных данных для разработки нового ПО является начальник отдела СИ. Входные данные согласовываются с начальником отдела РПО.

Процесс кодирования ППО находится под контролем отдела РПО, при этом все участники кодирования подчиняются общим правилам, определенным для разработки ППО.

Подготовка выходных данных процесса находится в сфере ответственности начальника отдела РПО.

4.7 Интеграция и предварительные тесты

4.7.1 Интеграции может быть подвергнута только стабильная версия ПО, находящаяся в репозитории (т.е. учтенная).

4.7.2 На данной стадии должны быть разработаны и согласованы следующие документы:

- описание конфигурационной базы данных;
- описание интерфейса связи с внешними системами (в случаях, где это применимо);
- программа и методика испытаний ПО, интегрированного на оборудование АС.

За подготовку указанных документов несут ответственность:

– описание КБД и описание интерфейса связи с внешними системами – отдел СИ (согласуется с отделом РПО);

– ПМ испытаний ППО – отдел РПО (согласуется с отделом СИ).

4.7.3 Результаты предварительного тестирования оформляются протоколом с приложением, подтверждающим соответствие приемочным критериям.

4.7.4 В обоснованных случаях допускается для проведения предварительных тестов использовать оборудование, идентичное штатному оборудованию АС (например, в случае задержки поставок штатного оборудования АС, изготавливаемого другими предприятиями). В таких случаях при интеграции ППО, КБД или ТПО необходимо максимально использовать СПО, предназначенное для интеграции на штатное оборудование.

4.8 Валидация

4.8.1 Целью валидации является доказательство того, что в готовой к поставке Заказчику или завершенной АС интегрированное ПО соответствует требованиям к функциональности, характеристикам и интерфейсу. Валидация включает в себя обоснование того, что:

– функции ПО корректно выполняются в реальных условиях эксплуатации, когда входные данные находятся в допустимых (указанных в требованиях к ПО) диапазонах;

– обеспечивается защита от человеческого фактора и отказов внешних других систем (защищенность).

4.8.2 Валидация ПО выполняется в соответствии с положениями плана валидации (АС в целом или отдельно ПО, в зависимости от влияния АС на безопасность объекта внедрения и/или требований Заказчика). План валидации устанавливает необходимые действия по валидации (комплекс валидационных тестов и условия их выполнения), а также показывает, что учтены все требования, предъявляемые к ПО.

4.8.3 Комплекс валидационных тестов представляет собой набор воздействий на ПО или его отдельные модули и набор известных откликов ПО на указанные воздействия. Воздействия по своим характеристикам должны быть максимально приближены к реальным условиям эксплуатации ПО.

4.8.4 Разработка плана осуществляется группой валидации, назначаемой распоряжением руководителя Предприятия (или руководителя проекта в рамках поставочного контракта). В группу должны входить специалисты отделов РПО и СИ, а также, по крайней мере, один специалист, не участвующий в разработке и реализации проекта ПО (АС).

4.8.5 Допускается проводить валидацию в несколько этапов (например, этап до поставки АС и этап на объекте внедрения). В обоснованных случаях для проведения валидационных

тестов до поставки АС на объект внедрения допускается использовать техническое обеспечение, идентичное штатному. При этом необходимо максимально использовать СПО, предназначенное для интеграции на штатное оборудование.

4.8.6 Свидетельством выполнения плана валидации является отчет о валидации. Отчет обязательно должен содержать данные о примененной конфигурации ПО и конфигурации окружающей среды при проведении валидации (в частности, версию КБД).

4.8.7 В случае необходимости проведения модификации ПО должно быть предусмотрено повторение валидационных тестов (полное или частичное) для оценки степени возможных изменений в работе ПО.

4.9 Верификация

4.9.1 Целью верификации является доказательство того, что разрабатываемое ПО соответствует установленным требованиям. Верификация проводится при разработке ПО АС, важных для безопасности, если не оговорено иначе.

4.9.2 Верификация проводится на следующих этапах ЖЦ:

– разработка проекта ПО;
– кодирование;
– валидация.

4.9.3 Группа верификации назначается распоряжением руководителя Предприятия (или руководителя проекта в рамках поставочного контракта). В группу должны входить специалисты отделов РПО и СИ, а также, по крайней мере, один специалист, не участвующий в разработке и реализации проекта ПО (АС).

4.9.4 На стадии проекта выполняется:

– обзор проекта ПО;
– анализ соответствия входных и выходных данных смежных модулей;
– проверка выполнения требований по устойчивости к сбоям;
– проверка выполнения требований ТЗ.

4.9.5 При обзоре проекта ПО применяются следующие методы: инспекция, критический обзор, качественная оценка характеристик. Таблица 1содержит сведения о целях и действиях, выполняемых на данном этапе.

Таблица 1 – Действия, выполняемые при обзоре проекта ПО

Метод	Цель	Действия
Инспекция	обнаружение в документации неточностей и ошибок, связанных с методикой, используемой при разработке документации или характером документа	– рассмотрение проектов документации (руководств системного программиста и оператора); – анализ найденных неточностей, выдача предложений по устранению неточностей разработчикам ПО; – оформление отчета
Критический обзор	подготовка новых предложений по улучшению и критика существующих положений	– рассмотрение проектов документации (руководств системного программиста и оператора); – выдача предложений по улучшению разработчикам ПО; – оформление отчета
Качественная оценка характеристик	прогнозирование характеристик программы перед этапом кодирования (исходя из исходных данных)	– исследование взаимодействия между модулями ПО; – анализ количества входов и выходов в модулях с целью возможного их сокращения (упрощения структуры); – оформление отчета

4.9.6 Анализ соответствия входных и выходных данных смежных модулей проводится методами инспекции и анализа трассируемости. Таблица 2 содержит сведения о целях и действиях, выполняемых на данном этапе.

Таблица 2 – Действия, выполняемые при анализе соответствия данных

Метод	Цель	Действия
Инспекция	сопоставление выходных и входных данных модулей на предмет соответствия	– группа верификации сопоставляет выходные и входные данные смежных модулей на предмет соответствия и готовят свои вопросы и предложения; – решение возникших вопросов в ходе взаимодействия между разработчиками и группой верификации; – оформление отчета
Анализ трассируемости	проверка достаточности входных данных для решения функциональных задач верифицируемого модуля	– рассмотрение функциональных задачи модулей ПО и данных, требующиеся для их решения; – проверка достаточности входных данных модулей для получения требуемых выходных данных; – оформление отчета

4.9.7 Оценка отказоустойчивости проводится с помощью имитации неблагоприятной работы целевой АС. Цель – проверка соответствия ПО требованиям по устойчивости к сбоям (ГОСТ 28195-89 в части надежности программного обеспечения). В ходе проверки группой

верификации проводится анализ возможных сбоев. Информация по сбоям должна включать описание сбоя, причины сбоя, последствия для безопасности.

При анализе выявленных сбоев следует руководствоваться следующими принципами:

– должны быть выявлены все возможные случайные или общие причины сбоев и их последствия;

– все выявленные сбои, опасные для функционирования ПО или АС, должны либо не приводить к неправильному функционированию ПО или активизировать функции сигнализации.

Результаты анализа неблагоприятных событий выявленных сбоев оформляются отчетом. Типовая форма отчета приведена в Таблице 3.

Таблица 3 – Результаты анализа неблагоприятных событий

Неблагоприятные события применительно к испытуемому ПО (модулю)	Возможные последствия	Действия испытуемой программы по предотвращению последствий неблагоприятных событий
Наличие ошибок в данных, поступающих от смежных модулей	Неверное функционирование, аварийное завершение, выдача сигнализации или "зависание"	Контроль допустимости входных данных
Наличие ошибок в запросах оператора	Неверное функционирование, аварийное завершение, выдача сигнализации или "зависание"	Контроль запросов оператора
Сбой операционной системы, процессора, внешних устройств и т.д.	Неверное функционирование, аварийное завершение или "зависание"	Рестарт программного модуля при его "зависании"
Нехватка системных ресурсов	Неверное функционирование, аварийное завершение или "зависание"	Контроль системных ресурсов, информирование оператора

4.9.8 Проверка выполнения требований ТЗ на этапе проектирования проводится с целью подтверждения того, что требования, сформулированные в ТЗ, были учтены при проектировании ПО.

Действия:

– должны быть идентифицированы требования ТЗ, предъявляемые к ПО (проверка проводится сотрудником, имеющим достаточные знания в методах решения поставленной задачи);

– проверка на стадии проектирования соответствия программы требованиям ТЗ по функциональности и надежности;

– оформление результатов проверки в виде отчета

4.9.9 На этапе кодирования проводится функциональный и структурный анализ ПО (модулей). Целью является проверка соответствия кода требованиям ТЗ.

4.9.10 При проведении функционального анализа производится проверка того, что выполняет ПО (без анализа, как оно это делает). Основной метод – подача на вход известных воздействий и сравнение выходных данных с ожидаемым результатом. По результатам функционального анализа составляется матрица верификации Таблица 4.

Таблица 4 – Матрица верификации

Название теста	Диапазон изменения параметров						
	Количество расчетов	Параметр 1			Параметр 2		Параметр
		Значение 1	Значение 2	...	Диапазон 1	Диапазон 2	...
Тест N 1 (характеристика теста, источник)							
Тест N 2							
Примечание - В ячейках матрицы значком "+" или "-" указывают выполнение или отсутствие тестов, а также величину максимального расхождения результатов расчетов с тестом.							

5. Модификация ПО

5.1 Модификация существующего ПО (СПО, ППО, ТПО, КБД) или его модулей может проводиться в следующих случаях:

– невозможность дальнейшего сопровождения ПО или его компонентов;

– реализация новых функций;

– изменение форматов отображения и форматов хранения данных;

– изменение алгоритма работы;

– изменение проектных данных после поставки ПО на объект внедрения;

– обнаружение проблем функционирования ПО в процессе пусконаладочных работ или при эксплуатации на объекте внедрения.

5.2 Решение о необходимости модификации существующего ПО, в зависимости от причины, принимается руководителем проекта или разработчиком ПО на основе информации от подразделения, осуществляющего внедрение АС, или от Заказчика.

5.3 Модифицированные компоненты ПО должны быть подвергнуты повторному тестированию, а также, в обоснованных случаях, валидации и верификации. Результаты повторного тестирования, верификации и валидации оформляются в соответствии с требованиями, изложенными в подразделе 4.7 настоящего документа.

5.4 Учет изменений производится:

– в репозитории Предприятия (программному обеспечению присваивается новый номер сборки, фиксируются изменения по отношению к предыдущей сборке);

– в архиве Предприятия (при необходимости изменения документации на модифицируемое ПО).

5.5 Ответственным за проведение изменений и их учет является подразделение-разработчик модифицируемого ПО.

6. Внедрение и сопровождение АС

6.1 Документальное сопровождение ПО (СПО, ТПО, ППО) должно включать в себя "Руководство системного программиста" и "Руководство оператора". В оговоренных случаях в документальное сопровождение может также включаться формуляр.

6.2 "Руководство системного программиста" должно содержать следующую информацию:

– назначение ПО, описание его основных функций;

– требования к техническому обеспечению и, если это применимо, к программному обеспечению, которые должны быть выполнены для корректной установки и функционирования ПО;

– процедуру установки и настройки (при необходимости) ПО на штатном месте (т.е. на конкретной АС);

– описание способов проверки, позволяющих дать общее заключение о работоспособности ПО до начала полномасштабной эксплуатации АС;

– перечень сообщений или записей в системные журналы, формируемых ПО при настройке, проверке и штатном функционировании;

– описание действий, которые необходимо предпринять в случае формирования тех или иных сообщений.

"Руководство системного программиста" должно обеспечивать гарантированную установку актуальной и полной версии ПО. Разработку и корректировку документа выполняет подразделение-разработчик ПО.

6.3 "Руководство оператора" должно содержать следующую информацию:

– назначение ПО, его основные функции;

– условия, необходимые для корректного выполнения ПО (требования к техническому обеспечению и, если это применимо, к программному обеспечению);

– последовательность действий оператора, обеспечивающих функционирование ПО (запуск, выполнение, завершение программы);

– описание форматов и элементов управления, с помощью которых оператор взаимодействует с ПО;

– перечень сообщений или записей в системные журналы, формируемых ПО при настройке, проверке и штатном функционировании;

– описание действий, которые необходимо предпринять в случае формирования тех или иных сообщений.

Разработку и корректировку документа выполняет подразделение-разработчик ПО.

6.4 Внедрением ПО АС на объекте занимается отдел КД

7. Метрологическая аттестация ПО

7.1 В соответствии с ГОСТ Р 8.654-2015 метрологически значимое ПО, выпускаемое на Предприятии, подразделяется на два типа:

–ПО измерительных систем;

–ПО контроллеров и вычислительных блоков, не входящих в состав измерительных систем, а также технических систем и устройств с измерительными функциями, осуществляющих обработку и представление измерительной информации.

7.2 Решение о необходимости метрологической аттестации принимается на основании метрологической экспертизы документации на ПО или АС (экспертиза проводится в соответствии с МИ 2174-91).

7.3 Метрологическая аттестация метрологически значимой части ПО проводится на базе подразделения-разработчика с целью получения окончательных характеристик ПО и выдачи технического формуляра (паспорта).

7.4 Аттестация проводится в соответствии с программой и методикой (ПМ) испытаний. При проведении аттестации рекомендуется участие представителя Заказчика.

8. Нормативные ссылки

– ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования.

– Издание МАГАТЭ GS-R-3.

– ГОСТ 34.201-89 Автоматизированные системы. Виды, комплектность и обозначение документов.

– ГОСТ 34.601-90 Автоматизированные системы. Стадии создания.

– РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов.

– ГОСТ 19.201-78 ЕСПД. Техническое задание.

– ГОСТ 29075-91 Системы ядерного приборостроения.

– ГОСТ Р МЭК 61513-2011 СКУ важные для безопасности. Общие требования.

– ГОСТ Р МЭК 62138-2010 СКУ важные для безопасности. ПО систем В, С.

– IEC 60880-2 Software for computers important to safety for nuclear power plants. Software aspects of defense against common cause failures, use of software tools and of pre-developed software.

– ГОСТ Р 8.654-2015 ГСИ. Требования к программному обеспечению средств измерений.

– ГОСТ Р 8.596-2002 ГСИ. МО измерительных систем. Основные положения.

– ГОСТ Р 57700.1-2017. Численное моделирование для разработки и сдачи в эксплуатацию высокотехнологичных промышленных изделий. Сертификация программного обеспечения.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводи-тельного докум. и дата	Подпись	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					