МЕЖГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ КОМИТЕТ
АВИАЦИОННЫЙ РЕГИСТР

28 октября 2004 г.

ДИРЕКТИВНОЕ ПИСЬМО
№ 07-2004

О ВВЕДЕНИИ В ДЕЙСТВИЕ РЕКОМЕНДАТЕЛЬНОГО МАТЕРИАЛА АВИАРЕГИСТРА МАК «ОЦЕНКА СООТВЕТСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВОЙ АППАРАТУРЫ И СИСТЕМ ТРЕБОВАНИЯМ КТ-178В»

Настоящим Директивным письмом вводится в действие Рекомендательный материал РМ-178В «Оценка соответствия программного обеспечения бортовой аппаратуры и систем требованиям КТ-178В» (далее по тексту – РМ-178В).

Прилагаемый Рекомендательный материал РМ-178В является руководством для экспертов Авиарегистра МАК, привлекаемых к работам по сертификации программного обеспечения в соответствии с пунктом 2.2 Директивного письма № 06-2004, и определяет необходимые действия для обеспечения полноты аудиторских проверок и минимизации временных затрат.

РМ-178В может быть использован разработчиками авиационной техники при подготовке материалов, представляемых группе экспертов Авиарегистра МАК, а также при контроле выполнения требований документа КТ-178В для комплектующих изделий категории "Б".

Приложение: Рекомендательный материал РМ-178В на 42 листах.

Заместитель редседателя
Авиарегистра МАК **Е.Ф. Жариков**

gost.e-ecolog.ru

МЕЖГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ КОМИТЕТ
АВИАЦИОННЫЙ РЕГИСТР

РЕКОМЕНДАТЕЛЬНЫЙ МАТЕРИАЛ

РМ-178В

ОЦЕНКА СООТВЕТСТВИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВОЙ АППАРАТУРЫ И СИСТЕМ ТРЕБОВАНИЯМ КТ-178В

1. ВВЕДЕНИЕ

Настоящий документ рекомендует порядок действий экспертной группы, который следует применять при оценке соответствия программного обеспечения (ПО) бортовой аппаратуры и систем (далее по тексту – систем) Квалификационным требованиям КТ-178В. Описанные действия будут приемлемыми в большинстве случаев. Допускается коррекция указанных действий, обусловленная спецификой конкретной разработки аппаратуры или системы.

Приведенные наименования проверок и их объем достаточно условны, но отражают содержание процессов создания программного обеспечения, определенных в КТ-178В. Количество проверок и их объем могут быть скорректированы исходя из специфики конкретной разработки аппаратуры или системы.

В ходе проверок экспертная группа создает следующие документы: «Акт аудиторской проверки процесса создания ПО» (по результатам каждой проверки), «Акт экспертизы документации на ПО», «Заключение о соответствии ПО», «Сводку результатов проверок» (рабочий документ группы). Для обеспечения единообразия в оформлении результатов работы группы в Приложении 1 приведены формы документов, составляемых в ходе проверок (Актов и Заключения). В Приложении 2 даны «Руководящие положения по оценке данных квалификации инструментов разработки и верификации», а Приложение 3 содержит перечень подлежащих оценке характеристик процесса создания ПО, оформленный в виде «Сводки результатов проверок».

Используемые в тексте наименования документов жизненного цикла ПО и подразумеваемое их содержание соответствуют КТ-178В. Если наименования и/или содержание документов Разработчика отличаются от приведенных, то в Актах следует показать, какие документы Разработчика представляются в качестве документов, описанных в КТ-178В. Представляемые Разработчиком документы могут быть выполнены в любом виде и на любом носителе информации, в соответствии с его «Планом управления конфигурацией» (за исключением некоторых документов типа «Плана сертификации ПО» и «Итогового заключения о ПО»). Если документы Разработчика выполнены не на основном языке АР МАК (русском), имеют нетрадиционную форму или носитель, то Разработчик должен обеспечить группе возможность работы с такими документами.

Предполагается, что настоящий документ будет использоваться экспертами совместно с КТ-178В, а не заменять его. Поэтому «Сводка результатов проверок» содержит ссылки на пункты КТ-178В, для подтверждения которых выполняется оценка характеристик процесса создания ПО. В случае возникновения затруднений следует обращаться к положениям КТ-178В и использовать их при уточнении назначения характеристик.

Настоящий документ разработан специалистами ЛИИ им. М.М. Громова, АР МАК, ГосНИИ «Аэронавигация» и ОАО «Ил».

2. ПОДГОТОВКА К ПРОВЕДЕНИЮ ПРОВЕРОК

При подготовке к проверкам следует обратить внимание на порядок взаимодействия участников проводимых экспертиз с учетом необходимости рассмотрения аспектов безопасности на уровне системы, процесса разработки и обеспечения качества всех процессов создания ПО.

Проверки, как правило, должны проводиться в помещениях Разработчика ПО. В случае когда Разработчик комплектующего изделия (Заявитель) и Разработчик ПО не являются одной и той же организацией, «Заключение о соответствии ПО» должно выдаваться Разработчику комплектующего изделия.

При подготовке к проверкам руководителю группы экспертов следует:

– ознакомиться с «Планом сертификации ПО» и подготовить предложения для экспертной группы по ее действиям;

– согласовать в экспертной группе порядок действий при проведении проверок;

– уведомить Разработчика о принятом порядке действий;

– подготовить проекты необходимых документов для каждой проверки;

– уведомить экспертов о дате и объеме проверки;
– в начале каждой проверки согласовать с участниками график работы.

При подготовке к проверкам экспертам группы следует:
– согласовать вопросы порядка действий и своего участия в проверках;
– подготовить для себя экземпляр «Сводки результатов проверок».

Количество проверок и состав выполняемых работ при проведении каждой проверки могут отличаться от рекомендуемых настоящим документом, и это должно найти отражение в составляемых «Актах проверок». Однако «Сводка результатов проверок» при этом не должна изменяться, поскольку она содержит совокупность необходимых оценок.

3. ПРОВЕРКА «ПЛАНИРОВАНИЕ»

Цель

Оценить уровень программного обеспечения системы.

Оценить планы Разработчика.

Оценить процессы при начальном планировании создания ПО.

Когда проводится

По завершении процесса начального планирования создания ПО, когда планы и стандарты разработаны и проверены.

Рассматриваемые документы

«План сертификации ПО», «План разработки ПО», «План верификации ПО», «План управления конфигурацией ПО», «План гарантии качества ПО», «Стандарты разработки требований к ПО», «Стандарты на проектирование ПО», «Стандарты на кодирование», «Планы квалификации инструментов», «Результаты верификации ПО», «Протоколы УКПО», «Протоколы ГКПО», «Сообщения о проблемах», «Материалы оценки безопасности полета при отказах системы» и другие документы (если необходимо).

Критерии оценки

Установленный уровень ПО в целом и его компонентов, а также инструментов согласуется с материалами оценки безопасности полета при отказах системы.

Планы и стандарты согласуются с указанными в разд. 11 КТ-178В и уровнем ПО.

Достигнуты применимые к процессу «Планирование» цели Приложения А КТ-178В: табл. А-1 (все цели), табл. А-8 (цели 1-4), табл. А-9 (цель 1), табл. А-10 (цели 1, 2).

Инструкции

Рассмотреть представленные материалы оценки безопасности полета при отказах системы.

Рассмотреть представленные документы жизненного цикла ПО.

Рассмотреть планы с точки зрения использования ПО при квалификации комплектующих изделий системы на внешние воздействия.

Рассмотреть каждую характеристику раздела «Планирование» «Сводки результатов проверки» и отметить результаты оценки в крайней правой колонке (знак «√» – характеристика подтверждена, знак «?» – имеется замечание).

Подготовить замечания по результатам проверки (недостатки в процессе создания ПО и предложения по улучшению процесса).

Обсудить замечания со специалистами Разработчика.

Оформление результатов

Результаты проверки оформляются в виде Акта (см. Приложение 1 КТ-178В).

4. ПРОВЕРКА «РАЗРАБОТКА»

Цель

Оценить материалы жизненного цикла ПО, относящиеся к процессам разработки требований к ПО, проектирования ПО, кодирования и связанных интегральных процессов.

Оценить эффективность применения планов и стандартов.

Оценить любые изменения в планах и стандартах.

Оценить квалификацию разработанных инструментов.

Когда проводится

По достижении высокой степени завершенности процессов разработки требований к ПО, проектирования ПО и кодирования, когда значительная часть таких документов, как «Требования к ПО», «Описание проекта ПО» и «Исходный код» разработана и проверена.

Рассматриваемые документы

«Требования к ПО», «Описание проекта ПО», «Исходный код», «Каталог среды жизненного цикла ПО», «Примеры и процедуры верификации ПО», «Результаты верификации ПО», «Протоколы УКПО», «Протоколы ГКПО», «Сообщения о проблемах», «Материалы квалификации инструментов», документы предшествующей проверки и другие документы (если необходимо).

Критерии оценки

Рассматриваемые документы согласуются с указанными в разд. 11 КТ-178В.

Процессы и документы выполняются в соответствии с планами и стандартами.

Достигнуты применимые к рассматриваемым процессам цели Приложения А КТ-178В: табл. А-2 (цели 1-6), табл. А-3 (все цели), табл. А-4 (все цели), табл. А-5 (цели 1-6), табл. А-8 (цели 1-4, 6), табл. А-9 (цели 1, 2), табл. А-10 (цель 3).

Квалификация используемых инструментов достаточна и корректна.

Инструкции

Рассмотреть представленные документы жизненного цикла ПО.

Рассмотреть материалы квалификации инструментов.

Рассмотреть и оценить каждую характеристику раздела «Разработка» «Сводки результатов проверки».

Подготовить замечания по результатам проверки и обсудить их со специалистами Разработчика.

Оформление результатов

Результаты проверки оформляются в виде Акта (см. Приложение 1).

5. ПРОВЕРКА «ВЕРИФИКАЦИЯ»

Цель

Оценить выполнение Разработчиком планов и процедур верификации (следование планам и процедурам и достижение их целей).

Оценить любые изменения в планах и стандартах.

Оценить соответствие степени достижения целей процессов УКПО и ГКПО текущей стадии разработки ПО.

Оценить квалификацию использованных инструментов.

Когда проводится

По достижении высокой степени завершенности процесса верификации ПО, когда значительная часть таких документов, как «Примеры и процедуры верификации ПО» и «Результаты верификации ПО» задокументирована и проверена.

Рассматриваемые документы

«Требования к ПО», «Описание проекта ПО», «Исходный код», «План верификации ПО», «Примеры и процедуры верификации ПО», «Результаты верификации ПО», «Каталог среды жизненного цикла ПО», «Каталог комплектации ПО», «Сообщения о проблемах», «План УКПО», «Протоколы УКПО», «План ГКПО», «Протоколы ГКПО», «Материалы квалификации инструментов», документы предшествующих проверок и другие документы (если необходимо).

Критерии оценки

Рассматриваемые документы согласуются с указанным в разд. 11 КТ-178В.

Процессы и документы выполняются в соответствии с планами и стандартами.

Достигнуты применимые к рассматриваемым процессам цели Приложения А КТ-178В: табл. А-5 (цель 7), табл. А-6 (все цели), табл. А-7 (все цели), табл. А-8 (все цели), табл. А-9 (цели 1, 2), табл. А-10 (цель 3).

Квалификация используемых инструментов достаточна и корректна.

Инструкции

Рассмотреть представленные документы жизненного цикла ПО.

Рассмотреть материалы квалификации инструментов.

Рассмотреть и оценить каждую характеристику раздела «Верификация» «Сводки результатов проверки».

Подготовить замечания по результатам проверки и обсудить их со специалистами Разработчика.

Оформление результатов

Результаты проверки оформляются в виде Акта (см. Приложение 1).

6. ПРОВЕРКА «ЗАВЕРШЕНИЕ»

Цель

Оценить итоговое «Рассмотрение соответствия ПО требованиям».

Оценить соответствие программного продукта требованиям КТ-178В.

Оценить завершение всех действий по разработке ПО, верификации, гарантии качества, управления конфигурацией и взаимодействия Заявителя и Сертифицирующего органа.

Когда проводится

По завершении разработки и верификации ПО, после проведения рассмотрения соответствия ПО требованиям и устранения выявленных недостатков, когда ПО готово к завершению квалификации системы.

Рассматриваемые документы

«Каталог комплектации ПО», «Каталог среды жизненного цикла ПО», «Итоговое заключение о ПО», «Сообщения о проблемах», «Протоколы ГКПО», Акты предшествующих проверок и связанные с ними материалы, другие документы в соответствии с разд. 11 КТ-178В.

Оцениваемые характеристики

Завершено рассмотрение соответствия ПО требованиям.
Надлежаще оформлены все документы жизненного цикла ПО.
Все цели КТ-178В, в соответствии с уровнем ПО, достигнуты.

Инструкции

Рассмотреть представленные документы жизненного цикла ПО.
Рассмотреть Акты предшествующих проверок и результаты устранения замечаний.
Рассмотреть и оценить каждую характеристику раздела «Завершение» «Сводки результатов проверки».

Оформление результатов

Результаты проверки оформляются в виде «Акта экспертизы» (см. Приложение 1).

7. ПЕРЕДАЧА ЗАКЛЮЧЕНИЯ О СООТВЕТСТВИИ ПО

Цель

Закончить экспертизу процесса создания ПО системы и оформить «Заключение о соответствии ПО».

Инструкции

Следует передать Разработчику комплектующего изделия «Заключение о соответствии ПО» в день последней проверки.

Форма Заключения приведена в Приложении 1.

Приложение 1

ФОРМЫ РАБОЧИХ И ОТЧЕТНЫХ ДОКУМЕНТОВ ГРУППЫ ЭКСПЕРТОВ

Приведенные формы «Акта проверки», «Акта экспертизы» и Заключения могут использоваться для оформления рабочих документов экспертной группы.

Длительность проверок и содержание каждой из них могут изменяться в зависимости от сложности системы. При этом следует соответствующим образом изменить содержание «Актов проверок».

Содержание «Акта аудиторской проверки процесса создания ПО» будет отражать результаты каждой проверки. Здесь же можно отметить выполнение мероприятий по результатам предшествующих проверок. Оформлению Акта следует уделить время в конце встречи, но формулировку и согласование замечаний целесообразно готовить заранее, в ходе проверки.

«Акт экспертизы документации на ПО» следует выпустить отдельным документом, содержание которого подводит итог всех работ.

«Заключение о соответствии ПО» передается Заявителю после оформления «Акта экспертизы».

АКТ № X
аудиторской проверки
процесса создания программного обеспечения
системы <АБВ> самолета <ЭЮЯ>

<дата проверки>
<место проверки>

1. Действия экспертной группы

1.1. Экспертная группа в составе <Ф.И.О.>, <Ф.И.О.>, <Ф.И.О.> выполнила аудиторскую проверку процесса создания программного обеспечения системы <АБВ> самолета <ЭЮЯ> на соответствие требованиям КТ-178В.

Оборудование системы:

<тип блока>, версия ПО – <номер версии>;

.....

<тип блока>, версия ПО – <номер версии>.

1.2. Рассмотрена документация:

<номер документа> <наименование документа> <аббревиатура> <номер соответствующего подраздела разд. 11 КТ-178В>;

.....

<номер документа> <наименование документа> <аббревиатура> <номер соответствующего подраздела разд. 11 КТ-178В>.

1.3. Рассмотрены характеристики процесса создания программного обеспечения по следующим пунктам КТ-178В: <перечисляются номера пунктов КТ-178В по таблицам Приложений 2 и 3>. Характеристики по следующим пунктам КТ-178В: <перечисляются номера пунктов КТ-178В по таблицам Приложений 2 и 3> не оценивались как необязательные для программного обеспечения заявленного уровня.

2. Результаты проверки

2.1. Разработка ПО < ведется, в основном ведется> в соответствии с требованиями КТ-178В. Степень достижения целей процессов разработки (КТ-178В, Приложение А) и качество процессов <соответствуют, не соответствуют> проверяемому этапу разработки.

2.2. Выявлены следующие недостатки в разработке ПО, препятствующие выполнению требований КТ-178В:

2.2.1. <формулировка недостатка> (<номер пункта КТ-178В>).

.....

2.3. Выданы следующие предложения по улучшению процесса создания ПО:

2.3.1. <формулировка предложения> (<номер пункта КТ-178В>);

.....

Руководитель группы <Ф.И.О.>

Эксперты

<Ф.И.О.>

<Ф.И.О.>

АКТ № X
экспертизы документации на программное обеспечение
системы <АБВ> самолета <ЭЮЯ>

<дата проверки>
<место проверки>

1. Действия экспертной группы

1.1. Экспертная группа в составе <Ф.И.О.>, <Ф.И.О.>, <Ф.И.О.> выполнила экспертизу документации на программное обеспечение системы <АБВ> самолета <ЭЮЯ> на соответствие требованиям КТ-178В.

Оборудование системы:

<тип блока>, версия ПО – <номер версии>;

.....

<тип блока>, версия ПО – <номер версии>.

1.2. Рассмотрена документация:

<номер документа> <наименование документа> <аббревиатура> <номер соответствующего подраздела разд. 11 КТ-178В>;

.....

<номер документа> <наименование документа> <аббревиатура> <номер соответствующего подраздела разд. 11 КТ-178В>.

1.3. Рассмотрены результаты выполнения мероприятий по устранению замечаний, изложенных в «Актах аудиторских проверок».

2. Результаты проверки

2.1. Документация на программное обеспечение системы <АБВ> самолета <ЭЮЯ> соответствует предъявляемым требованиям КТ-178В.

2.2. Мероприятия по устранению замечаний, изложенных в «Актах аудиторских проверок», выполнены в согласованном объеме.

2.3. Может быть оформлено Заключение о соответствии программного обеспечения системы <АБВ> самолета <ЭЮЯ> требованиям КТ-178В.

Руководитель группы <Ф.И.О.>

Эксперты <Ф.И.О.>

<Ф.И.О.>

ЗАКЛЮЧЕНИЕ
о соответствии программного обеспечения
системы <АБВ> самолета <ЭЮЯ>
требованиям КТ-178В

Оборудование системы <АБВ>:
<полное (и краткое) наименование блока>: аппаратура – <тип блока>, версия ПО – <номер версии>;
.....
<полное (и краткое) наименование блока>: аппаратура – <тип блока>, версия ПО – <номер версии>.

Уровень ПО системы – <обозначение уровня>.
Каталог комплектации ПО – <номер каталога>.
Программное обеспечение системы <АБВ> самолета <ЭЮЯ> соответствует требованиям КТ-178В.

Руководитель группы <Ф.И.О.>

Эксперты
<Ф.И.О.>

<Ф.И.О.>

Приложение 2

РУКОВОДЯЩИЕ ПОЛОЖЕНИЯ ПО ОЦЕНКЕ ДАННЫХ КВАЛИФИКАЦИИ ИНСТРУМЕНТОВ РАЗРАБОТКИ И ВЕРИФИКАЦИИ

1. Процесс квалификации инструмента может применяться как к отдельному инструменту, так и к их набору.

2. Только детерминированные инструменты могут быть квалифицированы. Интерпретация детерминизма должна применяться ко всем инструментам, выходы которых могут изменяться вне контроля пользователя.

3. При квалификации каждого инструмента верификации ПО следует проверить характеристики, приведенные в табл. 1.

Таблица 1

№ п/п	Характеристики процесса квалификации инструмента верификации ПО	Пункт КТ-178В	Оценка (√ / ?)
1	Инструмент описан в «Плане сертификации ПО» и указаны документы по квалификации инструмента	12.2.3a 12.2.4	
2	Инструмент используется для упрощения или автоматизации процессов верификации без проверки его выходных результатов согласно инструкциям разд. 6 КТ-178В	12.2	
3	Инструмент детерминирован – дает один и тот же результат при одних и тех же входных данных и одной и той же среде	12.2	
4	Если продемонстрировано обособление функций инструмента, то квалифицируются функции, которые используются для упрощения и автоматизации мероприятий верификации и выходы которых не проверяются	12.2	
5	«Эксплуатационные требования к инструменту» надлежаще выполнены	12.2.3.2	
5.1	Документ включает в себя описание функций, выполняемых инструментом, и его технические особенности	12.2.3.2a	
5.2	Приведена информация для пользователя (такая, как Инструкция по установке и Руководство пользователя)	12.2.3.2b	
5.3	Приведено описание среды, поддерживающей эксплуатацию инструмента	12.2.3.2c	
5.4	«Результаты верификации» показывают выполнение установленных проверок документа (каждое требование точно сформулировано, имеет однозначное толкование и не противоречит другим требованиям)	12.2	
5.5	Показано соответствие инструмента «Эксплуатационным требованиям к инструменту» при нормальных эксплуатационных условиях	12.2.2	
6	Документы квалификации инструмента контролируются в соответствии с категорией контроля 2	12.1.3b	
7	Подтверждены цели процесса управления конфигурацией инструмента, установленные для бортового ПО	12.2c	
8	Подтверждены цели процесса гарантии качества инструмента, установленные для бортового ПО	12.2c	

4. При квалификации каждого инструмента разработки ПО следует проверить характеристики, приведенные в табл. 2.

Таблица 2

№ п/п	Характеристики процесса квалификации инструмента разработки ПО	Пункт КТ-178В	Оценка (√ / ?)
1	Инструмент описан в «Плане сертификации ПО» и указаны документы по квалификации инструмента	12.2.3a	
2	Инструмент используется для упрощения или автоматизации процессов разработки без проверки его выходных результатов согласно инструкциям разд. 6 КТ-178В	12.2	
3	Инструмент детерминирован – дает один и тот же результат при одних и тех же входных данных и одной и той же среде	12.2	

№ п/п	Характеристики процесса квалификации инструмента разработки ПО	Пункт КТ-178B	Оценка (√ / ?)
4	Если продемонстрировано обособление функций инструмента, то квалифицируются функции, которые используются для упрощения и автоматизации мероприятий разработки и выходы которых не проверяются	12.2	
5	Документы квалификации инструмента соответствуют инструктивному материалу разд. 11 КТ-178B, имеют характеристики и содержание такие же, как у соответствующих документов на бортовое ПО	12.2.3c	
6	«План квалификации инструмента» надлежаще выполнен	12.2.3	
6.1	Документ имеет надлежащее содержание	12.2.3.1	
6.1.1	Имеется идентификация конфигурации инструмента	12.2.3.1a	
6.1.2	Приведены сведения относительно сути сертификационного зачета, который предполагается получить, – какие мероприятия процесса верификации ПО исключаются, упрощаются или автоматизируются	12.2.3.1b	
6.1.3	Указан заявляемый уровень ПО для инструмента	12.2.3.1c	
6.1.4	Инструменту назначен тот же уровень ПО, что и бортовому ПО, для разработки которого он используется, или доказана допустимость снижения этого уровня	12.2.1b	
6.1.5	Приведено описание архитектуры инструмента	12.2.3.1d	
6.1.6	Указан перечень мероприятий квалификации инструмента, подлежащих выполнению	12.2.3.1e	
6.1.7	Приведен перечень документов по квалификации инструмента, которые будут подготовлены	12.2.3.1f	
6.2	Документ удовлетворяет тем же целям, что и «Требования к ПО» соответствующего бортового ПО	12.2.3c(1)	
7	«Эксплуатационные требования к инструменту» надлежаще выполнены	12.2.3	
7.1	Документ имеет надлежащее содержание	12.2.3.2	
7.1.1	Документ включает в себя описание функций, выполняемых инструментом, и его технические особенности	12.2.3.2a	
7.1.2	Дано описание мероприятий процесса разработки, выполняемых данным инструментом	12.2.3.2a	
7.1.3	Приведена информация для пользователя (такая, как Инструкция по установке и Руководство пользователя)	12.2.3.2b	
7.1.4	Приведено описание среды, поддерживающей эксплуатацию инструмента	12.2.3.2c	
7.2	Документ удовлетворяет тем же целям, что и «Требования к ПО» соответствующего бортового ПО	12.2.3c(2)	
8	Показано соответствие инструмента «Эксплуатационным требованиям к инструменту»	12.2.1	
8.1	Выполнены рассмотрения «Эксплуатационных требований к инструменту» в соответствии с 6.3.1, a, b КТ-178B	12.2.1d(1)	
8.2	Продемонстрировано соответствие инструмента «Эксплуатационным требованиям к инструменту» в нормальных эксплуатационных условиях	12.2.1d(2)	
8.3	Продемонстрировано соответствие инструмента «Эксплуатационным требованиям к инструменту» при ненормальных эксплуатационных условиях (в том числе при действии внешних возмущений и при некоторых выбранных отказах в самом инструменте и в среде, поддерживающей его работу)	12.2.1d(3)	
8.4	Выполнены анализ покрытия требований и дополнительные испытания для достижения покрытия этих требований	12.2.1d(4)	
8.5	Выполнен анализ структурного покрытия, соответствующего уровню ПО инструмента	12.2.1d(5)	

№ п/п	Характеристики процесса квалификации инструмента разработки ПО	Пункт КТ-178В	Оценка (√ / ?)
8.6	Выполнены робастные испытания для инструмента, имеющего сложные потоки данных и управления, как указано в 6.4.2.2 КТ-178В	12.2.1d(6)	
8.7	Выполнен анализ возможных ошибок, порожденных инструментом, для того чтобы подтвердить обоснованность «Плана квалификации инструмента»	12.2.1d(7)	
9	«Итоговое заключение по квалификации инструмента» удовлетворяет тем же целям, что и «Итоговое заключение о ПО» соответствующего бортового ПО	12.2.3c(3)	
10	Процессы разработки программного обеспечения для инструмента удовлетворяют тем же целям, что и процесс разработки ПО для бортового ПО	12.2a	
11	Документы квалификации инструмента контролируются в соответствии с категорией контроля 1	12.1.3c	
12	Подтверждено достижение цели процесса управления конфигурацией инструмента (совпадает с целью для бортового ПО)	12.2c	
13	Подтверждено достижение цели процесса гарантии качества инструмента (совпадает с целью для бортового ПО)	12.2c	

5. При квалификации комбинированных инструментов, используемых и для разработки, и для верификации ПО, следует проверить характеристики, приведенные в табл. 2, если не продемонстрировано обособление между функциями разработки и верификации. Приемлемым доказательством этого обособления может служить тот факт, что выход одной функции инструмента не имеет никакого влияния на выход другой функции инструмента. Когда показывается обособление между функциями разработки и функциями верификации, обособленные функции могут быть квалифицированы так, как будто они отдельно являлись инструментами разработки и верификации.

6. Для того чтобы выполнить цели КТ-178В в отношении использования квалифицированных инструментов, эти инструменты должны находиться под управлением конфигурацией.

7. При всех изменениях инструментов, которые были предварительно квалифицированы, должен проводиться анализ влияния таких изменений на бортовое программное обеспечение. Анализ должен оценивать воздействие изменения инструмента на его выход, а также на другие инструменты, связанные с ним.

Приложение 3
ФОРМА СВОДКИ РЕЗУЛЬТАТОВ ПРОВЕРОК

Приведенная ниже форма «Сводки результатов проверок» содержит набор характеристик процесса создания программного обеспечения, оценка которых должна быть получена для подтверждения соответствия требованиям КТ-178В.

В зависимости от уровня программного обеспечения некоторые характеристики должны быть подтверждены с независимостью или могут быть исключены из рассмотрения. В таких случаях в конце описания характеристики приводится (в скобках) ее применимость. Например, если приведено – (уровень А*, В), то характеристика применима только к ПО уровня А или В и должна быть подтверждена с независимостью для ПО уровня А.

Если в ходе проверки характеристика подтверждена, то в колонке оценки рекомендуется поставить знак «√». Знак «?» в этой колонке следует использовать для отметки того, что по этой характеристике имеется замечание.

Сводка может использоваться каждым проверяющим как путеводитель в ходе рассмотрения того или иного процесса создания ПО или его части.

Сводку следует уточнять в конце каждого дня проверки при обсуждении группой совместно с персоналом Заявителя итогов дня. Рекомендуется одновременно с этим обсуждать формулировки недостатков и предложений, включаемых в Акт проверки.

СВОДКА РЕЗУЛЬТАТОВ ПРОВЕРОК СИСТЕМЫ <АБВ> САМОЛЕТА <ЭЮЯ>

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178В	Оценка (√ / ?)
1	**Планирование**		
1.1	«План сертификации ПО» надлежаще выполнен	4.1f	
1.1.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1	9.1a, табл. А-1	
1.1.2	Документ имеет надлежащие характеристики	11	
1.1.2.1	Используются термины, имеющие однозначное толкование	11a	
1.1.2.2	Может применяться без дополнительных поясняющих данных	11b	
1.1.2.3	Правильность документа можно проверить	11c	
1.1.2.4	Никакие внутренние положения не противоречат друг другу	11d	
1.1.2.5	Возможно внесение изменений с сохранением структуры документа	11e	
1.1.2.6	Предусмотрена трассировка информации документа	11f	
1.1.2.7	Форма документа обеспечивает воспроизведение и рассмотрение	11g	
1.1.3	Документ имеет надлежащее содержание	11.1	
1.1.3.1	Приведено обзорное описание системы, в том числе методов обеспечения безопасности полета	11.1a	
1.1.3.2	Приведено обзорное описание ПО, в том числе концепций обеспечения безопасности и обособления	11.1b	
1.1.3.3	Дана сводка сертификационных аспектов ПО, установлен уровень ПО и приведено его обоснование, полученное в процессе анализа безопасности полета при отказах системы	11.1c	
1.1.3.4	Описаны жизненный цикл ПО, его процессы и методы достижения целей этих процессов, участники работ и распределение ответственности	11.1d	
1.1.3.5	Определен планируемый состав документов, их форма и взаимосвязь, способ представления в АР МАК	11.1e	
1.1.3.6	Описано, каким образом будет информироваться АР МАК о мероприятиях процессов жизненного цикла ПО, для планирования соответствующих экспертиз	11.1f	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
1.1.3.7	Приведены специфические особенности, которые могут повлиять на сертификационный процесс (альтернативные методы определения соответствия, квалификация инструментов, ранее разработанное ПО, опционное ПО, многоверсионное разнородное ПО и т.п.)	11.1g	
1.2	«План разработки ПО» надлежаще выполнен	4.1f	
1.2.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C, D)	9.2c, табл. A-1	
1.2.2	Документ имеет надлежащие характеристики (уровень A, B, C) (см. 1.1.2)	11	
1.2.3	Документ имеет надлежащее содержание (уровень A, B, C)	11.2	
1.2.3.1	Приведен перечень стандартов, которые предполагается использовать при разработке ПО и применявшихся при создании ранее разработанного ПО	11.2a	
1.2.3.2	Содержит описание процессов жизненного цикла ПО с подробностями, необходимыми для гарантии правильного выполнения этих процессов	11.2b	
1.2.3.3	Указана среда разработки ПО, включая: – выбранные методы и инструменты разработки требований; – выбранные методы и инструменты проектирования; – используемые языки программирования, средства кодирования, компиляторы, редакторы связей, загрузчики; – аппаратное обеспечение (платформы) для инструментов	11.2c	
1.3	«План верификации ПО» надлежаще выполнен	4.1f	
1.3.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C, D)	9.2c, табл. A-1	
1.3.2	Документ имеет надлежащие характеристики (уровень A, B, C) (см. 1.1.2)	11	
1.3.3	Документ имеет надлежащее содержание (уровень A, B, C)	11.3	
1.3.3.1	Приведены сведения об ответственности за процесс верификации ПО и взаимодействии с другими процессами жизненного цикла ПО	11.3a	
1.3.3.2	Описаны методы обеспечения независимости верификации, когда это требуется	11.3b	
1.3.3.3	Описаны предполагаемые методы верификации: – методы рассмотрения, включая проверочные перечни и другие средства; – методы анализа, включая трассируемость и анализ покрытия; – методы испытаний, в том числе инструктивный материал относительно разработки тестовых примеров, предполагаемые тестовые процедуры, подготавливаемая документация по испытаниям	11.3c	
1.3.3.4	Описано испытательное оборудование, средства испытаний, инструменты анализа, инструкции по применению этих инструментов	11.3d	
1.3.3.5	Указаны критерии перехода, при удовлетворении которых осуществляется переход к процессу верификации ПО	11.3e	
1.3.3.6	Указаны методы верификации целостности обособления (если применимо)	11.3f	
1.3.3.7	Описаны принятые допущения относительно корректности компилятора, редактора связей и загрузчика	11.3g	
1.3.3.8	Описаны методы определения частей ПО, затронутых изменениями, а также методы определения измененных частей «Исполняемого объектного кода»; повторная верификация будет выполняться так, чтобы гарантировать устранение ранее выявленных ошибок или классов ошибок	11.3h	
1.3.3.9	Приведено описание методов достижения целей КТ-178B, применяемых к ранее разработанному ПО (если применялись другие методы)	11.3i	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
1.3.3.10	Описаны мероприятия процесса верификации многоверсионного разнородного ПО (если такое ПО применяется)	11.3j	
1.3.3.11	Описаны дополнительные мероприятия процесса верификации, выполняемые при выявлении в результате анализа структурного покрытия структуры кода, не работавшей при проведении испытаний (уровень A, B, C)	6.4.3.3	
1.3.3.11.1	Вследствие недостатков в тестовых примерах на основе требований или процедур (дополнительные тестовые примеры или изменение тестовых процедур)	6.4.3.3a	
1.3.3.11.2	Вследствие недостаточности требований к ПО (уточнение требований, разработка дополнительных тестовых примеров, выполнение дополнительных тестовых процедур)	6.4.3.3b	
1.3.3.11.3	Вследствие наличия «мертвого» кода (удаление такого кода, оценка последствий и необходимости повторной верификации)	6.4.3.3c	
1.3.3.11.4	Вследствие наличия отключенного кода (сочетание анализа и испытаний для демонстрации, что средства, позволяющие ненамеренно включить выполнение не предназначенного для выполнения ни при какой конфигурации отключенного кода, защищены, изолированы или отключены; определение конфигурации среды, необходимой для нормального выполнения отключенного кода, выполняемого только в определенных конфигурациях, и разработка дополнительных тестовых примеров и процедур для обеспечения требуемого покрытия)	6.4.3.3d	
1.4	«План управления конфигурацией ПО» надлежаще выполнен	4.1f	
1.4.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C, D)	9.2c, табл. A-1	
1.4.2	Документ имеет надлежащие характеристики (уровень A, B, C) (см. 1.1.2)	11	
1.4.3	Документ имеет надлежащее содержание (уровень A, B, C)	11.4	
1.4.3.1	Описана среда, которую предполагается использовать для УКПО, включая процедуры, инструменты, методы, стандарты, ответственность, взаимодействие при выполнении мероприятий	11.4a	
1.4.3.2	Описаны подлежащие идентификации единицы конфигурации (данные жизненного цикла, отдельно контролируемый компонент данных, комбинация данных), когда они будут идентифицироваться (до начала управления изменениями, регистрации данных трассируемости, использования в других процессах, ссылок в других данных, использования для производства и загрузки), правила идентификации данных (однозначно определяется каждая единица конфигурации и ее последовательные версии), связь идентификации ПО и идентификации системы (физическая проверка или доступность для другого оборудования)	11.4.b(1), 7.2.1	
1.4.3.3	Приведены правила введения базовых версий (для единиц конфигурации, используемых для получения сертификационного зачета, для программного продукта, для производной версии, для библиотек ПО, применение мероприятий управления изменениями), когда они будут вводиться, контроль библиотек ПО (гарантия целостности, защита от изменений), трассируемость единиц конфигурации и базовой версии (между текущей и предыдущей, с определяющим ее документом, со связанным с ней процессом)	11.4b(2), 7.2.2	
1.4.3.4	Описаны содержание и идентификация «Сообщений о проблемах» в программном продукте и в процессах жизненного цикла ПО (идентификация единицы конфигурации или мероприятия процесса, в которых обнаружена проблема, в чем процесс не соответствует планам, каковы недостатки результата процесса, проявление ненормальной	11.4.b(3), 7.2.3	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
	работы ПО, предпринимаемые корректирующие действия, идентификация единиц конфигурации, которые будут изменены, или описание процесса, в который будут внесены изменения, состояние «Сообщения о проблеме», данные об утверждении или закрытии Сообщения), когда они выпускаются, порядок утверждения или закрытий «Сообщений о проблемах», связь требующих действий Сообщений с мероприятиями управления изменениями		
1.4.3.5	Приведены единицы конфигурации и базовые версии, подлежащие управлению (единицы конфигурации, базовые версии), когда они будут контролироваться, мероприятия по управлению изменениями (регистрация, утверждение, отслеживание, изменения в ПО прослеживаются до их источников, процессы повторяются с точки начала влияния изменения на их результаты), управление до сертификации и после сертификации, методы сохранения целостности базовых версий и единиц конфигурации (защита от изменений, изменение идентификации конфигурации при любом изменении, обновление измененных документов)	11.4.b(4), 7.2.4	
1.4.3.6	Описаны порядок организации обратных связей от одних процессов к другим, порядок оценки и назначения приоритетов проблемам, утверждения изменений, порядок разрешения возникающих проблем, реализации изменений, связь этих правил с мероприятиями «Сообщений о проблемах» и управления изменениями	11.4.b(5), 7.2.5	
1.4.3.7	Указаны данные, которые предполагается регистрировать для учета состояния конфигурации (регистрация идентификации единиц конфигурации, базовой версии, состояния «Сообщений о проблемах», хронология изменений и состояния выпуска программного продукта, перечень хранимых документов), где эти данные будут храниться (средства записи и регистрации), как они могут быть получены для составления отчетов и когда они появятся	11.4.b(6), 7.2.6	
1.4.3.8	Описаны контроль целостности, порядок и полномочия на выпуск, хранение данных (обеспечивается возможность воспроизведения данных; установлены процедуры, гарантирующие целостность хранимых данных посредством гарантии невозможности внесения несанкционированных изменений, выбора надлежащего носителя данных, периодической проверки сохранности и обновления архивных данных, раздельного хранения дубликатов; процедуры гарантируют безошибочное копирование «Исполняемого объектного кода», и этот процесс проверяем; единицы конфигурации идентифицируются и выпускаются до начала производства ПО, назначен орган, ответственный за выпуск, процедуре выпуска подвергаются, как минимум, «Исполняемый объектный код» и соответствующий носитель, используемый для загрузки ПО)	11.4.b(7), 7.2.7	
1.4.3.9	Описаны меры предосторожности при загрузке ПО (нанесение блочных номеров и идентификация носителей, идентифицирующих конфигурации ПО, которые должны быть утверждены для загрузки), протокол загрузки (сохранение документов, подтверждающих совместимость ПО с аппаратным обеспечением системы)	11.4.b(8), 7.2.8	
1.4.3.10	Указан контроль инструментов, используемых для разработки, производства, верификации и загрузки ПО (идентифицирован «Объектный код инструментов», установлены категории контроля квалифицированных инструментов и инструментов сборки и загрузки ПО)	11.4.b(9), 7.2.9	
1.4.3.11	Описаны процедуры, соответствующие категориям контроля данных 1 и 2 (КК1: идентификация конфигураций, базовые версии, трассируемость, «Сообщения о проблемах», целостность и идентификация при управлении изменениями, отслеживание при управлении изменениями, рассмотрение изменений, учет состояния конфигурации, воспроизведение, защита от несанкционированных изменений, выбор, обновление и воспроизведение	11.4.b(10), 7.3	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178В	Оценка (√ / ?)
	носителей, выпуск, хранение документов; КК2: идентификация конфигураций, трассируемость, целостность и идентификация при управлении изменениями, воспроизведение, защита от несанкционированных изменений, хранение документов)		
1.4.3.12	Указаны критерии перехода к процессу УКПО	11.4c	
1.4.3.13	Определены документы, составляемые в результате мероприятий УКПО	11.4d	
1.4.3.14	Описан порядок распространения требований процесса УКПО на поставщиков	11.4e	
1.5	«План гарантии качества ПО» надлежаще выполнен	4.1f	
1.5.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C, D)	9.2c, табл. A-1	
1.5.2	Документ имеет надлежащие характеристики (уровень A, B, C) (см. 1.1.2)	11	
1.5.3	Документ имеет надлежащее содержание (уровень A, B, C)	11.5	
1.5.3.1	Описана среда ГКПО, включая сферу действия ГКПО, распределение ответственности и взаимодействие, стандарты, процедуры, инструменты и методы	11.5a	
1.5.3.2	Приведено положение о полномочиях ГКПО, распределение ответственности и независимость, включая полномочия утверждения программных продуктов	11.5b 8.2a	
1.5.3.3	Описаны мероприятия ГКПО применительно к каждому процессу жизненного цикла, включая: – методы и средства ГКПО (рассмотрения, аудиторские проверки, составление Актов, инспекции, непрерывный контроль процессов жизненного цикла); – мероприятия, связанные с «Сообщениями о проблемах», отслеживанием и корректирующими действиями; – рассмотрение соответствия ПО требованиям	11.5c 8.2b 8.2c 8.2d 8.2e 8.2f 8.2g	
1.5.3.4	Определены критерии перехода к процессам ГКПО	11.5d	
1.5.3.5	Указана временная привязка мероприятий процесса ГКПО к мероприятиям процессов жизненного цикла ПО	11.5e	
1.5.3.6	Определены протоколы, составляемые в процессе ГКПО	11.5f 8.2h	
1.5.3.7	Описаны методы и средства, гарантирующие, что процессы поставщиков и выходные результаты поставщиков соответствуют этому плану	11.5g	
1.6	«Стандарты на разработку требований к ПО» надлежаще выполнены (уровень A, B, C)	4.1e	
1.6.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C)	9.2c, табл. A-1	
1.6.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
1.6.3	Документ имеет надлежащее содержание	11.6	
1.6.3.1	Приведены методы, которые предполагается использовать при разработке требований к ПО	11.6a	
1.6.3.2	Указаны методы и способы обозначений, которые предполагается использовать для формулирования требований	11.6b	
1.6.3.3	Введены ограничения на использование инструментов при разработке требований	11.6c	
1.6.3.4	Описан метод, который предполагается использовать для разработки производных требований	11.6d	
1.7	«Стандарты на проектирование ПО» надлежаще выполнены (уровень A, B, C)	4.1e	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
1.7.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C)	9.2c, табл. A-1	
1.7.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
1.7.3	Документ имеет надлежащее содержание	11.7	
1.7.3.1	Содержатся используемые методы описания проекта	11.7a	
1.7.3.2	Приведены правила наименования	11.7b	
1.7.3.3	Указаны ограничения, накладываемые на разрешенные методы проектирования (диспетчеризацию, использование прерываний, динамическое управление задачами, глобальные переменные, обработку особых ситуаций и т.п.), и обоснование таких ограничений	11.7c	
1.7.3.4	Введены ограничения на использование инструментов проектирования	11.7d	
1.7.3.5	Введены ограничения на проект (исключение рекурсии, динамических объектов, альтернативных имен данных, компактных выражений и т.п.)	11.7e	
1.7.3.6	Введены ограничения на сложность (максимальная вложенность вызовов или условных операторов, использование безусловных переходов, количество точек входа/выхода в компоненты программы и т.п.)	11.7f	
1.8	«Стандарты на кодирование» надлежаще выполнены (уровень A, B, C)	4.1e	
1.8.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C)	9.2c, табл. A-1	
1.8.2	Документ имеет надлежащие характеристики (см.1.1.2)	11	
1.8.3	Документ имеет надлежащее содержание	11.8	
1.8.3.1	Указаны языки программирования, которые предполагается использовать, и/или их подмножества, документы, характеризующие язык программирования и однозначно определяющие его синтаксис, управление данными и побочные эффекты	11.8a	
1.8.3.2	Указаны стандарты на форму представления (ограничения длины строк, отступы, пустые строки и т.п.) и документацию (имя автора, хронология версий, входы и выходы программы, изменяемые глобальные данные и т.п.) «Исходного кода»	11.8b	
1.8.3.3	Приведены правила наименования компонентов, подпрограмм, переменных и констант	11.8c	
1.8.3.4	Приведены условия и ограничения, накладываемые на принятые соглашения о приемах кодирования (степень взаимосвязи между компонентами программы, сложность логических и численных выражений и т.п.), а также обоснование их применения	11.8d	
1.8.3.5	Введены ограничения на применение инструментов кодирования	11.8e	
1.9	«Планы квалификации инструментов» надлежаще выполнены (см. Приложение 2)	4.1c	
1.10	Достигнуты цели процесса планирования создания ПО	4.1, табл. A-1	
1.10.1	Рассмотренные материалы показывают, что определены мероприятия процессов разработки ПО и интегральных процессов	4.1.a 4.3 A-1 № 1	
1.10.1.1	Планы ПО обеспечивают своевременное руководство для персонала, участвующего в процессе разработки и интегральных процессах	4.2a	
1.10.1.2	Определены стандарты разработки ПО рассматриваемого проекта	4.2b	
1.10.1.3	Выбраны методы и инструменты, обеспечивающие предотвращение ошибок в процессе разработки ПО	4.2c	
1.10.1.4	Обеспечена координация процессов разработки и интегральных процессов	4.2d	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
1.10.1.5	Предусмотрена процедура пересмотра планов	4.2e	
1.10.1.6	Выбраны методы и инструменты, учитывающие использование в системе многоверсионного разнородного ПО	4.2f	
1.10.1.7	Планы и стандарты на разработку ПО находятся под управлением изменениями, а их рассмотрения завершены	4.2g	
1.10.1.8	Рассмотрения и мероприятия ГКПО подтверждают, что выбранные методы обеспечат достижения целей КТ-178B	4.6a	
1.10.1.9	Рассмотрения и мероприятия ГКПО подтверждают, что процессы жизненного цикла ПО могут применяться согласованно	4.6b	
1.10.1.10	Рассмотрения и мероприятия ГКПО подтверждают, что результаты каждого процесса могут быть трассированы на его мероприятия и входные данные, показывая степень независимости мероприятия, среду и используемые методы	4.6c	
1.10.1.11	Рассмотрения и мероприятия ГКПО подтверждают, что результаты процесса планирования создания ПО согласованы и соответствуют разд. 11 КТ-178A	4.6d 4.3a	
1.10.1.12	Наличие отключенного кода надлежаще отражено в мероприятиях планов и стандартов создания ПО; описаны методы определения отключенного кода, его верификация и правила обращения с ним	4.2h	
1.10.1.13	Наличие модифицируемого пользователем кода надлежаще отражено в мероприятиях планов и стандартов создания ПО; указаны процесс, инструменты, среда и данные, доказывающие, что немодифицируемые компоненты защищены от влияния модифицируемых и представленные средства изменения модифицированных компонентов являются единственными	4.2i 5.2.3a 5.2.3b	
1.10.2	Рассмотренные материалы показывают, что определены жизненный цикл ПО, критерии перехода, взаимосвязи и последовательность процессов (уровень A, B, C)	4.1b A-1 № 2	
1.10.2.1	В планах определены критерии перехода между процессами и указаны: входные данные (включая обратные связи от других процессов), мероприятия интегральных процессов для реакции на эти входные данные, доступность инструментов, методов, планов и процедур	4.3b	
1.10.2.2	В планах создания ПО установлены процедуры внесения изменений в ПО и, при необходимости, в сами планы до применения ПО на сертифицированном воздушном судне или двигателе	4.3c	
1.10.3	Рассмотренные материалы показывают, что определена среда жизненного цикла ПО, включая методы и инструменты каждого процесса жизненного цикла (уровень A, B, C)	4.1c A-1 № 3	
1.10.4	Рассмотренные материалы показывают, что учтены дополнительные инструктивные материалы, подобные приведенным в разд. 12 КТ-178B	4.1d A-1 № 4	
1.10.5	Рассмотренные материалы показывают, что установлены необходимые стандарты разработки ПО (уровень A, B, C)	4.1e A-1 № 5	
1.10.5.1	Стандарты на разработку ПО соответствуют изложенному в разд. 11 КТ-178B	4.5a	
1.10.5.2	Стандарты на разработку ПО предоставляют возможность единообразного проектирования и реализации заданного программного продукта	4.5b	
1.10.5.3	Стандарты на разработку ПО запрещают использование конструкций и методов, приводящих к результатам, не поддающимся проверке или несовместимым с требованиями безопасности	4.5c	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178В	Оценка (√ / ?)
1.10.6	Рассмотренные материалы показывают, что планы создания ПО соответствуют изложенному в разд. 11 КТ-178В (уровень А, В, С)	4.1f 4.3a 4.6 А-1 № 6	
1.10.7	Рассмотренные материалы показывают, что обеспечивается координация разработки и пересмотра планов создания ПО (уровень А, В, С)	4.1g 4.6 А-1 № 7	
1.11	Достигнуты цели процесса управления конфигурацией ПО	7.1, табл. А-8	
1.11.1	«Протоколы УКПО» показывают, что единицы конфигурации идентифицированы	7.2.1 А-8 № 1	
1.11.2	«Протоколы УКПО» показывают, что базовые версии и трассируемость установлены	7.2.2 А-8 № 2	
1.11.3	«Протоколы УКПО» и «Сообщения о проблемах» показывают, что порядок сообщений о проблемах, управления изменениями, рассмотрения изменений и учета состояния конфигурации установлен	7.2.3 7.2.4 7.2.5 7.2.6 А-8 № 3	
1.11.4	«Протоколы УКПО» показывают, что порядок архивирования, воспроизведения и выпуска установлен	7.2.7 А-8 № 4	
1.12	Достигнуты цели процесса гарантии качества ПО	8.1, табл. А-9	
1.12.1	«Протоколы ГКПО» гарантируют, что процессы разработки ПО и интегральные процессы соответствуют утвержденным планам и стандартам	8.1a А-9 № 1	
1.13	Достигнуты цели процесса взаимодействия Заявителя и Сертифицирующего органа	9, табл. А-10	
1.13.1	Взаимодействие и взаимопонимание между Заявителем и Сертифицирующим органом установлены	9 А-10 № 1	
1.13.2	Методы определения соответствия предложены, «План сертификации ПО» согласован	9.1 А-10 № 2	
1.14	Документы и процессы, рассмотренные в ходе проверки, понятны персоналу (по результатам бесед)	1.1	
2	**Разработка**		
2.1	«Требования к ПО» надлежаще выполнены	5.1.2	
2.1.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1	9.2c, табл. А-2	
2.1.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
2.1.3	Документ имеет надлежащее содержание	11.9	
2.1.3.1	Описано, каким образом требования к системе трансформируются в требования к ПО, в том числе требования к безопасности и возможные отказные состояния	11.9a	
2.1.3.2	Приведены функциональные и технические требования для каждого режима работы	11.9b	
2.1.3.3	Указаны критерии исполнения (точность, правильность и т.п.)	11.9c	
2.1.3.4	Введены временные требования и ограничения	11.9d	
2.1.3.5	Указаны ограничения по памяти	11.9e	
2.1.3.6	Описано взаимодействие аппаратуры и ПО	11.9f	
2.1.3.7	Приведены требования к обнаружению отказов и контролю безопасности	11.9g	
2.1.3.8	Указаны требования по обособлению, относящиеся к ПО (если применимо)	11.9h	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
2.1.4	Прошли экспертизу требования различных типов (интерфейс, назначение, контроль и т.п.)	9.2	
2.2	«Описание проекта ПО» надлежаще выполнено	5.2.2	
2.2.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C, D)	9.2c, табл. A-2	
2.2.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
2.2.3	Документ имеет надлежащее содержание	11.10	
2.2.3.1	Приведено описание того, каким образом ПО удовлетворяет предъявляемым требованиям к ПО высокого уровня, включая алгоритмы, структуры данных и распределение требований по процессорам и задачам	11.10a	
2.2.3.2	Приведено описание архитектуры ПО, определяющей конкретную структуру программы для выполнения требований	11.10b	
2.2.3.3	Приведено описание входов/выходов (внешних и внутренних)	11.10c	
2.2.3.4	Показан поток данных и поток управления	11.10d	
2.2.3.5	Дано распределение ресурсов и связанные с этим ограничения, наличие запасов по ресурсам и методы их измерения (по быстродействию, по памяти и т.п.)	11.10e	
2.2.3.6	Приведены процедуры диспетчеризации и схемы межпроцессорного и межзадачного обмена, включая жесткое временное упорядочивание, принудительное разделение времени, прерывания	11.10f	
2.2.3.7	Указаны методы проектирования и подробные сведения относительно их применения	11.10g	
2.2.3.8	Установлены методы обособления и способы предотвращения нарушения обособления	11.10h	
2.2.3.9	Имеется описание всех вновь или ранее разработанных компонентов ПО и, если они разработаны ранее, то даны ссылки на базовые версии, в которых они получены	11.10i	
2.2.3.10	Описаны производные требования, появившиеся в процессе проектирования	11.10j	
2.2.3.11	Для отключенного кода дано описание средств, гарантирующих, что он не будет активизирован в целевом вычислителе	11.10k	
2.2.3.12	Имеется обоснование тех проектных решений, которые трассируемы на требования к безопасности системы	11.10l	
2.2.4	Прошли экспертизу требования проекта различных типов	9.2	
2.3	«Исходный код» надлежаще выполнен	5.3.2	
2.3.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1	9.2c, табл. A-2	
2.3.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
2.3.3	Документ имеет надлежащее содержание	11.11	
2.2.3.1	Приведен код, записанный на исходном языке программирования, инструкции компилятору для генерации объектного кода, данные для редактирования связей и загрузки, данные идентификации ПО (наименование, версия или дата модификации и т.п.)	11.11	
2.3.4	Прошли экспертизу компоненты «Исходного кода» различных типов	9.2	
2.4	«Результаты верификации ПО» надлежаще выполнены	6.2	
2.4.1	Документ имеет надлежащее состояние и отнесен к категории контроля 2	9.2c, табл. A-3	
2.4.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
2.4.3	Документ имеет надлежащее содержание	11.14	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
2.4.3.1	В документе содержатся результаты каждого рассмотрения, анализа, испытания, показывающие для каждой процедуры, проходит она или не проходит, а также общий результат «проходит/не проходит»	11.14a	
2.4.3.2	В документе содержится идентификация единиц конфигурации или версий ПО, которые проходили рассмотрение, анализ или испытание	11.14b	
2.4.3.3	В документе содержатся результаты испытаний, рассмотрений и анализов, включая анализ покрытия и анализ трассируемости	11.14c	
2.4.4	Верификация прошедших экспертизу компонентов «Требований к ПО», «Проекта ПО» и «Исходного кода» корректно описана в документе	9.2	
2.5	«Каталог среды жизненного цикла ПО» надлежаще выполнен	7.2.9	
2.5.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B, C) или 2 (уровень D)	9.2c, табл. A-8	
2.5.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
2.5.3	Документ имеет надлежащее содержание	11.15	
2.5.3.1	В документе идентифицированы аппаратные средства среды жизненного цикла ПО и их операционные системы	11.15a	
2.5.3.2	В документе идентифицированы инструменты разработки ПО (компиляторы, редакторы связей, загрузчики и т.п.), а также инструменты, обеспечивающие целостность данных (формирующие и встраивающие тестовые суммы или проверки с использованием циклического избыточного кода)	11.15b	
2.5.3.3	В документе идентифицирована используемая среда испытаний для верификации (инструменты верификации ПО и т.п.)	11.15c	
2.5.3.4	В документе идентифицированы квалифицированные инструменты и данные по их квалификации	11.15d	
2.5.4	Данные квалификации инструментов достаточны и корректны (см. Приложение 2)	12.2	
2.6	«Сообщения о проблемах» надлежаще выполнены	7.2.3	
2.6.1	Документ имеет надлежащее состояние и отнесен к категории контроля 2	9.2c, табл. A-8	
2.6.2	Документ имеет надлежащее содержание	11.17	
2.6.2.1	В документах содержится идентификация единиц конфигурации ПО и/или наименование мероприятия процесса жизненного цикла ПО, в котором обнаружена проблема	11.17a	
2.6.2.2	В документах содержится идентификация единиц конфигурации, которые будут изменены, или описание процесса, в который будут внесены изменения	11.17b	
2.6.2.3	В документах содержится описание проблемы, позволяющее понять ее суть и разрешить ее	11.17c	
2.6.2.4	В документах содержится описание корректирующих действий для разрешения обнаруженной проблемы	11.17d	
2.7	«Протоколы УКПО» надлежаще выполнены	7	
2.7.1	Документ имеет надлежащее состояние и отнесен к категории контроля 2	9.2c, табл. A-8	
2.7.2	В документе регистрируются результаты мероприятий, проводимых в соответствии с «Планом управления конфигурацией ПО»	11.18 11.4d	
2.8	«Протоколы ГКПО» надлежаще выполнены	11.19	
2.8.1	Документ имеет надлежащее состояние и отнесен к категории контроля 2	9.2c, табл. A-9	
2.8.2	В документе регистрируются результаты мероприятий, проводимых в соответствии с «Планом управления конфигурацией ПО»	11.19 11.5f	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178В	Оценка (√ / ?)
2.9	Достигнуты относящиеся цели процессов разработки ПО	5.1.1 5.2.1 5.3.1 табл. А-2	
2.9.1	Рассмотренные материалы показывают, что разработаны требования высокого уровня	5.1.1a А-2 № 1	
2.9.1.1	Проанализированы функциональные требования и требования к взаимодействию для исключения неоднозначности, противоречий и неопределенности условий	5.1.2a	
2.9.1.2	Неверные или недостаточные входные данные процесса разработки требований к ПО возвращаются на входы соответствующих процессов для внесения ясности и поправок	5.1.2b	
2.9.1.3	Каждое требование к системе, отнесенное к ПО, включено в требования высокого уровня	5.1.2c	
2.9.1.4	Определены требования высокого уровня, связанные с требованиями к системе и отнесенные к ПО, которые введены для предотвращения опасности применения системы	5.1.2d	
2.9.1.5	Требования высокого уровня удовлетворяют «Стандартам на разработку требований к ПО», проверяемы и согласованы	5.1.2e	
2.9.1.6	Требования высокого уровня установлены в количественной форме с указанием допусков там, где это применимо	5.1.2f	
2.9.1.7	Требования высокого уровня не содержат детали разработки и верификации, за исключением установленных и обоснованных проектных ограничений	5.1.2g	
2.9.1.8	Каждое требование к системе, отнесенное к ПО, трассируемо на одно или более требований высокого уровня	5.1.2h	
2.9.1.9	Каждое требование высокого уровня трассируемо на одно или более требований к системе	5.1.2i 5.5a	
2.9.2	Рассмотренные материалы показывают, что определены производные требования высокого уровня	5.1.1b А-2 № 2	
2.9.2.1	Производные требования высокого уровня переданы в процесс оценки безопасности системы	5.1.2j	
2.9.3	Рассмотренные материалы показывают, что определена архитектура ПО и разработаны требования низкого уровня	5.2.1a А-2 № 3 А-2 № 4	
2.9.3.1	Требования низкого уровня и архитектура ПО, разработанные в процессе проектирования, удовлетворяют «Стандартам на проектирование ПО», трассируемы, проверяемы и согласованы	5.2.2a 5.5b	
2.9.3.2	При формулировании требований к безопасности предусмотрен контроль потоков управления и данных (сторожевой таймер, проверка на непротиворечивость, перекрестное сравнение каналов и т.п.)	5.2.2d	
2.9.3.3	Реакция на отказные состояния удовлетворяет требованиям к безопасности	5.2.2e	
2.9.3.4	Недостаточные и неправильные входные данные, выявленные в процессе проектирования, возвращаются в процесс жизненного цикла системы, процесс разработки требований к ПО или в процесс планирования создания ПО для внесения ясности и поправок	5.2.2f	
2.9.3.5	При проектировании ПО, модифицируемого пользователем, немодифицируемые компоненты защищены от влияния модифицируемых для предотвращения неблагоприятного воздействия вторых на работу первых (эта защита реализована аппаратными или программными средствами, средствами для внесения изменений или комбинацией этих средств)	5.2.3a	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
2.9.3.6	При проектировании ПО, модифицируемого пользователем, показано, что представленные средства являются единственными, с помощью которых в модифицируемый компонент можно внести изменения	5.2.3b	
2.9.4	Рассмотренные материалы показывают, что определены производные требования низкого уровня	5.2.1b A-2 № 5	
2.9.4.1	Для гарантии отсутствия нарушения требований высокого уровня установлены и проанализированы производные требования	5.2.2b	
2.9.4.2	При использовании обособления или других архитектурных решений, которые могут изменить уровни ПО отдельных его компонентов, определены дополнительные производные требования и выданы для анализа в процессе оценки безопасности системы	5.2.2c	
2.9.5	Рассмотренные материалы показывают, что разработан «Исходный код»	5.3.1a A-2 № 6	
2.9.5.1	«Исходный код» реализует требования низкого уровня и соответствует архитектуре ПО	5.3.2a	
2.9.5.2	«Исходный код» соответствует «Стандартам на кодирование»	5.3.2b	
2.9.5.3	«Исходный код» трассируем на «Описание проекта ПО»	5.3.2c 5.5c	
2.9.5.4	Недостаточные и неправильные входные данные, выявленные в процессе кодирования, возвращаются в процесс разработки требований к ПО, в процесс проектирования ПО или в процесс планирования создания ПО для внесения ясности и поправок	5.3.2d	
2.10	Достигнуты относящиеся цели процесса верификации ПО	6.1	
2.10.1	Рассмотренные материалы показывают, что проверены требования высокого уровня	6.1a, табл. A-3	
2.10.1.1	Требования высокого уровня к ПО соответствуют требованиям к системе (функции системы, выполняемые ПО, определены; функциональные и технические требования, а также требования по безопасности системы удовлетворяются требованиями высокого уровня; производные требования и причины их введения определены правильно) (уровень A*, B*, C, D)	6.3.1a, A-3 № 1	
2.10.1.2	Требования высокого уровня точны и непротиворечивы (каждое требование высокого уровня точно сформулировано, имеет однозначное толкование, достаточно детализировано и не противоречит другим требованиям) (уровень A*, B*, C, D)	6.3.1b A-3 № 2	
2.10.1.3	Требования высокого уровня совместимы с целевым вычислителем (отсутствуют несоответствия между требованиями высокого уровня и характеристиками аппаратуры и ПО целевого вычислителя в отношении времени реакции системы и аппаратных средств ввода/вывода и т.п.) (уровень A, B)	6.3.1c A-3 № 3	
2.10.1.4	Требования высокого уровня проверяемы (каждое требование высокого уровня может быть проверено) (уровень A, B, C)	6.3.1d A-3 № 4	
2.10.1.5	Требования высокого уровня соответствуют стандартам (процесс разработки требований осуществлялся в соответствии со «Стандартами на разработку требований к ПО», отступления от стандартов обоснованы) (уровень A, B, C)	6.3.1e A-3 № 5	
2.10.1.6	Требования высокого уровня трассируемы на требования к системе (уровень A, B, C, D)	6.3.1f A-3 № 6	
2.10.1.7	Алгоритмы правильны (обеспечивается точная и правильная работа предложенных алгоритмов, особенно вблизи точек разрыва) (уровень A*, B*, C)	6.3.1g A-3 № 7	
2.10.2	Рассмотренные материалы показывают, что проверены требования низкого уровня и архитектура ПО	6.1b, табл. A-4	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
2.10.2.1	Требования низкого уровня удовлетворяют требованиям высокого уровня (требования низкого уровня соответствуют требованиям к ПО высокого уровня; производные требования и причины их появления в проекте определены правильно) (уровень A*, B*, C)	6.3.2a A-4 № 1	
2.10.2.2	Требования низкого уровня правильны и непротиворечивы (каждое требование низкого уровня точно сформулировано, имеет однозначное толкование и не противоречит другим требованиям) (уровень A*, B*, C)	6.3.2b A-4 № 2	
2.10.2.3	Требования низкого уровня совместимы с целевым вычислителем (отсутствуют несоответствия между требованиями к ПО низкого уровня и аппаратно-программными характеристиками целевого вычислителя, в том числе в отношении использования ресурсов, времени реакции системы и аппаратных средств ввода/вывода) (уровень A, B)	6.3.2c A-4 № 3	
2.10.2.4	Требования низкого уровня проверяемы (каждое требование низкого уровня может быть проверено) (уровень A, B)	6.3.2d A-4 № 4	
2.10.2.5	Требования низкого уровня соответствуют стандартам (процесс проектирования ПО осуществлялся в соответствии со «Стандартами на проектирование ПО», отступления от стандартов обоснованы) (уровень A, B, C)	6.3.2t A-4 № 5	
2.10.2.6	Требования низкого уровня трассируемы на требования высокого уровня (уровень A, B, C)	6.3.2f A-4 № 6	
2.10.2.7	Алгоритмы правильны (обеспечивается точная и правильная работа алгоритмов, особенно вблизи точек разрыва) (уровень A*, B*, C)	6.3.2g A-4 № 7	
2.10.2.8	Архитектура ПО совместима с требованиями высокого уровня (архитектура ПО совместима с требованиями высокого уровня, в особенности с требованиями к функциям, гарантирующим целостность системы) (уровень A*, B, C)	6.3.3a A-4 № 8	
2.10.2.9	Архитектура ПО непротиворечива (между компонентами архитектуры установлена правильная взаимосвязь через поток данных и поток управления) (уровень A*, B, C)	6.3.3b A-4 № 9	
2.10.2.10	Архитектура ПО совместима с целевым вычислителем (отсутствуют противоречия между архитектурой ПО и характеристиками аппаратуры и ПО целевого вычислителя, в особенности в части инициализации, асинхронной работы, синхронизации и прерываний) (уровень A, B)	6.3.3c A-4 № 10	
2.10.2.11	Архитектура ПО проверяема (архитектура ПО может быть проверена, в том числе отсутствуют неограниченные рекурсивные алгоритмы) (уровень A, B)	6.3.3d A-4 № 11	
2.10.2.12	Архитектура ПО соответствует стандартам (процесс проектирования ПО осуществлялся в соответствии со «Стандартами на проектирование ПО», отступления от стандартов обоснованы, в особенности в части ограничений на сложность и проектные решения, которые могли бы противоречить требованиям к безопасности) (уровень A, B, C)	6.3.3e A-4 № 12	
2.10.2.13	Целостность обособления ПО подтверждена (нарушения обособления предотвращены) (уровень A*, B, C, D)	6.3.3f A-4 № 13	
2.10.3	Рассмотренные материалы показывают, что проверен «Исходный код»	6.1c	
2.10.3.1	«Исходный код» удовлетворяет требованиям низкого уровня («Исходный код» правилен и полон по отношению к требованиям к ПО низкого уровня, и в нем не реализовано выполнение незадокументированных функций) (уровень A*, B*, C)	6.3.4a A-1 № 1	
2.10.3.2	«Исходный код» согласуется с архитектурой ПО («Исходный код» согласуется с потоком данных и потоком управления, которые определены в архитектуре ПО) (уровень A*, B, C)	6.3.4b A-1 № 2	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
2.10.3.3	«Исходный код» проверяем («Исходный код» не содержит операторов и структур, которые не могут быть проверены, и для испытаний в него не требуется вносить изменения) (уровень A, B)	6.3.4c A-1 № 3	
2.10.3.4	«Исходный код» удовлетворяет стандартам (кодирование осуществлено в соответствии со «Стандартами на кодирование», в особенности в части ограничений на сложность и на конструкции кода, введенные для удовлетворения требований к безопасности; отступления от стандартов оправданы; сложность включает степень связи между компонентами ПО, уровни вложенности управляющих структур, сложность логических и численных выражений) (уровень A, B, C)	6.3.4d A-1 № 4	
2.10.3.5	«Исходный код» трассируем на требования низкого уровня (уровень A, B, C)	6.3.4e A-1 № 5	
2.10.3.6	«Исходный код» правилен и непротиворечив (выполнена оценка применения стеков, возможности переполнения и разрешающей способности арифметики с фиксированной запятой, конкуренции в использовании ресурсов, наихудшего случая с точки зрения времени счета, обработки исключительных операций, использования неинициализированных переменных или констант, неиспользуемых переменных или констант, а также нарушение целостности из-за конфликтов задач или прерываний) (уровень A*, B, C)	6.3.4f A-1 № 6	
2.10.4	Рассмотренные материалы показывают, что использованные в проверках средства технически правильны и достаточны (см. Приложение 2)	6.1e 12.2	
2.10.5	Недостатки и ошибки, выявленные в процессе верификации ПО, передаются в процессы разработки ПО для внесения ясности и исправлений	6.2e	
2.11	Достигнуты относящиеся цели процесса управления конфигурацией ПО	7.1, табл. A-8	
2.11.1	«Протоколы УКПО» показывают, что единицы конфигурации идентифицированы	7.2.1 A-8 № 1	
2.11.2	«Протоколы УКПО» показывают, что базовые версии и трассируемость установлены	7.2.2 A-8 № 2	
2.11.3	«Протоколы УКПО» и «Сообщения о проблемах» показывают, что порядок сообщений о проблемах, управления изменениями, рассмотрения изменений и учета состояния конфигурации установлен	7.2.3 7.2.4 7.2.5 7.2.6 A-8 № 3	
2.11.4	«Протоколы УКПО» показывают, что порядок архивирования, воспроизведения и выпуска установлен	7.2.7 A-8 № 4	
2.11.5	«Протоколы УКПО» и «Каталог среды жизненного цикла ПО» показывают, что установлен контроль за средой жизненного цикла ПО	7.2.9 A-8 № 6	
2.12	Достигнуты относящиеся цели процесса гарантии качества ПО	8.1, табл. A-9	
2.12.1	«Протоколы ГКПО» гарантируют, что процессы разработки ПО и интегральные процессы соответствуют утвержденным планам и стандартам	8.1a A-9 № 1	
2.12.2	«Протоколы ГКПО» гарантируют, что критерии перехода для процессов жизненного цикла ПО удовлетворяются (уровень A, B)	8.1b A-9 № 2	
2.13	Достигнуты относящиеся цели процесса взаимодействия Заявителя и Сертифицирующего органа	9, табл. A-10	
2.13.1	Обоснование соответствия приведено	9.2 A-10 № 3	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
2.14	Процессы, рассмотренные в ходе проверки, понятны персоналу и соблюдались в ходе разработки (по результатам бесед)	1.1	
3	**Верификация**		
3.1	«Примеры и процедуры верификации ПО» надлежаще выполнены	6.2	
3.1.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1 (уровень A, B) или 2 (уровень C, D)	9.2c, табл. A-6	
3.1.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
3.1.3	Документ имеет надлежащее содержание	11.13	
3.1.3.1	В документе содержатся процедуры рассмотрения и анализа (подробные сведения, дополняющие «План верификации ПО»)	11.13a	
3.1.3.2	Предусмотрен анализ покрытия требований к ПО для определения того, какие требования не были испытаны	6.4c	
3.1.3.2.1	При выполнении анализа предусмотрена демонстрация того, что для каждого требования к ПО есть тестовые примеры	6.4.4.1a	
3.1.3.2.2	При выполнении анализа предусмотрена демонстрация того, что тестовые примеры удовлетворяют критериям нормальных и робастных испытаний	6.4.4.1b	
3.1.3.3	Предусмотрен анализ структурного покрытия для определения того, какие программные структуры не были проверены (уровень A, B, C)	6.4d	
3.1.3.3.1	При выполнении анализа подтверждается степень структурного покрытия, соответствующая уровню ПО	6.4.4.2a	
3.1.3.3.2	Предусмотрено выполнение структурного анализа покрытия с использованием объектного кода (уровень A и в случае если компилятор генерирует объектный код, который не трассируется прямо на операторы «Исходного кода») или по «Исходному коду»	6.4.4.2b	
3.1.3.3.3	При выполнении структурного анализа подтверждается связь между компонентами кода по данным и по управлению	6.4.4.2c	
3.1.3.4	В документе содержатся тестовые примеры (приведено назначение каждого тестового примера, набор входов, условий, ожидаемых результатов, критерий «проходит/не проходит»)	11.13b	
3.1.3.4.1	Тестовые примеры разработаны, главным образом на основе требований к ПО	6.4a	
3.1.3.4.2	Разработка тестовых примеров проведена таким образом, что обеспечены проверка правильности функционирования и определение условий, при которых проявляются ошибки	6.4b	
3.1.3.4.3	Предусмотрены две категории тестовых примеров: тестовые примеры в допустимом диапазоне и робастные тестовые примеры (вне допустимого диапазона)	6.4.2a	
3.1.3.4.4	Разработаны специальные тестовые примеры на основе требований к ПО и с учетом источников ошибок, присущих процессам разработки ПО	6.4.2b	
3.1.3.4.5	Разработаны тестовые примеры для проверки действительных и целых входных переменных с использованием достоверных классов эквивалентности и граничных значений	6.4.2.1a	
3.1.3.4.6	Разработаны тестовые примеры с многократным исполнением кода для проверки характеристик динамических функций (фильтры, интегрирующие звенья, задержки и т.п.)	6.4.2.1b	
3.1.3.4.7	Разработаны тестовые примеры для проверки переходов, возможных при нормальной работе (при использовании «состояний/переходов»)	6.4.2.1c	
3.1.3.4.8	Разработаны тестовые примеры для проверки в допустимом диапазоне использования переменных и булевых операторов (для требований, сформулированных в виде логических уравнений)	6.4.2.1d	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
3.1.3.4.9	Разработаны тестовые примеры для проверки действительных и целых переменных, при этом использовался выбор классов эквивалентности недопустимых значений	6.4.2.2a	
3.1.3.4.10	Разработаны тестовые примеры для проверки инициализации системы при ненормальных условиях	6.4.2.2b	
3.1.3.4.11	Определены возможные виды отказов входных данных, поступающих от внешних систем, и разработаны тестовые примеры для проверки работы ПО	6.4.2.2c	
3.1.3.4.12	Для циклов, заданное повторение которых является вычисляемой величиной, разработаны тестовые примеры, в которых делается попытка вычислить заданное количество повторений, выходящее за пределы допустимого диапазона	6.4.2.2d	
3.1.3.4.13	Разработаны тестовые примеры для проверки механизма защиты от выхода за установленное время счета	6.4.2.2e	
3.1.3.4.14	Для динамических звеньев (фильтры, интегрирующие звенья, запаздывания и т.п.) разработаны тестовые примеры для проверки механизмов защиты от арифметического переполнения	6.4.2.2f	
3.1.3.4.15	Разработаны тестовые примеры для воспроизведения переходов, не допустимых в соответствии с требованиями к ПО (при использовании «состояний/переходов»)	6.4.2.2g	
3.1.3.5	В документе содержатся процедуры испытаний (пооперационные инструкции относительно: подготовки и проведения испытаний по каждому тестовому примеру, оценки результатов испытаний, применения испытательного оборудования)	11.13c	
3.1.3.5.1	Описаны процедуры ряда испытаний, проводимых в интегрированной среде целевого вычислителя	6.4.1a	
3.1.3.5.2	Описаны процедуры испытаний интеграции аппаратных средств и ПО на основе требований	6.4.3a	
3.1.3.5.3	Описаны процедуры испытаний интеграции ПО на основе требований	6.4.3b	
3.1.3.5.4	Описаны процедуры испытаний на основе требований низкого уровня (уровень A, B, C)	6.4.3c	
3.2	«Результаты верификации ПО» надлежаще выполнены	6.2	
3.2.1	Документ имеет надлежащее состояние и отнесен к категории контроля 2	9.2c, табл. A-6	
3.2.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
3.2.3	Документ имеет надлежащее содержание	11.14	
3.2.3.1	В документе содержатся результаты каждого рассмотрения, анализа, испытания, показывающие для каждой процедуры, проходит она или не проходит, а также общий результат «проходит/не проходит»	11.14a	
3.2.3.2	В документе содержится идентификация единиц конфигурации или версий ПО, которые проходили рассмотрение, анализ или испытание	11.14b	
3.2.3.3	В документе содержатся результаты испытаний, рассмотрений и анализов, включая анализ покрытия и анализ трассируемости	11.14c	
3.2.4	Продемонстрированные испытания корректно отражены в документе	9.2	
3.3	«Каталог среды жизненного цикла ПО» надлежаще выполнен (см. 2.5)	7.2.9	
3.4	«Каталог комплектации ПО» надлежаще выполнен	9.2b	
3.4.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1	9.2c, табл. A-10	
3.4.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
3.4.3	Документ имеет надлежащее содержание	11.16	
3.4.3.1	В документе идентифицирован программный продукт	11.16a	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
3.4.3.2	В документе идентифицирован «Исполняемый объектный код»	11.16b	
3.4.3.3	В документе идентифицирован каждый компонент «Исходного кода»	11.16c	
3.4.3.4	В документе идентифицировано ранее разработанное ПО, входящее в состав программного продукта, если таковое имеется	11.16d	
3.4.3.5	В документе идентифицированы документы жизненного цикла ПО	11.16e	
3.4.3.6	В документе идентифицированы носители для архивации и выпуска	11.16f	
3.4.3.7	В документе идентифицированы инструкции по генерации «Исполняемого объектного кода» (инструкции и данные для компиляции и редактирования связей; процедуры, используемые для воспроизведения программного обеспечения при его повторной генерации, испытании или модификации, и т.п.)	11.16g	
3.4.3.8	В документе идентифицирована ссылка на «Каталог среды жизненного цикла ПО», если он скомплектован отдельно	11.16h	
3.4.3.9	В документе идентифицированы данные проверки целостности «Исполняемого объектного кода», если они используются	11.16i	
3.5	«Сообщения о проблемах» надлежаще выполнены (см. 2.6)	11.17	
3.6	«Протоколы УКПО» надлежаще выполнены (см. 2.7)	11.18	
3.7	«Протоколы ГКПО» надлежаще выполнены (см. 2.8)	11.19	
3.8	Достигнуты относящиеся цели процессов разработки ПО	5.4.1, табл. A-2	
3.8.1	Рассмотренные материалы показывают, что «Исполняемый объектный код» загружается в целевой вычислитель для интеграции ПО и аппаратных средств	5.4.1a A-2 № 7	
3.8.1.1	«Исполняемый объектный код» генерируется из «Исходного кода» и данных для редактирования связей и загрузки данных	5.4.2a	
3.8.1.2	Для интеграции ПО и аппаратных средств программное обеспечение загружается в целевой вычислитель	5.4.2b	
3.8.1.3	Недостаточные и неправильные входные данные, выявленные в процессе интеграции, возвращаются в процесс разработки требований к ПО, в процесс проектирования ПО, процесс кодирования или в процесс планирования создания ПО для внесения ясности и поправок	5.4.2c	
3.8.1.4	Предоставлено достаточное доказательство того, что в условиях, для которых это не предусмотрено, отключенная программа не будет выполняться	5.4.3a	
3.8.1.5	Методы обращения с отключенными программами соответствуют указаниям, изложенным в планах создания ПО	5.4.3b	
3.8.1.6	«Заплаты» используются в ограниченных конкретно рассматриваемых случаях	5.4.3c	
3.8.1.7	При использовании «заплат»: процесс управления конфигурацией ПО позволяет отслеживать каждую «заплату»; проведен регрессивный анализ, доказывающий, что «заплата» удовлетворяет всем целям ПО, разработанного принятыми методами	5.4.3d	
3.9	Достигнуты относящиеся цели процесса верификации ПО	6.1	
3.9.1	Рассмотренные материалы показывают, что «Исполняемый объектный код» удовлетворяет требованиям к ПО	6.1d, табл. A-5, A-6, A-7	
3.9.1.1	Интеграция ПО завершена и выполнена правильно (уровень A, B, C)	6.3.5 A-5 № 7	
3.9.1.1.1	При выполнении проверки данных редактирования связей и загрузки и карты распределения памяти рассмотрены неправильные адреса аппаратных средств	6.3.5a	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
3.9.1.1.2	При выполнении проверки данных редактирования связей и загрузки и карты распределения памяти рассмотрены перекрытия областей памяти	6.3.5b	
3.9.1.1.3	При выполнении проверки данных редактирования связей и загрузки и карты распределения памяти рассмотрены потерянные компоненты ПО	6.3.5c	
3.9.1.2	Процедуры испытаний корректны (на основе тестовых примеров правильно подготовлены тестовые процедуры и ожидаемые результаты) (уровень A*, B, C)	6.3.6b A-7 № 1	
3.9.1.3	Результаты испытаний корректны, расхождения между действительными и ожидаемыми результатами объяснены (уровень A*, B, C)	6.3.6c A-7 № 2	
3.9.1.4	Покрытие требований высокого уровня по результатам испытаний достигается (уровень A*, B, C, D)	6.4.4.1 A-7 № 3	
3.9.1.4.1	Выполненный анализ тестовых покрытий на основе требований показывает, что для каждого требования высокого уровня есть тестовые примеры	6.4.4.1a	
3.9.1.4.2	Выполненный анализ тестовых покрытий на основе требований показывает, что тестовые примеры удовлетворяют критериям нормальных и робастных испытаний	6.4.4.1b	
3.9.1.5	«Исполняемый объектный код» удовлетворяет требованиям высокого уровня	6.4.2.1 6.4.3 A-6 № 1	
3.9.1.6	«Исполняемый объектный код» является робастным по отношению к требованиям высокого уровня	6.4.2.2 6.4.3 A-6 № 2	
3.9.1.7	Покрытие требований низкого уровня по результатам испытаний достигается (уровень A*, B, C)	6.4.4.1 A-7 № 4	
3.9.1.7.1	Выполненный анализ тестовых покрытий на основе требований показывает, что для каждого требования низкого уровня есть тестовые примеры	6.4.4.1a	
3.9.1.7.2	Выполненный анализ тестовых покрытий на основе требований показывает, что тестовые примеры удовлетворяют критериям нормальных и робастных испытаний	6.4.4.1b	
3.9.1.8	Рассмотренные материалы показывают, что «Исполняемый объектный код» удовлетворяет требованиям низкого уровня (уровень A*, B, C)	6.4.2.1 6.4.3 A-6 № 3	
3.9.1.9	Рассмотренные материалы показывают, что «Исполняемый объектный код» является робастным по отношению к требованиям низкого уровня (уровень A*, B, C)	6.4.2.2 6.4.3 A-6 № 4	
3.9.1.10	Рассмотренные материалы показывают, что покрытие структуры программы (модифицированное покрытие условий/решений) по результатам испытаний достигается (уровень A*)	6.4.4.2 A-7 № 5	
3.9.1.11	Рассмотренные материалы показывают, что покрытие структуры программы (покрытие решений) по результатам испытаний достигается (уровень A*, B*)	6.4.4.2a 6.4.4.2b A-7 № 6	
3.9.1.12	Рассмотренные материалы показывают, что покрытие структуры программы (покрытие операторов) по результатам испытаний достигается (уровень A*, B, C)	6.4.4.2a 6.4.4.2b A-7 № 7	
3.9.1.13	Рассмотренные материалы показывают, что покрытие структуры программы (связи по данным и управлению) по результатам испытаний достигается (уровень A*, B, C)	6.4.4.2c A-7 № 8	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
3.9.1.14	Рассмотренные материалы показывают, что «Исполняемый объектный код» совместим с целевым вычислителем (уровень A*, B, C)	6.4.3a A-6 № 5	
3.9.2	Рассмотренные материалы показывают, что использованные в проверках средства технически правильны и достаточны	6.1e 12.2	
3.9.3	Недостатки и ошибки, выявленные в процессе верификации ПО, передаются в процессы разработки ПО для внесения ясности и исправлений	6.2e	
3.10	Достигнуты относящиеся цели процесса управления конфигурацией ПО	7.1, табл. A-8	
3.10.1	«Протоколы УКПО» показывают, что единицы конфигурации идентифицированы	7.2.1 A-8 № 1	
3.10.2	«Протоколы УКПО» показывают, что базовые версии и трассируемость установлены	7.2.2 A-8 № 2	
3.10.3	«Протоколы УКПО» и «Сообщения о проблемах» показывают, что порядок сообщений о проблемах, управления изменениями, рассмотрения изменений и учета состояния конфигурации установлен	7.2.3 7.2.4 7.2.5 7.2.6 A-8 № 3	
3.10.4	«Протоколы УКПО» показывают, что порядок архивирования, воспроизведения и выпуска установлен	7.2.7 A-8 № 4	
3.10.5	«Протоколы УКПО» показывают, что контроль загрузки ПО установлен	7.2.8 A-8 № 5	
3.10.6	«Протоколы УКПО» и «Каталог среды жизненного цикла ПО» показывают, что установлен контроль за средой жизненного цикла ПО	7.2.9 A-8 № 6	
3.11	Достигнуты относящиеся цели процесса гарантии качества ПО	8.1, табл. A-9	
3.11.1	«Протоколы ГКПО» гарантируют, что процессы разработки ПО и интегральные процессы соответствуют утвержденным планам и стандартам	8.1a A-9 № 1	
3.11.2	«Протоколы ГКПО» гарантируют, что критерии перехода для процессов жизненного цикла ПО удовлетворяются (уровень A, B)	8.1b A-9 № 2	
3.12	Достигнуты относящиеся цели процесса взаимодействия Заявителя и Сертифицирующего органа	9, табл. A-10	
3.12.1	Обоснование соответствия приведено	9.2 A-10 № 3	
4	**Завершение**		
4.1	«Протокол ГКПО» о выполнении «Рассмотрения соответствия ПО требованиям» надлежаще выполнен	8.2g	
4.1.1	Документ имеет надлежащее состояние и отнесен к категории контроля 2	9.2c, табл. A-9	
4.1.2	Документ показывает, что «Рассмотрение соответствия ПО требованиям» достигло установленной цели	8.3	
4.1.2.1	Запланированные для получения сертификационного зачета мероприятия жизненного цикла ПО, включая подготовку пакета данных жизненного цикла ПО, завершены и протоколы об их завершении сохраняются	8.3a	
4.1.2.2	Данные жизненного цикла ПО, разработанные на основании конкретных требований к системе, требований по безопасности или требований к ПО, трассируемы на эти требования	8.3b	
4.1.2.3	Данные жизненного цикла ПО соответствуют планам и стандартам и находятся под контролем в соответствии с «Планом УКПО»	8.3c	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178B	Оценка (√ / ?)
4.1.2.4	«Сообщения о проблемах» соответствуют «Плану УКПО», оценены, их статус зарегистрирован	8.3d	
4.1.2.5	Отступления от требований к ПО зарегистрированы и утверждены	8.3e	
4.1.2.6	«Исполняемый объектный код» может быть повторно сгенерирован из хранящегося в архиве «Исходного кода»	8.3f	
4.1.2.7	Утвержденное ПО может быть успешно загружено с использованием выпущенных инструкций	8.3g	
4.1.2.8	«Сообщения о проблемах», отложенные по результатам предыдущих рассмотрений соответствия ПО требованиям, повторно оценены для определения их статуса	8.3h	
4.1.2.9	При использовании ранее разработанного ПО настоящая базовая версия программного продукта трассируема с предыдущей базовой версией и с утвержденными изменениями для этой базовой версии	8.3i	
4.2	«Каталог среды жизненного цикла ПО» надлежаще выполнен (см. 2.5)	7.2.9	
4.3	«Каталог комплектации ПО» надлежаще выполнен (см. 3.4)	9.2b	
4.4	«Итоговое заключение о ПО» надлежаще выполнено	9.2b	
4.4.1	Документ имеет надлежащее состояние и отнесен к категории контроля 1	9.2c	
4.4.2	Документ имеет надлежащие характеристики (см. 1.1.2)	11	
4.4.3	Документ имеет надлежащее содержание	11.20	
4.4.3.1	Приведено обзорное описание системы и указаны все отличия от обзорного описания системы, приведенного в «Плане сертификации ПО»	11.20a	
4.4.3.2	Приведено обзорное описание ПО и указаны все отличия от обзорного описания ПО, приведенного в «Плане сертификации ПО»	11.20b	
4.4.3.3	Дана сводка сертификационных аспектов ПО, установлен уровень ПО, приведено его обоснование, полученное в процессе анализа безопасности полета при отказах системы, и указаны все отличия от сертификационных аспектов в «Плане сертификации ПО»	11.20c	
4.4.3.4	Приведены характеристики ПО (объем «Исполняемого объектного кода», запасы по быстродействию и объему памяти, ограничения по ресурсам) и способы измерения каждой из характеристик	11.20d	
4.4.3.5	Дано обобщенное описание действительно выполненного жизненного цикла ПО и объяснены отличия от цикла и его процессов, предложенных в «Плане сертификации ПО»	11.20e	
4.4.3.6	Указаны документы жизненного цикла ПО, подготовленные в процессах разработки ПО и интегральных процессах; описана взаимосвязь этих документов между собой и с другими документами, определяющими систему; описаны все отличия от «Плана сертификации ПО»	11.20f	
4.4.3.7	Описаны дополнительные соображения по сертификационным вопросам и указаны документы, им посвященные	11.20g	
4.4.3.8	Указана конфигурация программного обеспечения в виде его маркировочного номера и версии	11.20h	
4.4.3.9	Дана сводка изменений в процессах жизненного цикла ПО, имевших место после предыдущей сертификации	11.20i	
4.4.3.10	Приведена сводка сообщений о проблемах, по которым на момент сертификации не приняты решения, и указаны ограничения на выполняемые функции	11.20j	

№ п/п	Характеристика процесса создания ПО	Пункт КТ-178В	Оценка (√ / ?)
4.4.3.11	Приведена констатация соответствия КТ-178В и дана сводка методов, использованных для демонстрации соответствия критериям, указанным в планах создания ПО; рассмотрены дополнительные правила и отступления от планов создания ПО, стандартов и КТ-178В	11.20k	
4.4.3.12	Приведены сведения по квалификации использованных инструментов разработки и верификации ПО	12.2.4	
4.5	Достигнуты все цели процессов создания программного обеспечения	9.2 А-10 № 3	
4.5.1	Устранены замечания, изложенные в Актах аудиторских проверок	9.2a	
4.5.2	Открытые вопросы в сообщениях о проблеме не влияют на безопасность и эксплуатацию системы	9.2a	
4.5.3	Все рассмотренные документы жизненного цикла ПО надлежаще оформлены и подтверждают достижение целей процессов жизненного цикла ПО	9.2b 9.2c	
4.6	Получили положительную оценку все рассмотренные ранее характеристики процесса создания ПО	9.2	

Руководитель группы < Ф.И.О. >

От ГосНИИ «Аэронавигация» От ЛИИ им. М.М. Громова

gost.e-ecolog.ru