ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 27.016— 2020 (МЭК 62853:2018)

Надежность в технике

НАДЕЖНОСТЬ ОТКРЫТЫХ СИСТЕМ

(IEC 62853:2018, Open systems dependability, MOD)

Издание официальное

Москва
Стандартинформ
2020

Предисловие

1 ПОДГОТОВЛЕН Закрытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (ЗАО «НИЦ КД») на основе собственного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 119 «Надежность в технике»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 6 августа 2020 г. № 472-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту МЭК 62853:2018 «Надежность открытых систем» (IEC 62853:2018 «Open systems dependability», MOD) путем внесения технических отклонений, объяснение которых приведено во введении к настоящему стандарту.

Международный стандарт разработан Техническим комитетом МЭК 56.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Открытой системой является система, границы, функции и структура которой изменяются в процессе жизненного цикла, которую распознают и описывают по-разному в зависимости от точки зрения. Надежность открытой системы является ключевым понятием жизненного цикла системы, которая находится в эксплуатации в реальных условиях продолжительный период времени. Надежность открытых систем позволяет учесть способность открытых систем адаптироваться к изменениям в целях, задачах, окружающей среде, фактическом функционировании и непрерывно поддерживать ответственность заинтересованных сторон за представление ожидаемых услуг в соответствии с установленными требованиями. Свойства надежности (готовность, безотказность, ремонтопригодность) и обеспечение технического обслуживания одинаковы для открытых и обычных систем, но необходимо учитывать, что ни одна заинтересованная сторона не имеет полного понимания системы и соответствующего ей риска.

Для открытых систем безопасность особенно важна, так как такие системы подвержены атакам вредоносного программного обеспечения. Поскольку открытая система постоянно изменяется в течение срока службы, процесс проектирования, описываемый, например, адаптивной моделью разработки продукции, продолжается в течение всего срока службы системы.

Настоящий стандарт детализирует требования *ГОСТ Р МЭК 60300-1*, поскольку устанавливает дополнительное руководство по менеджменту надежности открытых систем.

В настоящем стандарте приведено руководство по надежности открытых систем, основанное на четырех видах анализа процесса, каждый из которых выбирает и объединяет процессы, действия и задачи жизненного цикла системы в соответствии с *[1]*:

- анализ процесса адаптации изменений;
- анализ процесса обеспечения ответственности;
- анализ процесса реагирования на отказ;
- анализ процесса достижения консенсуса.

Проведение перечисленных видов анализа процесса является крайне важным для понимания проблемы заинтересованными сторонами и согласования границ их ответственности, а также при определении отчетности за выполнение изменений и управление изменениями для обеспечения надежности открытых систем.

Пользователями настоящего стандарта могут быть работники, владельцы и потребители организаций, ответственных за обеспечение выполнения требований к надежности открытых систем. Это могут быть организации всех видов и размеров, частные и государственные организации, такие как государственные органы, коммерческие и некоммерческие ассоциации.

В настоящем стандарте ссылки на международные стандарты заменены ссылками на национальные стандарты.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Надежность в технике

НАДЕЖНОСТЬ ОТКРЫТЫХ СИСТЕМ

Dependability in technics. Open systems dependability

Дата введения — 2021—07—01

1 Область применения

В настоящем стандарте установлено руководство по определению требований к жизненному циклу открытой системы для обеспечения ее надежности.

В настоящем стандарте детализированы требования *ГОСТ Р МЭК 60300-1* по отношению к открытым системам. В настоящем стандарте определены виды анализа процесса на основании требований *[1]*, где идентифицирован набор процессов жизненного цикла системы.

Настоящий стандарт применим к стадиям жизненного цикла продукции, систем, процессов или услуг, включая аппаратные средства, программные средства и человеческий фактор или их комбинации.

Для открытых систем особенно важна безопасность, так как эти системы подвержены неблагоприятным воздействиям.

Настоящий стандарт может быть использован для повышения надежности открытых систем и обеспечения уверенности в том, что анализ процесса открытой системы соответствует ожидаемым результатам. Настоящий стандарт может помочь организации определить деятельность и задачи, которые должны быть выполнены для достижения целей в области надежности открытой системы, включая обмен информацией о надежности, оценку и сопоставление показателей надежности на всех стадиях жизненного цикла системы.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 27.002 Надежность в технике. Термины и определения

ГОСТ IEC 61000-4-30 Электромагнитная совместимость (ЭМС). Часть 4-30. Методы испытаний и измерений. Методы измерений качества электрической энергии

ГОСТ Р 27.003 Надежность в технике. Управление надежностью. Руководство по заданию технических требований к надежности

ГОСТ Р 27.014 (МЭК 62347) Надежность в технике. Управление надежностью. Руководство по установлению требований к надежности систем

ГОСТ Р 27.302 Надежность в технике. Анализ дерева неисправностей

ГОСТ Р ИСО 15489-1 Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы

ГОСТ Р ИСО 26000 Руководство по социальной ответственности

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р ИСО/МЭК 31010 Менеджмент риска. Методы оценки риска

ГОСТ Р 51897 Менеджмент риска. Термины и определения

ГОСТ Р 51901.12 (МЭК 60812) Менеджмент риска. Метод анализа видов и последствий отказов

ГОСТ Р 51901.14 (МЭК 61078:2006) Менеджмент риска. Структурная схема надежности и булевы методы

Издание официальное

ГОСТ Р 56923/ISO/IEC TR 24748-3:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 3. Руководство по применению ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

ГОСТ Р 57098/ISO/IEC TR 24774 Системная и программная инженерия. Управление жизненным циклом. Руководство для описания процесса

ГОСТ Р 57100/ISO/IEC/IEEE 42010 Системная и программная инженерия. Описание архитектуры

ГОСТ Р 57102/ISO/IEC TR 24748-2:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 2. Руководство по применению ИСО/МЭК 15288

ГОСТ Р 58607/ISO/IEC/IEEE 24748-4:2016 Системная и программная инженерия. Управление жизненным циклом. Часть 4. Планирование системной инженерии

ГОСТ Р МЭК 60300-1 Менеджмент риска. Руководство по применению менеджмента надежности (МЭК 60300-1 Менеджмент надежности. Часть 1. Руководство по управлению и применению)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины *по ГОСТ 27.002*, *ГОСТ Р 51897* и *[2]*, а также следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации по следующим адресам:

- МЭК Electropedia: доступна на http://www.electropedia.org/;
- ИСО, Интернет-онлайн-платформа: доступна на http://www.iso.org/obp.

3.1 **ответственность (подотчетность)** (accountability): Состояние ответственности за решения и деятельность перед руководящими органами организации, правовыми органами и заинтересованными сторонами организации.

Примечание 1 — Ответственность включает ответственность перед обществом в целом.

Примечание 2 — В соответствии с *ГОСТ Р ИСО 26000*: Ответственность включает обязательства со стороны руководства быть ответственным перед лицами, контролирующими организацию, за выполнение организацией правовых и обязательных требований. Ответственность за общее воздействие решений и действий организации на общество и окружающую среду также подразумевает ответственность организации за нарушения в результате ее решений и действий перед обществом в целом в зависимости от вида воздействий и обстоятельств.

Примечание 3 — Определение по *ГОСТ Р ИСО 15489-1*: Принцип, в соответствии с которым частные лица, организации и общество ответственны за свои действия.

3.2 **гарантийный случай, случай гарантии** (assurance case): Создаваемый обоснованный проверяемый артефакт, подтверждающий, что удовлетворяется претензия верхнего уровня (или совокупность претензий), включая поддерживающие претензию систематическую аргументацию и ее явные предположения.

Примечание 1 — В гарантийный случай входят следующие составляющие и их отношения:

- одна или более претензий по свойствам;
- аргументы, которые логически связывают доказательство и любые предположения с претензией или претензиями;
- доказательная база и, возможно, предположения, поддерживающие эти аргументы для претензии (претензий);
- обоснование выбора претензии верхнего уровня и метода доказательства.

Примечание 2 — Гарантийный случай можно рассматривать как обоснованный убедительный аргумент, подкрепленный свидетельством того, что система, услуга или организация будут функционировать в соответствии с назначением конкретным применением в заданных условиях в течение установленного срока службы.

3.3 **аккомодация изменений** (change accommodation): Набор действий, которые модифицируют и адаптируют систему в соответствии с изменениями ее целей, задач, окружающей среды или фактической работы, которые требуют в отношении системы установления нового перечня заинтересованных сторон.

3.4 **консенсус** (consensus): Общее согласие, характеризующееся отсутствием серьезных возражений по существенным вопросам у большинства заинтересованных сторон и достигаемое в результате процедуры, направленной на учет мнений всех сторон и сближение несовпадающих точек зрения.

Примечание 1 — Консенсус не обязательно подразумевает полное единодушие.

3.5 **свидетельства надежности** (dependability case): Основанные на фактах аргументированные, прослеживаемые доводы в поддержку утверждения о том, что система удовлетворяет или будет удовлетворять требованиям к надежности.

Примечание 1 — Свидетельства надежности являются гарантийным случаем, в котором заявление высшего уровня относится к надежности.

3.6 **обмен информацией о надежности** (dependability communication): Непрерывный итеративный процесс, который выполняет заинтересованная сторона для обеспечения, выделения или получения информации и участия в диалоге с другими заинтересованными сторонами в отношении менеджмента надежности.

Примечание 1 — Обмен информацией о надежности в менеджменте надежности открытой системы мало чем отличается от обмена информацией о риске в менеджменте риска.

Примечание 2 — См. определение «обмен информацией и консультации» в *ГОСТ Р 51897*.

3.7 **окружающая среда (системы)** (environment): Условия, определяющие окружающую обстановку и детали всех воздействий на систему.

3.8 **реагирование на отказ** (failure response): Совокупность действий, незамедлительно осуществляемых при прогнозировании или обнаружении отказа, с целью предотвращения отказа или снижения его воздействия, а также для анализа причин отказа, предотвращения их повторного появления и подготовки необходимых отчетов.

3.9 **структура исходных сведений** (frame of reference): Набор правил для формирования, интерпретации и использования документов, описывающих общее понимание и четкие соглашения о системе, ее цели, задачах, окружающей среде, фактической работе, жизненном цикле и их изменениях.

3.10 **ошибка взаимодействия** (interaction error): Ошибка, которая происходит при взаимодействии объектов, несмотря на то что функционирование каждого объекта соответствует установленным требованиям.

3.11 **мониторинг** (monitoring): Определение состояния системы, процесса или деятельности.

Примечание — При определении состояния может возникнуть необходимость в проведении проверки, наблюдения или глубокого изучения.

3.12 **открытая система** (open system): Система, границы, функции и структура которой изменяются во времени, по-разному распознаваемая и описываемая с различных точек зрения.

Примечания

1 Изменения включают не только адаптацию с определенной целью, но также и непосредственное развитие. Например, эти изменения включают непосредственные и нескоординированные изменения внутри системы, которые охватывают несколько областей с различным руководством.

2 Границы, функции и структура открытой системы не только изменяются во времени, но могут быть неопределенными в любой момент времени, их по-разному распознают различные заинтересованные стороны. Это уточняет определение системы в *[2]* для данного уровня абстракции и данной точки зрения. Границы могут быть четко определены на одном уровне абстракции, но они могут стать более неопределенными на более детальном уровне. Уровень детализации, необходимый для данной цели или заинтересованной стороны, может быть заранее не предопределен и не обязательно достижим.

3 Открытая система обменивается ресурсами через свои границы с другими системами или окружающей средой, при этом возможно изменение границ системы.

4 У каждой существующей системы имеются аспекты и открытой системы, и обычной системы. Термин «открытая система» не используют для классификации систем. Термин применяют к системе, когда ее аспекты открытой системы являются существенными в данный момент.

5 Тот факт, что программное обеспечение системы может быть «открытым», не важен для признания системы открытой, за исключением того, что общедоступное программное обеспечение обязательно включает аспекты открытых систем, так же как и отсутствие централизованного управления.

3.13 **надежность открытых систем** (open system dependability): Способность системы адаптироваться к изменениям в целях, задачах, среде, фактическом функционировании и непрерывно обеспечивать ответственность за выполнение ожидаемых функций, как и когда это требуется.

3.14 **процесс** (process): Совокупность взаимосвязанных и (или) взаимодействующих видов деятельности, использующих входы для получения намеченного результата.

Примечания

1 В зависимости от контекста «намеченный результат» называется выходом, продукцией или услугой.

2 Входами для процесса обычно являются выходы других процессов, а выходы процессов обычно являются входами для других процессов.

3 Два или более взаимосвязанных и взаимодействующих процессов совместно могут также рассматриваться как процесс.

4 Процессы в организации, как правило, планируются и осуществляются в управляемых условиях с целью добавления ценности.

5 Процесс, в котором подтверждение соответствия конечного выхода затруднено или экономически нецелесообразно, часто называют «специальным процессом».

6 Термин является одним из числа общих терминов и определений для стандартов ИСО на системы менеджмента, приведенных в приложении SL к Сводным дополнениям ИСО Директив ИСО/МЭК, часть 1. Исходное определение изменено; добавлены примечания 1—5 для разграничения понятий «процесс» и «выход».

3.15 **анализ процесса** (process view): Набор процессов, действий и задач, который обеспечивает ориентацию на конкретную озабоченность заинтересованных сторон в отношении системы таким способом, что охватывает весь жизненный цикл системы или его части.

3.16 **устойчивость организации** (resilience): Способность организации к адаптации в сложной и изменяющейся окружающей среде.

Примечания

1 Определение устойчивости в *[3]*: Способность системы, сообщества или общества, подверженных угрозам, противостоять последствиям угроз, переносить их, приспосабливаться к ним и восстанавливаться своевременно и эффективно, в том числе посредством сохранения и восстановления своих основополагающих структур и функций.

2 Определение в *[4]*: Постоянство предоставления услуг, которому можно оправданно доверять при изменениях.

3.17 **заинтересованная сторона** (stakeholder): Лицо или организация, которые могут воздействовать на осуществление деятельности или принятие решения, быть подверженными их воздействию или воспринимать себя в качестве последних.

Пример — Потребители, владельцы, работники в организации, поставщики, банкиры, регулирующие органы, союзы, партнеры или сообщество, которое может включать конкурентов или группы противодействия.

Примечания

1 Некоторые заинтересованные стороны могут иметь интересы, противоречащие интересам других сторон или системы.

2 Термин является одним из числа общих терминов и определений для стандартов ИСО на системы менеджмента.

4 Надежность открытых систем

4.1 Открытые системы

Открытые системы имеют следующие характеристики *[5]*.

- Открытые системы являются большими, сложными со сложными внутренними взаимосвязями.
- Открытые системы могут включать компоненты, представляемые в виде черного ящика.

Примечание 1 — Компонент, представляемый в виде черного ящика, — компонент, пользователи которого не знают деталей его работы, не могут управлять его функциями и взаимодействиями.

- Цели, задачи, окружающая среда и фактическое функционирование открытых систем не определены и изменяются в течение жизненного цикла. Непрогнозируемые изменения требований пользователей, целей обслуживания, общепризнанных услуг, полученных через сети компонентов черного ящика, технологической базы и т. д. являются обычными.

- Границы, функции и структура открытых систем постоянно развиваются, их по-разному воспринимают различные заинтересованные стороны. Для устранения неясности в их определении необходимы дополнительные усилия.

- Ответственность жизненно важна на всех этапах жизненного цикла системы и для контроля риска, при этом необходимы усилия для установления ответственности из-за отсутствия эффективного централизованного управления системой.

- Понимание заинтересованными сторонами системы и ее риска в любой момент времени не является ни полным, ни определенным.

- Возможность отказов из-за неполного понимания системы, непредвиденных событий и изменений не может быть устранена или спрогнозирована. Система должна быть гибкой, обеспечена средствами контроля риска, включая выявление ошибок, должна быть восстанавливаемой после отказов и адаптируемой для предупреждения их повторного появления.

- Обеспечение надежности требует применения итеративного подхода и зависит от эксплуатации и разработки системы. Выполнение действий надежности на всех этапах жизненного цикла системы и их итерация так часто, как это необходимо, особенно важны для открытых систем.

Примечание 2 — Некоторые из этих особенностей открытой системы присущи так называемой «системе систем» *[6]*, *[7]* и «неограниченным или слабо ограниченным системам».

Примечание 3 — Большая часть систем имеет такие особенности в той или иной степени. Система является открытой, если эти особенности системы являются существенными для работы в данный момент, независимо от того, является ли она системой систем.

Система обязательно обменивается различными функциями с другими связанными, независимо управляемыми системами. Управление этими окружающими системами подчиняется принципам и требованиям заинтересованных сторон, и взаимодействия с ними подвержены изменениям по различным причинам. Система должна служить разнообразным заинтересованным сторонам. У каждой заинтересованной стороны есть свои цели, единого органа управления системой может не быть; кроме того, цели основной системы и окружающих систем изменяются во времени. Условия работы системы, такие как требования и ограничения, изменяются часто и непредсказуемо. Таким образом, этим системам присущи неопределенность и неполнота этих условий, в каждый момент времени они не могут быть полностью поняты.

Так как открытая система непрерывно изменяется на всех этапах жизненного цикла, процесс проектирования, построенный по спиральной модели разработки продукции, продолжается в определенной степени на всех этапах жизненного цикла системы.

Кроме того, неопределенность и неполнота также присутствуют внутри самой системы по отношению к ее функциям, внутренней структуре и границам. Ее подсистемами часто управляют различные участники, при этом стороны, вовлеченные в интеграцию и координацию границ системы, могут не иметь полного знания и управления подсистемами. Услуги и компоненты могут быть добавлены или удалены из системы во время ее эксплуатации различными заинтересованными сторонами или по их требованию. Динамический характер таких систем делает их границы, функции и структуру неоднозначными в действии, даже если теоретически нет никакой неоднозначности в любое конкретное время с определенной точки зрения.

По этим причинам, в том числе из-за невероятной сложности и масштаба системы, заинтересованным сторонам очень трудно определить, понять, контролировать систему и управлять системой с достаточной достоверностью. Непредвиденные изменения и отказы в различной степени являются частью особенности системы. Использование термина «открытая система» подчеркивает этот аспект систем.

Истинные, предполагаемые ожидания для системы всегда относительны при наличии других окружающих систем и заинтересованных сторон. Цели различных уровней систем, окружающих базовую систему, должны быть учтены. Поскольку условия меняются, а неполнота и неопределенность так или иначе снижаются, система должна адаптироваться к соответствующим изменениям в требованиях и предположениях. Данные изменения невозможно ожидать или определить заранее.

4.2 Особенности надежности открытых систем

Надежность открытых систем направлена на достижение непрерывности функционирования систем в течение длительного периода времени, несмотря на изменения и отказы системы. Достижение непрерывности функционирования системы связано с выполнением соответствующих требований на всех этапах жизненного цикла системы и действий по постоянному улучшению.

Менеджмент надежности, установленный в *ГОСТ Р МЭК 60300-1*, обычно применяют к открытым системам, настоящий стандарт следует использовать вместе с *ГОСТ Р МЭК 60300-1*. В *ГОСТ Р МЭК 60300-1* установлены требования, согласно которым достижение улучшений обеспечено планированием, управлением действиями по улучшению и проведением анализа результатов улучшения. Теория надежности открытых систем детально разработана для открытых систем, в которых надежность непосредственно зависит от улучшений, выполняемых вследствие частых непредсказуемых изменений. Итеративный подход к жизненному циклу может быть применен для аккомодации таких изменений (см. приложение А).

Область применения менеджмента надежности открытой системы нельзя назвать простой из-за особенностей, описанных в 4.1. Недостаточно простого соответствия требованиям, установленным в соглашениях, поскольку соглашения не могут охватить все аспекты рассматриваемой системы, так как открытые системы не могут быть полностью определены. Заинтересованные стороны должны быть готовы действовать вне соглашений на основе общего понимания системы и ее окружающей среды. Обеспечение надежности открытых систем стремится к уверенности в соответствии системы даже при нарушении предположений и требований, ставших недействительными в результате изменений в системе и возможных отказов системы.

Все это подчеркивает важность процесса, который постоянно анализирует, пересматривает область применения менеджмента надежности, а также обеспечивает ее четкое документирование и согласование. Согласование заинтересованными сторонами области применения менеджмента надежности должно быть установлено соответствующими соглашениями о распределении ответственности и подотчетности.

Непредвиденные причины не могут быть предотвращены. Возможна лишь идентификация ключевых функций, предупреждение возможных последствий потери ключевых функций и защита ключевых функций таким образом, чтобы их можно было быстро восстановить или охватить резервированием.

4.3 Цель

Цель надежности открытых систем состоит в поддержании непрерывного функционирования системы в условиях наличия окружающих систем, заинтересованных сторон и среды до тех пор, пока это практически осуществимо при наличии непредвиденных событий и изменений, неполноты и неопределенности знаний о системе у заинтересованных сторон.

Систему не считают определенной, а рассматривают как открытую, если знания о ней не могут быть полными и определенными. Система, к которой применяют подход надежности открытых систем, должна быть способна:

- непрерывно удалять факторы, вызывающие отказы и, следовательно, улучшать себя;
- выполнять быстрые и соответствующие действия в случае отказа;
- предупреждать, минимизировать и смягчать ущерб;
- непрерывно обеспечивать функции, ожидаемые заинтересованными сторонами, в максимально возможной степени (постепенное ухудшение);
- поддерживать действия и задачи для обеспечения ответственности за эксплуатацию и процессы системы,
- помогать в понимании и обмене информацией о предположениях, сделанных при описании системы, документировании этих предположений, и определении надежности системы на основе документации и полномочий по ее приемке.

Ожидается, что такими возможностями обладают системы, даже если они имеют особое значение для открытой системы, имеющей более высокую вероятность нарушения работы под воздействием других систем, с которыми она связана. Особенности надежности открытых систем являются следствием неполноты и неопределенности, в рамках которых достигнуты установленные возможности. Характеристика надежности открытых систем связана с процессом достижения установленной способности системы выполнять требуемые функции, и в этом надежность открытых систем не отличается от традиционной надежности.

4.4 Обеспечение надежности открытых систем

Для обеспечения надежности открытой системы ее жизненный цикл должен допускать выполнение заинтересованными сторонами следующих действий:

a) установление понимания всеми заинтересованными сторонами системы ее цели, функционирования, окружающих условий и изменений и затем установление общей структуры понимания и четкого соглашения по всем этим вопросам;

b) установление прозрачных соотношений между невыполнением пункта соглашения заинтересованных сторон и воздействием этого невыполнения на заинтересованные стороны и общество в целом, включая обязательства ответственных заинтересованных сторон по максимальному выполнению соглашения и обеспечению доступности средств предупреждения возможного ущерба;

c) планирование и выполнение незамедлительных действий при возникновении отказов для обеспечения функционирования системы в максимально возможном объеме с наименее возможными разрушениями и ущербом самым целесообразным образом в существующих условиях;

d) организация необходимых действий при адаптации системы к изменениям в окружающей среде, цели, соглашений и т. д., приобретение опыта при возникновении отказов для непрерывного улучшения надежности системы.

Эти четыре метода работают вместе, и каждый зависит от остальных. Действия, указанные в перечислении a), обеспечивают основу для методов, указанных в перечислениях b), c) и d). Действия, указанные в перечислении b), помогают привести в действие соглашение, указанное в перечислении a), и способствуют уверенности и доверию общества к системе путем обмена информацией о планах и действиях, выполняемых в соответствии с перечислениями c) и d). Действия, указанные в перечислении c), дают необходимую информацию для выполнения действий, указанных в перечислении b), и используют действия, указанные в перечислении d), для предотвращения повторения отказа. Действия, указанные в перечислении d), перезапускают действия, указанные в перечислении a), чтобы учесть изменения, зависящие от времени, в общем понимании и четких соглашениях, упомянутых в перечислении a), эти действия являются этапом непрерывного обновления.

Способы объединения и взаимодействия этих четырех методов могут быть представлены в моделях жизненного цикла. В приложении А приведены соответствующие примеры. Пример применения надежности открытых систем к конкретной открытой системе приведен в приложении С.

4.5 Взаимосвязь устойчивости системы с отказоустойчивостью

Концепция устойчивости очень похожа для открытых и традиционных систем. Традиционное понятие устойчивости системы (см. 3.16, примечание 1) подчеркивает способность системы возвратиться к нормальному функционированию после нарушений работы, в то время как надежность открытых систем охватывает тот факт, что даже определение «нормальной эксплуатации» изменяется время от времени или в зависимости от точки зрения. Более свежая концепция устойчивости (примечание 2 в 3.16) рассматривает более широкий диапазон изменений и применима к надежности открытых систем. Различие состоит в том, что надежность открытых систем сосредоточена на случаях, где изменения и потребность в адаптации следуют из открытости системы, следовательно, сосредоточена на консенсусе и ответственности (подотчетности) заинтересованных сторон на всех стадиях жизненного цикла системы.

С другой стороны, идея отказоустойчивости различна для традиционных и открытых систем. Для традиционной системы считается возможным, по крайней мере в теории, перечислить все возможные существенные ошибки. Таким образом, для обеспечения отказоустойчивости может быть создана конкретная процедура возвращения к нормальной эксплуатации, когда отклонение и нормальная эксплуатация четко определены. Надежность открытых систем относится к ситуации, когда эти процедуры не могут быть четко определены.

5 Соответствие

Для подтверждения надежности открытых систем на стадиях жизненного цикла системы необходимо представить свидетельства надежности, которые должны обеспечить демонстрацию следующего *[8]. [9]*:

a) обеспечения жизненным циклом системы выполнения установленных требований ко всем процессам, установленным в разделе 6;

b) адекватности этих требований для обеспечения надежности рассматриваемой системы.

Примечания

1 Свидетельства надежности необходимы для обеспечения того, что заинтересованные стороны понимают и договариваются о границах своих обязанностей, распределяют ответственность за внедрение и менеджмент изменений соответственно.

2 Открытым системам не свойственен набор достаточных условий. Каждое применение настоящего стандарта оценивают на соответствие требованиям с учетом качества дополнительного рассмотрения этого применения [см. перечисление b)] относительно особенностей текущей цели.

Пример свидетельства надежности, который демонстрирует вышеупомянутые требования, приведен в приложении В.

6 Анализ процесса обеспечения надежности открытой системы

6.1 Общие положения

В разделе 6 приведено описание четырех видов анализа процесса, которые связаны с четырьмя подходами, установленными в 4.4 [см. перечисления a) — d)]. Часть действий и задач, необходимых для выполнения процессов, приведена в соответствии с *[1]*.

Каждый подход к надежности открытых систем требует выполнения ряда действий и задач, которые проходят сквозь стадии жизненного цикла. Концепция анализа процесса введена для того, чтобы объединить в группу связанные между собой действия, как описано в *[1]* (см. *[1]*, приложение Е).

В разделе 6 приведены четыре вида анализа процесса в соответствии с точкой зрения, установленной в *[1]*. Анализ процесса проводят на основе следующей информации:

a) наименование анализа процесса;

b) цели анализа процесса;

c) результаты анализа процесса;

d) идентификация и описания процессов, действий и задач, которые выполняют при проведении анализа процесса, и ссылки на источники данных об этих процессах, действиях и задачах в других стандартах.

В разделе 6 установлен каждый из четырех видов анализа процесса с учетом перечислений a) — d).

Эти четыре вида анализа процесса выполняют совместно для достижения целей надежности открытых систем. Вместе с процессами жизненного цикла системы и другими видами анализа процесса они формируют модель жизненного цикла системы, как это требуется в соответствии с *[1]* (см. *[1]*, приложение А).

Примечания

1 В *[1]* детализированы процессы, их действия и задачи. Выбранные наборы процессов могут быть применены на всех стадиях жизненного цикла для управления и выполнения стадий жизненного цикла системы.

2 В предпоследнем абзаце 4.4 показано соотношение между четырьмя видами анализа процесса. В приложении А.2 подробно описаны соотношения на примере модели жизненного цикла.

В остальной части раздела 6 каждый подпункт (т. е. 6.*i*) обеспечивает анализ процесса и организован следующим образом.

Наименование подпункта 6.*i* является наименованием анализа процесса (a).

В 6.*i*.1 «Цель» установлена цель анализа процесса (b). В первом абзаце установлена основная цель, а в следующих абзацах приведены пояснения.

В 6.*i*.2 «Результаты» перечислены выходы (результаты) процесса (c). В некоторых случаях результаты представлены иерархически. В приложении В представлена структура аргументов для свидетельств надежности, использующих результаты. Это обеспечивает некоторые соотношения для выбора результатов.

Содержание 6.*i*.3 «Процессы, действия и задачи» представляет собой основную часть настоящего стандарта. Представлен перечень процессов, действий и задач (d), установленных в *[1]*, которые осуществляют анализ процесса вместе с рекомендациями по реализации надежности открытых систем. Для каждого процесса, указанного в *[1]*, приведен дополнительный абзац, в котором описана его связь с анализом процесса, а также приведено более подробное описание соответствующих действий и задач с признаками результатов анализа процесса. Описания в 6.*i*.3 должны быть использованы вместе с описаниями в *[1]*, которые обеспечивают определение и условия применения связанных процессов, действий и задач.

В 6.*i*.3 приведены ссылки на разделы *[1]* и настоящего стандарта. Их различают следующим образом. Угловые скобки (< >) использованы для обозначения номера раздела в *[1]* и приведено наименование элемента перечня действий или задач процесса. Например, «<6.4.2> Процесс определения требований и потребностей заинтересованных сторон» относится к 6.4.2 из *[1]*, а в пределах содержания <6.4.2>, «<a)1)>» относится к задаче «1) Идентификация заинтересованных сторон, которым необходимы сведения о системе в течение всего жизненного цикла» в пределах действия, «a) Подготовка определения требований и потребностей заинтересованных сторон». Для двухуровневого перечня ссылки на элемент перечня уровня 1, например «<a)>», относится ко всем элементам уровня 2 <a)1)>, <a),2)>..., <a)n)>, которые составляют элемент уровня 1 <a)>. Квадратные скобки ([ ]) использованы для ссылки на элемент перечня результатов анализа процесса в 6.*i*.2 настоящего стандарта.

6.2 Анализ процесса достижения консенсуса

6.2.1 Цель

Целью анализа процесса достижения консенсуса является установление и поддержание общего понимания с четкими соглашениями о системе, ее назначении, цели, задачах, окружающей среде, фактическом изготовлении, жизненном цикле и их изменениях.

Примечание 1 — В отличие от четких соглашений, общее понимание системы не обязательно четко документировано и включает подход, убеждения, восприятие и ценности, которые разделяют заинтересованные стороны.

Цель анализа может быть достигнута при осознании следующего.

Должно быть обеспечено одинаковое понимание у всех заинтересованных сторон, при котором расхождения в интерпретациях являются приемлемыми. Четкие соглашения включают в себя преимущества и ответственность заинтересованных сторон в разработке и эксплуатации системы, а также в сделанных предположениях.

Установление общего понимания и четких соглашений обеспечивает общие превентивные меры по отношению к непредвиденным событиям.

Примечание 2 — Для некоторых заинтересованных сторон может быть достаточным понимание того, что другие заинтересованные стороны гарантируют желаемые результаты, без потребности в понимании технических деталей.

Достижение цели включает следующее:

- установление общего понимания и четких соглашений среди заинтересованных сторон [6.2.2, результаты a)1) — a)7)];
- поддержка понимания и соглашений [b)1) — b)5)].

Связь между целью и результатами анализа описана в В.2.

6.2.2 Результаты

a) Установлены общее понимание и четкие соглашения между заинтересованными сторонами.

1) Идентифицированы заинтересованные стороны системы.

Примечание 1 — Перечень заинтересованных сторон изменяется во времени в зависимости от точки зрения.

2) Установлена структура базового понимания для всех заинтересованных сторон. Эта структура включает термины и основные предположения об окружающей среде системы.

3) Назначение, задачи, окружающая среда, фактическое изготовление, жизненный цикл системы и их изменения в структуре базового понимания всех заинтересованных сторон одинаковы. Это включает предположения относительно системы и ответственности заинтересованных сторон.

4) Предварительно согласован арбитражный процесс для ситуаций, когда консенсус не может быть достигнут с целью разрешения конфликта интересов.

Примечание 2 — Конфликты интересов могут включать в себя права на интеллектуальную собственность.

5) На основе понимания [см. 3)] разработаны и документированы четкие соглашения. Записи включают отчеты о разработке и причинах, по которым различные компоненты соглашений можно считать целесообразными и выполнимыми.

6) Различия в интерпретации документов соглашения находятся в пределах приемлемого диапазона.

7) Результаты, указанные выше, достигнуты справедливым и беспристрастным для всех заинтересованных сторон способом.

Примечание 3 — Справедливость и беспристрастность обеспечивают устойчивость в случаях непредвиденных событий. Отсутствие беспристрастности и справедливости в конечном счете приводит к проблемам, которые влияют на все заинтересованные стороны.

Примечание 4 — Получение мнений и требований с помощью вымогательства и шантажа несправедливо и неразумно, поскольку может иметь непропорциональные долгосрочные последствия для больших открытых систем в виде достижения ими своих целей.

b) Осуществляется поддержка общего понимания и четкого соглашения среди заинтересованных сторон.

1) Установлена политика управления изменениями соглашений.

Примечание 5 — Эту политику применяют на всех этапах, включая начальную идентификацию требований к функциям системы и их пересмотру.

2) Осуществляется поддержка консенсуса заинтересованных сторон при изменении бизнес-целей, потребностей заинтересованных сторон, системы или ее окружающей среды.

Примечание 6 — Такие изменения могут потребоваться на этапе реагирования и восстановления после отказа.

Примечание 7 — Поддержание консенсуса заинтересованных сторон означает его пересмотр, утверждение и возобновление таким образом, чтобы консенсус отражал новые цели, потребности, систему и ее окружающую среду после изменений.

3) Анализ процесса достижения консенсуса выполняют при изменении бизнес-целей, потребностей заинтересованных сторон, системы или ее окружающей среды.

Примечание 8 — Консенсус может быть ограничен частью действий или некоторыми заинтересованными сторонами, в то время как изменения остальных действий или заинтересованных сторон изменения не оказывают влияния. Заинтересованные стороны могут решить не принимать участия в вопросах, которые не имеют для них значения или имеют незначительное значение. Часто действиями управляет небольшая группа назначенных заинтересованных сторон, в то время как остальная часть заинтересованных сторон соглашается с этим, пока работа является для них приемлемой и их жизненно важные интересы не затронуты.

Примечание 9 — Действия для вовлечения заинтересованных сторон описаны в *ГОСТ Р ИСО 60300-1*, пункт 5.3 (третье перечисление).

4) Определена ответственность за выполнение и одобрение свидетельства надежности.

5) Достижение консенсуса, записи о его разработке и причины, по которым консенсус считают допустимым и осуществимым, зарегистрированы в отчете о свидетельствах надежности (см. *[9]*).

6.2.3 Процессы, действия и задачи

Анализ процесса достижения консенсуса должен быть выполнен с использованием действий и задач следующих процессов (см. *[1]*).

Примечание 1 — Далее в угловых скобках (< >) указаны номера подпунктов и их наименования в *[1]*. В квадратных скобках ([ ]) указаны элементы перечня результатов анализа процесса из настоящего стандарта. Более подробная информация приведена в последнем абзаце 6.1.

<6.1.1> Процесс приобретения устанавливает и поддерживает соглашение между покупателем и поставщиком, что является частью четких соглашений, упомянутых в [a), b)]. Покупатели должны учитывать также интересы других сторон (не только покупателей и поставщиков), таких как конечные пользователи, местное сообщество и контролирующие органы [a)].

- <a)1)>: Стратегия приобретения должна быть направлена на достижение общего понимания и четких соглашений в соответствии с [a)].
- <c)1), c)4)>: Разработку и согласование изменений соглашения между покупателем и поставщиком необходимо проводить справедливо и внимательно [a)7)].
- <d)>: Мониторинг соглашения является частью политики и направлен на точную поддержку соглашения [b)1), b)2), b)3)].
- <d)1)>: Оценка выполнения соглашения должна включать оценку его справедливости и беспристрастности [a)7)].

<6.1.2> Процесс поставки устанавливает и поддерживает соглашение между покупателем и поставщиком, которое является частью четких соглашений в соответствии с [a), b)]. Поставщики должны

учитывать также интересы других сторон (не только покупателей и поставщиков), таких как конечные пользователи, местное сообщество и контролирующие органы [a)].

- <a)1)>: Идентификация покупателей является частью идентификации заинтересованных сторон [a)1)].

- <a)2)>: Стратегия поставки должна разъяснять способы ее выполнения [a)].

- <c)1), c)4), d)1)>: Согласование соглашения и его выполнение должны быть реализованы справедливо и беспристрастно [a)7)].

- <d)2)>: Оценка выполнения соглашения должна включать оценку его справедливости и беспристрастности [a)7)].

<6.2.1> Процесс управления моделью жизненного цикла должен установить связи между процессами жизненного цикла, что позволяет получить все результаты анализа процесса [a), b)].

<6.2.5> Процесс менеджмента качества формулирует аспекты общего понимания и четких соглашений в виде управляемых показателей качества. Он также управляет качеством общего понимания и четких соглашений [a), b)].

- <a)1)>: Политика, цели и процедуры менеджмента качества должны быть направлены на уровень общего понимания и согласия по отношению к точным соглашениям [a), b)]. Заинтересованные стороны должны выработать общее понимание и четкие соглашения относительно менеджмента качества, учитывая, что не существует одной организации, которая осуществляет менеджмент качества системы в целом [a), b)].

- <a)2), a)3)>: Общее понимание менеджмента качества должно признавать, что определение обязанностей и критериев оценки несовершенно и может быть изменено, а заинтересованные стороны должны быть готовы действовать, когда необходимо, вне определенной для них ответственности ради всеобщего качества [b)].

- <a)3)>: Критерии оценки должны быть справедливыми и беспристрастными [a)7)].

<6.2.6> Процесс менеджмента знаний обеспечивает общее понимание.

- <a)1), b)1), c)1)>: Стратегия менеджмента знаний, классификация разделения и систематизации знаний в организации должны обеспечить структуру базового понимания всех заинтересованных сторон [a)2)].

- <d)>: Поддержка знаний должна быть интегрирована в поддержку общего понимания и четких соглашений [b)].

<6.3.1> Процесс планирования проекта воплощает общее понимание и четкие соглашения, такие как планы [a), b)].

- <a), b)1) — b)6)>: Определение и планирование проекта (цели, ограничения, область применения, модель жизненного цикла, структура распределения работ, график, критерии выполнения стадий жизненного цикла, затраты и бюджет, функции, обязанности, ответственность персонала и т. д.) должны отражать общее понимание и четкие соглашения и, в свою очередь, углублять и разъяснять их, формируя основу их поддержки [a)2), a)3), a)5), a)6), b)1), b)2), b)3)].

- <b)4)>: Ответственность за свидетельства надежности должна быть определена в планах проекта [b)4)].

- <b)7)>: Планы обмена информацией и выполнения анализа должны быть частью разработки и поддержки четких соглашений; анализ должен обеспечивать и документировать обоснование положений соглашений [a)5), b)2), b)5)].

<6.3.2> Процесс оценки и управления проектом направлен на поддержание общего понимания и четких соглашений при появлении изменений.

- <b), c)>: Оценка и управление проектом включают оценку и управление (i) консенсусом заинтересованных сторон относительно изменений его содержания и (ii) выполнения соответствующих процессов относительно необходимых результатов анализа этих процессов [b)1), b)2), b)3)].

<6.3.3> Процесс менеджмента принимаемых решений обеспечивает разрешение конфликтов, возникающих при установлении и поддержании общего понимания и четких соглашений, а также управляет решениями по принятию единодушных мнений [a), b)].

- <a)1)>: Стратегия менеджмента принимаемых решений должна включать предварительно согласованный арбитражный процесс [a)4)].

- <a)3)>: Помимо заинтересованных сторон с конфликтом интересов те стороны, интересы которых затрагивают решения, должны быть идентифицированы и вовлечены [a)1), a)7)].

- <b)2)>: Желаемый результат и критерии выбора должны быть определены справедливым и беспристрастным способом при помощи рекурсивного применения анализа процесса достижения консенсуса [a)6), a)7)].

- <c)2), c)3)>: Записи резолюций, обоснования решений и предположений, прослеживания и оценки должны обеспечить учет формирования консенсуса и доказательства его справедливости и беспристрастности [a)7), b)5)].

Примечание 2 — Инициирование анализа процесса достижения консенсуса и инициирование процесса менеджмента принимаемых решений являются взаимно рекурсивными. Достижение консенсуса требует принятия решения, и каждое решение требует консенсуса по желаемым результатам и критериям выбора.

<6.3.6> Процесс управления информацией производит, получает, подтверждает, преобразовывает, сохраняет, восстанавливает, распространяет и удаляет ненужную информацию об общем понимании, четких соглашениях и управлении ими.

- <a)1), a)5)> Стратегия управления информацией и действиями по поддержке информации должна включать политику управления изменениями соглашений [b)1)], поддержку консенсуса заинтересованных сторон [b)2)], анализ процесса достижения консенсуса [b)3)]. Эти действия должны сократить различие интерпретаций [a)6)] и поддерживать справедливость и беспристрастность для всех заинтересованных сторон [a)7)].

- <a)2)>: Управляемые элементы информации должны включать перечень идентифицированных заинтересованных сторон [a)1)], структуру ссылок [a)2)], понимание цели системы и т. д. [a)3)], согласованный арбитражный процесс [a)4)], четкие соглашения [a)5)], свидетельства надежности [b)4)], учет разработок и обоснование консенсуса [b)5)].

- <a)3)>: Назначение обязанностей и полномочий по управлению информацией включает назначение обязанностей и полномочий в области свидетельства надежности [b)4)].

- <a)4)>: Форматы и структура элементов информации являются частью структуры в соответствии с [a)2)], их содержание должно отражать общее понимание [a)3), a)5)].

- <b)1)>: Разработка информации о четких соглашениях должна признавать согласованный арбитражный процесс разрешения конфликта интересов [a)4)]. Структура в соответствии с установленной в [a)2)] должна быть использована для преобразования информации в информацию, полезную для заинтересованных сторон.

- <b)5)>: Изъятие информации с учетом разработки четких соглашений и их обоснования [b)5)] должно быть выполнено только после внимательного рассмотрения значения информации для изменения договоренностей и обеспечения ответственности на более позднее время, включая случаи, когда они появляются в результате реагирования на отказ.

<6.3.8> Процесс менеджмента качества обеспечивает уверенность в том, что общее понимание и четкие соглашения установлены и поддерживаются на достаточном уровне качества и что их содержание в виде требований к качеству выполнено.

- <b), c)>: Оценка продукции или услуги и процесса должна быть частью поддержки общего понимания и четких соглашений [b)1), b)2)].

- <d)>: Запись действий по обеспечению качества должна обеспечивать отчет о достижении консенсуса [b)5)].

- <e)>: Обработка проблем должна включать анализ необходимости модификации общего понимания и четких соглашений и их процессов [b)1), b)2), b)3)].

<6.4.1> Процесс анализа деятельности или назначения обеспечивает структуру базового понимания и начинает создание общего понимания окружающей среды и т. д. в этой структуре. Применение этого процесса должно учитывать, что системе может недоставать организации, охватывающей все заинтересованные стороны.

- <a)2), b)2)>: Стратегия анализа и определение проблем области применения должны разъяснить структуру базового и общего понимания, они также должны быть справедливыми и беспристрастными [a)2), a)3), a)7)].

- <b)1)>: После анализа проблемы должно быть получено подтверждение, что все заинтересованные стороны разделяют одно и то же понимание области применения, основ или причин проблем и возможностей, указанных в <b)1) примечание 1> [a)2), a)3), a)6)].

- <c)1)>: Идентификация основных групп заинтересованных сторон должна учитывать, что заинтересованные стороны могут изменяться во времени, и каждая заинтересованная сторона может по своему понимать, какие субъекты являются основными группами заинтересованных сторон системы; каждая заинтересованная сторона должна быть идентифицирована вместе с ее функциями [a)1)]; предварительные концепции эксплуатации должны включать политику относительно функций системы, которая выражает общее понимание [a)2)].

- <c)2)>: Идентифицированные классы решений должны быть распределены среди всех заинтересованных сторон, и каждая заинтересованная сторона должна быть в состоянии рассмотреть решения со своей точки зрения для обеспечения справедливости и беспристрастности [a)3), a)7)].

- <d)>: Выполняющий оценку и метод оценки должны быть идентифицированы и согласованы всеми заинтересованными сторонами [a)7)].

- <e)1)>: Прослеживаемость результатов анализа до и после изменений должна быть поддержана в дополнение к прослеживаемости результатов анализа и других артефактов в одной итерации жизненного цикла [b)2), b)5)] (см. <6.4.1.1, примечание 2>).

<6.4.2> Процесс определения потребностей и требований заинтересованных сторон разрабатывает общее понимание и четкие соглашения относительно цели системы и т. д. в виде определения потребностей и требований заинтересованных сторон [a)3), a)5)].

- <a)1)>: Идентификация заинтересованных сторон должна учитывать, что заинтересованные стороны могут изменяться во времени и каждая заинтересованная сторона может по-своему понимать, какие субъекты являются заинтересованными сторонами системы; каждая заинтересованная сторона должна быть идентифицирована вместе с ее функциями [a)1)].

- <a)2)>: Стратегия определения потребностей и требований заинтересованных сторон должна обеспечивать справедливое и беспристрастное разрешение различных мнений и конфликтов, что помогает обеспечивать гарантию и целостность системы [a)4), a)7)] (см. <6.4.2.3 a)2) примечание>); стратегия должна быть направлена на достижение общего понимания политики в отношении функций системы [a)3)].

- <b)1)>: Определение условий использования системы должно устранить разногласия в предположениях заинтересованных сторон справедливым и беспристрастным образом [a)2), a)3), a)7)].

- <b)2), b)3), b)4)>: При определении явных и неявных потребностей следует обратить особое внимание на <b)2), примечание 1>; потребности заинтересованных сторон должны быть выявлены вместе с их предположениями о системе и ее среде; следует учесть, что различия в предположениях могут стать очевидными только после некоторого периода эксплуатации; различия, препятствующие обмену информацией о надежности среди заинтересованных сторон, могут быть препятствием в достижении консенсуса и могут привести к нерациональным решениям [a)2), a)3)]; сбор информации, идентификация, выбор и определение потребностей заинтересованной стороны должны быть справедливыми и беспристрастными [a)7)].

- <c)>: Концепция эксплуатации должна включать политику относительно функций системы, которая должна отражать общее понимание [a)2)].

- <f)>: Необходимо управлять изменениями определения потребностей и требований заинтересованных сторон [b)].

<6.4.3> Процесс определения требований к системе преобразовывает консенсус заинтересованных сторон в конкретные требования к системе. Это облегчает техническое обслуживание, как и оценку результатов анализа этого процесса [a), b)].

- <b), c)>: До того как выбран особый набор технических требований, заинтересованные стороны должны достигнуть консенсуса относительно ожидаемых последствий и рисков, соответствующих этому набору для каждой заинтересованной стороны [a)5), a)6), a)7)].

<6.4.4> Определение структуры обеспечивает часть структуры исходных сведений и четких соглашений [a)2), a)5)].

- <b)1)>: С точки зрения структуры необходимо формировать структуру исходного базового понимания [a)2)].

- <f)2)>: Четкое принятие структуры должно формировать часть соглашений [a)5)].

<6.4.9> Процесс верификации является частью оценки четкого соглашения [a)6), b)2)].

- <c)3)>: Согласие заинтересованной стороны с тем, что система соответствует требованиям, является частью четких соглашений в соответствии с [a)5)].

<6.4.11> Процесс валидации является частью оценки четких соглашений [a)6), b)2)].

6.3 Анализ процесса обеспечения ответственности

6.3.1 Цель

Цель анализа процесса обеспечения ответственности состоит в установлении взаимосвязи между нарушением четкого соглашения и его значением для заинтересованных сторон и общества в целом. Это относится к обязательствам ответственных заинтересованных сторон обеспечивать средства

реализации консенсуса относительно системы, чтобы поддерживать доверие к системе и обеспечивать готовность средств устранения возможного вреда.

Примечания

1 Нарушение соглашения охватывает также такую ситуацию, в которой заинтересованная сторона неспособна обеспечить выполнение соглашения из-за непредвиденного неблагоприятного события.

2 Соглашения должны быть четкими, разъяснять причины, по которым каждая заинтересованная сторона должна обеспечивать свою ответственность (подотчетность). Четкие соглашения при необходимости могут ссылаться на негласные соглашения, например на промышленные своды правил.

Цель анализа может быть достигнута при осознании следующего.

Анализ процесса обеспечения ответственности также обеспечивает ответственность перед обществом в целом. Ответственность — это общая ответственность за принимаемые решения и действия в процессе жизненного цикла системы. Ответственность включает обязанность представления информации пользователям и другим заинтересованным сторонам, а также мониторинга и поддержания средств контроля идентифицированного риска. Так как у открытых систем не существует централизованного управления, трудно идентифицировать сторону, ответственную за конкретное решение, действие или особое управление.

Ответственность непосредственно влияет на доверие людей к системе, такие субъективные свойства системы важны для ее надежности. Отсутствие ответственности препятствует восстановлению работы некоторых систем вследствие невыполнения нормативных требований, негативного общественного мнения и других социальных причин.

Ответственность необходима для обеспечения надежности системы и повышения надежности в целом связанных независимо управляемых систем. Последствия отказа системы могут быть снижены за счет окружающих связанных систем, которые совместно используют информацию об отказе.

Достижение цели состоит из следующих действий:

- установление связи между нарушением соглашения и его последствиями, которое включает обязательства ответственных заинтересованных сторон обеспечивать средства устранения последствий до событий, для работы с которыми назначена ответственность [6.3.2 результаты a) — e)];

- выполнение действий предупреждения и реагирования на события, для выполнения которых назначена ответственность [f) — h)];

- представление достоверной информации заинтересованным сторонам и обществу в целом [от i)1) до i)5)].

Связь между целью и результатами анализа описана в приложении В.3.

6.3.2 Результаты

a) Идентифицированы ключевые решения по управлению жизненным циклом системы и риски жизненного цикла системы, включая управление результатами процессов и анализа процессов.

Примечание 1 — К ключевым решениям относят решения, принимаемые на стадиях жизненного цикла системы, а также решения, оказывающие большое влияние на дальнейшее развитие жизненного цикла системы.

b) Для каждого ключевого решения по управлению жизненным циклом системы и контролю риска в процессе жизненного цикла системы идентифицировано ответственное физическое и юридическое лицо.

c) Для каждого элемента каждого четкого соглашения идентифицированы ключевые решения, которые могут вызвать его отказ или нарушение.

Примечание 2 — Для нарушения соглашения, вызванного факторами вне системы, составляющие ключевые решения включают принятие риска и принятие результатов анализа несоответствующего риска.

Примечание 3 — Заинтересованные стороны, ответственные за нарушение соглашения, являются ответственными за ключевые решения, идентифицированные в качестве возможных причин нарушения.

d) Для каждого нарушения каждого четкого соглашения оценены воздействия этого нарушения на неответственные заинтересованные стороны и общество в целом.

Примечание 4 — Оценка включает анализ контроля этих воздействий ответственными заинтересованными сторонами с имеющимися у них полномочиями и ресурсами.

Примечание 5 — Каждый элемент каждого четкого соглашения сформулирован так, что такой анализ возможен.

e) Для каждого нарушения каждого четкого соглашения утверждены его последствия для ответственных заинтересованных сторон и средства защиты и устранения последствий неответственных заинтересованных сторон и общества в целом.

Примечание 6 — Последствия для ответственных заинтересованных сторон включают обязательства обеспечить согласованные средства защиты неответственных заинтересованных сторон и общества в целом. Анализ процесса достижения консенсуса необходим для пересмотра необходимого соглашения таким образом, чтобы у ответственных заинтересованных сторон было достаточно возможностей для выполнения обязательств.

Примечание 7 — Соглашение относительно последствий и средств защиты от нарушения базового соглашения включает рассмотрение случая, когда нарушение вызвано изменениями, не рассмотренными в перечислениях a) — d).

f) Проводятся мониторинг и оценка ожидаемых и непредвиденных воздействий принятых решений на систему. В том числе мониторинг нарушения соглашений.

g) Установлены обратные связи, информирующие лиц, принимающих решения, и другие заинтересованные стороны о результатах принятых решений и выполненных действиях.

Примечание 8 — Обратные связи распознают непреднамеренные результаты и инициируют соответствующие действия.

Примечание 9 — Обратные связи улучшают понимание работы системы и взаимодействие лиц, принимающих решения, ответственных за различные части системы. Обратные связи крайне важны, так как стороны, принимающие решения, не имеют полного понимания о системе в целом; следовательно, у решений могут быть непредсказуемые последствия для других частей системы.

Примечание 10 — Менеджмент принятия решений является особенно трудным в открытых системах. Это касается как анализа процесса достижения консенсуса, так и анализа процесса обеспечения ответственности. Проблемы возникают, когда при выполнении решений относительно консенсуса возникают неожиданные результаты принятия решений в других частях системы. Обратные связи помогают устранить эти проблемы.

h) При нарушении соглашения заинтересованные стороны, ответственные за него, своевременно обеспечивают средства защиты и устранение последствий для неответственных заинтересованных сторон и общества в целом.

i) Ответственные заинтересованные стороны своевременно представляют неответственным заинтересованным сторонам и обществу в целом достоверную и уместную информацию.

Примечание 11 — Существуют некоторые ситуации, когда информация о сложных процессах жизненного цикла должна быть объединена.

Примечание 12 — Информация является достоверной и уместной, когда она является всесторонней (1); понятной для получателей (2), позволяющей каждому получателю уменьшить собственный вред от отказа (3) и обоснованной и достоверной с точки зрения получателей.

1) Быстрая, обоснованная и адекватная реакция поступает в ответ на обоснованные запросы заинтересованной стороны относительно информации о системе.

2) Заинтересованные стороны имеют правомерную уверенность и доверие к предоставленной информации о системе.

3) После отказа достоверная и уместная информация выбрана и представлена заинтересованным сторонам конкретной системы, заинтересованным сторонам связанных систем и общественности.

Примечание 13 — Информация формируется в результате анализа процесса реагирования на отказ.

4) Информация об изменениях требований к системе, ожиданий от работы системы, описания и показателей системы выбрана и представлена заинтересованным сторонам конкретной системы, заинтересованным сторонам связанных систем и общественности.

5) При обнаружении информация о расхождениях в требованиях, ожиданиях, описаниях и показателях системы выбрана и предоставлена заинтересованным сторонам системы, заинтересованным сторонам связанных систем и общественности.

6.3.3 Процессы, действия и задачи

Анализ процесса обеспечения ответственности должен быть выполнен с использованием действий и задач процессов, приведенных в *[1]*.

<6.1.1> Процесс приобретения

- <c)>: Установление соглашения между покупателем и поставщиком (включая критерии приемки и обязанности покупателя) включает ключевые решения, управляющие жизненным циклом системы [a)];

их невыполнение является нарушением соглашения; ключевые решения, приводящие к нарушению и т. д., должны быть идентифицированы в соответствии с [b), c), d), e)].

- <d)>: Мониторинг соглашения является частью обратных связей [f), g)].

<6.1.2> Процесс поставки

- <c)>: Установление соглашения между покупателем и поставщиком, включая критерии приемки и обязательности покупателя, включает ключевые решения, управляющие жизненным циклом системы [a)]; его невыполнение является нарушением соглашения, ключевые решения, приводящие к нарушению и т. д., должны быть идентифицированы [b), c), d), e)]. Поддержка соглашения также должна обеспечивать результаты [f), g)].

- <e)4)>: Ответственность за продукцию или услугу должна быть преобразована таким образом, чтобы гарантировать непрерывное достижение результатов [f), g), h), i)].

<6.2.1> Процесс управления моделью жизненного цикла

- <a)3)>: Установление функций и т. д. должно включать идентификацию физического или юридического лица, ответственного за каждое ключевое решение [b)].

- <a)4)>: Определение бизнес-критериев и способов управления стадиями жизненного цикла включает ключевые решения [a), b)]. Отчеты об этих разработках должны быть документированы [i)].

- <a)5)>: Установленный стандарт моделей жизненного цикла должен определить связи между процессами жизненного цикла, которые дают возможность получения всех результатов анализа процесса обеспечения ответственности [от a) до i)].

<6.2.3> Процесс управления портфолио должен идентифицировать ключевые решения относительно управления взаимодействием между жизненными циклами системы и других систем [a)].

- <a)3)>: Определение ответственности и полномочий является частью достижения [a), b)] и должно рассматриваться [c), d), e)] совместно.

- <a)5)>: Распределение ресурсов ответственному физическому или юридическому лицу включает ключевые решения в соответствии с [a), b)].

- <c)1)>: Отмена и приостановка проекта должны быть учтены своевременно [i)].

<6.2.5> Процесс менеджмента качества

- <a)1), a)3)>: Установление политики менеджмента качества и другого и определение критериев и методов оценки качества включают ключевые решения [a)] и результаты [b), c), d), e), h)], которые должны быть рассмотрены совместно. Для идентификации и определения должна быть установлена ответственность.

- <a)2)>: Определение ответственности и полномочий для внедрения менеджмента качества является частью достижения [b)].

- <b)>: Оценка удовлетворенности потребителя является частью достижения [d), f), g)].

- <c)>: Планирование корректирующих и предупреждающих действий является частью обязательств ответственных заинтересованных сторон [e), h)]; планирование является частью обратных связей [g)].

<6.2.6> В условиях, когда знания должны быть разделены между несколькими организациями, должен быть внедрен процесс менеджмента знаний [f), g), i)]. Достоверная информация в [i)] должна включать «уроки» прошлого опыта, который ответственные заинтересованные стороны использовали в своих решениях.

<6.3.1> Процесс планирования проекта: все определения и идентификации, осуществленные в этом процессе, включают ключевые решения [a)] и должны быть рассмотрены вместе с [b), c), d), e), h)].

- <a)4)>: Четкая структура распределения работ должна сопровождаться назначением ответственности и идентификацией уместной информации для распространения [b), i)].

- <b)4)>: Установленная ответственность должна включать идентификацию информации для распространения в случае отказа системы [i)].

- <b)6)>: Планирование приобретения включает ключевые решения [a)] и должно быть рассмотрено вместе с [b), c), d), e), h)].

<6.3.2> Процесс оценки и управления проектом

- <a)1)>: Определение стратегии оценки и управления проектом включает ключевые решения [a)] и должно быть рассмотрено вместе с [b), c), d), e), h)].

- <b)>: Оценка проекта должна включать оценку в соответствии с [d)]. Результат должен быть обеспечен в информации об ответственности [i)].

- <c)>: Средства управления проектом должны включать обратные связи, упомянутые в [g)], инициирование корректирующих действий [h)] и представление отчетной информации [i)].

<6.3.3> Процесс менеджмента принимаемых решений: ответственность за принятие и контроль решений включает обязанность показывать, что ответственные заинтересованные стороны рассмотрели всю релевантную информацию и правильно действовали в соответствии с процессом менеджмента принимаемых решений.

- <a)1), c)3)>: Стратегия менеджмента принимаемых решений должна обеспечивать хорошие обратные связи [g)].

- <c)2), c)3)>: Записи о принимаемых решениях должны включать свидетельства того, что ответственность за принятие и контроль решений достигнута [i)].

<6.3.4> Процесс менеджмента риска: ответственность за менеджмент идентифицированного риска, т. е. мониторинг и обеспечение контроля риска особенно важны. Это должно быть четко определено даже для риска, который не полностью понят [b), e), f), h)].

- <a)1), d)>: Определение стратегии менеджмента риска и решений по обработке риска включает ключевые решения [a)] и должно быть рассмотрено вместе с [b), c), d), e), h)].

<6.3.5> Процесс управления конфигурацией

- <b), c)>: Идентификация конфигурации технических объектов и изменений в процессе управления конфигурацией включает ключевые решения [a)] и должна быть рассмотрена вместе с [b), c), d), e), h)].

- <d), e)>: Статус конфигурации, отчетность и оценка конфигурации должны обеспечивать часть достоверной информации в соответствии с [i)], которая помогает приобрести уверенность и доверие заинтересованных сторон к информации о системе [i)2)].

- <e)4), e)5)>: Оценка конфигурации должна быть выполнена как часть мониторинга нарушения соглашений [f)] и обратных связей, о которых информируют лиц, принимающих решения, [g)].

<6.3.6> Процесс управления информацией должен обеспечивать достоверной информацией в соответствии с [i)]. В частности, должны быть достигнуты достаточная уверенность и доверие заинтересованных сторон [i)2)]. При обеспечении информацией необходимо учитывать совместную работу нескольких процессов жизненного цикла.

<a)1)>: Стратегия управления информацией должна поддерживать обратные связи о результатах решений при принятии новых решений [g)].

- <a)2)>: Все процессы должны инициировать процесс управления информацией для сбора и управления данными о регистрации и другими свидетельствами, которые позволяют установить и обосновать адекватность и достоверность информации об ответственности; должно быть обеспечено объективное представление обоснований [i)2)].

- <b)1)>: Элементы информации должны быть собраны и использованы вместе с доказательствами их подлинности в форме, допускающей проверку пользователями информации [i)2)].

- <b)3)>: Публикация, распределение или предоставление доступа к информации должны быть выполнены в соответствии с [i)].

- <b)5)>: Удаление информации включает ключевые решения. Удаление информации возможно только после внимательного изучения его влияния на обеспечение ответственности в будущем [от a) до i)].

<6.3.7> Процесс измерений должен формировать часть обратных связей [g)].

- <a)3)>: Для обратных связей следует рассмотреть необходимую информацию для мониторинга непредвиденных результатов [f), g)].

<6.3.8> Процесс обеспечения качества

- <a)1)>: Определение стратегии обеспечения качества включает ключевые решения [a)] и должно быть рассмотрено вместе с [b), c), d), e), h)].

<6.4.1> Процесс анализа деятельности или назначения

- <c)>: Описание области применения решений должно включать описание ответственности каждой идентифицированной основной заинтересованной стороны [b)].

<6.4.2> Процесс определения требований и потребностей заинтересованных сторон

- <a)1), b), c), d)>: Идентификация заинтересованных сторон, определение потребностей заинтересованных сторон, определение концепции эксплуатации и других концепций жизненного цикла и определение требований заинтересованных сторон включают ключевые решения [a)] и должны быть рассмотрены вместе с [b), c), d), e), h)].

- <b)2), d)3)>: Потребности заинтересованных сторон должны быть идентифицированы вместе с их ответственностью [b), c), d), e), h)].

- <c)>: Концепция эксплуатации и другие концепции жизненного цикла должны включать определение ответственности основных групп заинтересованных сторон, идентифицированных в <6.4.1>.

Анализ сценариев должен идентифицировать ключевые решения, принятые заинтересованными сторонами в соответствии со сценариями, и анализировать возможные воздействия и последствия этих решений [a), b), c), d), e), h)].

- <e)>: Принятие результатов анализа потребностей заинтересованных сторон является ключевым решением, а лицо, ответственное за процесс определения потребностей и требований заинтересованной стороны, является ответственным за решение [a), b), c), d), e), h)].

- <e)3)>: Обратная информация о проанализированных требованиях к соответствующим заинтересованным сторонам является частью обратных связей [g)].

- <f)1)>: Четкое соглашение по требованиям заинтересованных сторон должно идентифицировать ответственность по каждому элементу соглашения [c), d), e), h)].

- <f)2)>: Назначение ответственности должно быть прослеживаемым [b)]. Прослеживаемость должна быть обеспечена соответствующим образом [c), d), e), i)]. Требования заинтересованной стороны должны быть прослежены до требований к мониторингу системы [f), g)].

- <f)3)>: Записи о выборе ключевых элементов информации для исходных состояний должны быть зафиксированы в отчете для использования в достижении [i)].

<6.4.3> Процесс определения требований к системе

- <a)1), b)2), b)4), d)3)>: Определение функциональных границ, ограничений выполнения требований к системе и выбора ключевой информации для исходных состояний включает ключевые решения [a)] и должно быть рассмотрено вместе с [b), c), d), e), h)].

- <a)1)>: Функциональные границы должны быть определены вместе с границами ответственности [a), b), c), d), e), h)].

- <b)1)>: Функции должны быть определены вместе с ответственностью за их выполнение [a), b), c), d), e), h)].

- <b)3)>: Требования, относящиеся к риску и критичности системы, должны быть идентифицированы вместе с ответственностью за них [c), d), e)].

- <b)4)>: Определение требований заинтересованных сторон и их обоснование должны разъяснять ключевые решения, которые влияют на определение требований, и ответственность за них [a), b), c), d), e), h)].

- <c)>: Принятие результатов анализа требований к системе является ключевым решением, а лицо, ответственное за процесс определения требований к системе, является ответственным за это решение [a), b), c), d), e), h)].

- <c)3)>: Обратная информация о проанализированных требованиях к заинтересованным сторонам является частью обратных связей [g)].

- <d)2)>: Назначение ответственности должно быть прослеживаемым [b)]. Прослеживаемость должна быть обеспечена соответствующим образом [c), d), e), i)].

<6.4.4> Процесс определения структуры

- <a)1), a)2), a)4), b), d)1), d)2), e)3), f)2)>: Ниже указаны ключевые решения [a)], которые должны быть рассмотрены вместе с [b), c), d), e), h)]: идентификация ключевых причинных факторов, идентификация озабоченностей заинтересованных сторон, определение критериев оценки, определение точки зрения на структуру, идентификация элементов системы, определение интерфейсов и взаимодействий между элементами системы и внешними юридическими лицами, выбор и принятие структуры.

- <a)4)>: Критерии оценки структуры должны включать критерии ответственности, описанные в вариантах структуры.

- <c)>: Должны быть разработаны модели и виды анализа, которые разъясняют способ достижения результатов [a), b), c), d), e), h)].

- <d)>: Взаимосвязь структуры и проекта должна определять матрицу ответственности.

- <f)6)>: Назначение ответственности должно быть прослеживаемым [b)]. Прослеживаемость должна быть обеспечена соответствующим образом [c), d), e), i)].

- <f)7)>: Записи о выборе ключевых элементов информации для исходных состояний должны быть зарегистрированы в отчете для использования в достижении [i)].

<6.4.5> Процесс определения проекта

- <b)1), b)2), b)5), c), d)4)>: Ниже указаны ключевые решения [a)], которые должны быть рассмотрены вместе с [b), c), d), e), h)]:
  - распределение требований к системе по элементам системы;
  - преобразование характеристик структуры в характеристики проекта;
  - определение интерфейса между элементами системы и внешними юридическими лицами;

- идентификация неразрабатываемых элементов (оценка вариантов приобретения элементов системы);

- выбор ключевых элементов информации для исходных состояний.

- <b)1)>: Распределение требований к системе по элементам системы должно также включать распределение ответственности [b), c), d), e), h)].

- <b)2)>: Если характеристики структуры преобразовывают в характеристики проекта, ответственность за них также должна быть назначена [b), c), d), e), h)].

- <b)5)>: Интерфейсы элементов системы должны быть определены вместе с областью ответственности за них [b), c), d), e), h)].

- <c)>: Ответственность за неразрабатываемые элементы должна быть разъяснена [b), c), d), e), h)].

- <d)3)>: Прослеживаемость подотчетности также должна быть поддержана [b), c), d), e), h), i)].

- <d)4)>: Записи о выборе ключевых элементов информации для исходных состояний должны быть зафиксированы в отчете для использования в достижении [i)].

<6.4.6> Процесс анализа системы: записи о следующих действиях должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)]:

- <a)1)>: идентификация проблемы, которая требует анализа системы;
- <a)2)>: идентификация сторон, заинтересованных в анализе системы;
- <a)3)>: определение области применения, целей и уровня достоверности анализа системы;
- <b)1)>: идентификация предположений;
- <b)4)>: установление заключений по результатам анализа;
- <c)2)>: выбор ключевого элемента информации для исходных состояний.

<6.4.7> Процесс изготовления

- <a)1), a)2)>: Определение стратегии изготовления, идентификация ограничений и технологии изготовления включают ключевые решения [a)] и должны быть рассмотрены вместе с [b), c), d), e), h)].

- <c)>: Записи установления критериев, используемых для выявления аномалий, и выбор ключевых элементов информации об исходных состояниях должны быть зафиксированы в отчете для использования в достижении [i)].

- <c)2)>: Прослеживаемость ответственности при изготовлении элементов системы должна также быть поддержана [b), c), d), e), h), i)].

<6.4.8> Процесс интеграции

- <a)5)>: Ограничения системы, связанные с интеграцией, должны быть включены в требования к системе, структуру или проект как часть обратной связи [g)].

- <c)1), c)3)>: Записи об использовании критериев для выявления аномалий и выбор ключевых элементов информации об исходных состояниях должны быть зафиксированы в отчете для использования в соответствии с [i)].

- <c)2)>: Прослеживаемость ответственности для интегрированных элементов системы также следует поддерживать [b), c), d), e), h), i)].

- <b)1), b)3)>: Приемка изготовленных элементов системы и оценка, которая следует из проверки интерфейсов и т. д., являются ключевыми решениями [a)] и должны быть рассмотрены вместе с [b), c), d), e), h)].

<6.4.9> Процесс верификации

- Записи следующих действий должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)]:

  - <a)1)>: идентификация области верификации и соответствующих действий верификации;
  - <b)>: выполнение верификации;
  - <c)1)>: определение способов использования критериев для выявления аномалий;
  - <c)3)>: получение согласия заинтересованных сторон о том, что система или элемент системы соответствуют установленному требованию;
  - <c)5)>: выбор ключевых элементов информации для исходных состояний.

- <a)5)>: Ограничения системы для обеспечения верификации должны быть включены в требования к системе, структуру или проект как часть обратной связи [g)].

- <c)3)>: Утверждение о том, что система или элемент системы соответствуют установленному требованию, является ключевым решением [a)] и должно быть рассмотрено вместе с [b), c), d), e), h)].

- <c)4)>: Прослеживаемость ответственности за верификацию системы элементов также должна поддерживаться [b), c), d), e), h), i)].

<6.4.10> Процесс перемещения

- Следующие действия включают ключевые решения [a)] и должны быть рассмотрены вместе с [b), c), d), e), h)]:

- <a)1)>: определение стратегии перемещения;
- <a)2)>: идентификация необходимых изменений оборудования или места;
- <a)3)>: идентификация необходимого обучения операторов, пользователей и других заинтересованных сторон;
- <b)10)>: решение о вводе системы в эксплуатацию.

- Записи следующих действий должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)]:

- <b)4)>: заключение о том, что система установлена правильно;
- <b)6)>: заключение о наличии отметки о проверке того, что установленная система соответствует требованиям заинтересованных сторон в условиях эксплуатации;
- <b)7)>: заключение о том, что способность установленной системы выполнять требуемые функции продемонстрирована;
- <b)8)>: заключение о том, что устойчивость установленной системы продемонстрирована при помощи подключения систем;
- <b)9)>: заключение о том, что готовность к эксплуатации продемонстрирована на основе осмотра;
- <c)1), c)2)>: установление критериев, используемых для выявления аномалий, инцидентов и проблем в эксплуатации;
- <c)3)>: выбор ключевых элементов информации для исходных состояний.

- <a)1)>: Стратегия перемещения должна включать назначение ответственности [b), c), d), e), h)].
- <a)3)>: Идентификация необходимого обучения операторов и т. д. должна включать идентификацию их ответственности [b), c), d), e), h)].
- <a)4)>: Ограничения системы для обеспечения перемещения должны быть включены в требованиях к системе, структуру или проект как часть обратной связи [g)].
- <b)5)>: Обучение операторов и т. д. должно включать обмен информацией об их ответственности [b), c), d), e), h)].
- <b)9)>: Анализ готовности к эксплуатации должен рассматривать перспективу обеспечения ответственности в установленной среде [b), c), d), e), h)].
- <c)3)>: Прослеживаемость ответственности для перемещения элементов системы также следует поддерживать [b), c), d), e), h), i)].

<6.4.11> Процесс валидации

- Записи о следующих действиях должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)]:

- <a)1)>: идентификация области валидации и соответствующих действий валидации;
- <b)>: выполнение валидации;
- <c)1)>: установление критериев, используемых для выявления аномалий;
- <c)3)>: получение согласия заинтересованных сторон в том, что система или элемент системы соответствует потребностям заинтересованной стороны;
- <c)5)>:выбор элементов ключевой информации для исходных состояний.

- <b)3), c)3)>: Подтверждение того, что система или элемент системы соответствует потребностям заинтересованной стороны, является ключевым решением [a)] и должен быть рассмотрен вместе с [b), c), d), e), h)];
- <b)3)>: Анализ результатов валидации должен рассматривать перспективу обеспечения ответственности [b), c), d), e), h)].
- <c)4)>: Прослеживаемость ответственности для перемещенных элементов системы также следует поддерживать [b), c), d), e), h), i)].

<6.4.12> Процесс эксплуатации является основой обеспечения ответственности [f), g), h), i)].

- Процесс эксплуатации включает следующие ключевые решения [a)] и должен быть рассмотрен вместе с [b), c), d), e), h)]:

- <a)1)>: определение стратегии эксплуатации;
- <a)2)>: идентификация ограничений системы в эксплуатации, которые должны быть включены в требования к системе, структуру или проект;
- <a)3)>: идентификация и планирование подключаемых систем или функций, необходимых для поддержания эксплуатации;

- <a)6)>: назначение обученного, компетентного персонала на должность операторов;
- <b)3)>: определение контролируемых элементов данных;
- <b)5)>: решение о необходимости эксплуатации в непредвиденных случаях.

- Записи о следующих действиях должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)]:
- <b)4)>: определение приемлемых диапазонов параметра при выполнении функций;
- <c)1), c)2)>: установление критериев, используемых для выявления аномалий, инцидентов и проблем в эксплуатации;
- <c)4)>: выбор ключевых элементов информации для исходных состояний;
- <d)3)>: определение степени, в которой функции системы удовлетворяют потребностям потребителей.
- <a)1)>: Стратегия эксплуатации должна разъяснять назначение ответственности за мониторинг и поддержку потребителей [b), c), d), e), f), g), h), i)].
- <a)3)>: Идентификация систем, обеспечивающих доступ при эксплуатации, должна включать идентификацию границ ответственности между системой и системами, обеспечивающими доступ [b), c), d), e), h)].
- <a)6)>: Обучение и квалификация операторов включают их понимание ответственности [h)].
- <b)3)>: Мониторинг эксплуатации системы должен охватывать ожидаемые и непредвиденные результаты решений во всей системе [f)]. Мониторинг должен формировать часть обратных связей [g)]. Мониторинг должен допускать быструю идентификацию ответственных заинтересованных сторон и предоставление информации об отчетности по отношению к аномалиям и отказам [h), i)]. Прослеживаемость между действиями мониторинга и нарушением соглашения в [6.3.2] должна быть установлена через цепь ответственности, поддерживаемую в соответствии с <6.4.5 d)3), 6.4.7 c)2), 6.4.8 c)2), 6.4.9 c)4), 6.4.10 c)3), 6.4.13 d)4)>.
- <b)4)>: Аномалии эксплуатации по отношению к соглашениям, требованиям заинтересованных сторон и ограничениям организации должны быть идентифицированы, проанализированы и зарегистрированы с помощью процесса анализа системы [h), i)].
- <b)5)>: Эксплуатация в непредвиденных обстоятельствах должна включать инициирование корректирующих действий ответственными заинтересованными сторонами [h)] и своевременное представление информации об ответственности [i)3)].
- <c)2)>: Разрешение инцидентов и проблем в эксплуатации должно быть прослежено до ответственных заинтересованных сторон и действий, которые они предприняли [h), i)].
- <c)3)>: Прослеживаемость ответственности для элементов эксплуатации также следует поддерживать [b), c), d), e), h), i)].
- <d)1), d)2)>: Поддержка потребителя должна быстро представить достоверную информацию относительно запроса [i)1), i)2)], во время отказов [i)3)], во время изменений [i)4)] и когда выявлено нарушение при функционировании [i)5)].
- <d)3)>: Определение степени удовлетворенности потребителя должно быть выполнено как часть обратных связей. Удовлетворенность заинтересованных сторон необходимо контролировать вместе со степенью их ответственности [f), g)].

<6.4.13> Процесс технического обслуживания

- Процесс технического обслуживания включает следующие ключевые решения [a)] и должен быть рассмотрен вместе с [b), c), d), e), h)]:
- <a)1)>: определение стратегии технического обслуживания;
- <a)2)>: идентификация ограничений системы, связанных с техническим обслуживанием;
- <b)1)>: идентификация будущих действий корректирующего, адаптивного, улучшающего и предупреждающего технического обслуживания;
- <b)5)>: решение о необходимости выполнения предупреждающего технического обслуживания;
- <b)6)>: идентификация отказов;
- <b)7)>: идентификация потребностей в адаптивном или улучшающем техническом обслуживании;
- <c)5)>: подтверждение, что логистические действия включают требования к обеспеченности технического обслуживания, которые должны быть запланированы, обеспечены ресурсами и выполнены;
- <d)3)>: идентификация трендов в области инцидента, проблем и действий технического обслуживания и логистики.

- Записи следующих действий должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)]:

- <a)3)>: идентификация видов коммерческой деятельности для системы действий технического обслуживания и логистики;

- <d)1), d)2)>: установление критериев, используемых для выявления аномалий, инцидентов и проблем в эксплуатации;

- <d)6)>: определение степени удовлетворенности потребителя системой и обеспеченностью технического обслуживания;

- <d)5)>: выбор ключевых элементов информации об исходном состоянии.

- <a)2)>: Ограничения системы для адаптации технического обслуживания должны быть включены в требования к системе, структуру или проект как часть обратной связи [g)].

- <b)1)>: Анализ инцидентов и проблем для идентификации будущих потребностей технического обслуживания должен исследовать полученную степень достижения [b), c), d), e), h)].

- <b)2), d)2)>: Решение о техническом обслуживании и инцидентах в эксплуатации должно быть прослеживаемым до ответственных заинтересованных сторон и их действий [h), i)].

- <d)4)>: Прослеживаемость ответственности для элементов технического обслуживания также следует поддерживать [b), c), d), e), h), i)].

- <d)6)>: Определение степени удовлетворенности потребителя должно быть выполнено как часть обратных связей; удовлетворение заинтересованных сторон следует контролировать вместе со степенью их ответственности [f), g)].

<6.4.14> Процесс распоряжения (вывода из эксплуатации и утилизации)

- Следующие действия включают ключевые решения [a)] и должны быть рассмотрены вместе с [b), c), d), e), h)]:

- <a)1)>: определение стратегии вывода из эксплуатации;

- <a)2)>: идентификация ограничений системы на этапе вывода из эксплуатации, которые должны быть включены в требования к системе, структуру или проект;

- <a)5)>: требования к реализации оборудования, местам хранения, критериям контроля и периодам хранения (если система должна быть сохранена);

- <a)6)>: определение предупреждающих методов для исключения элементов и материалов, которые не должны быть использованы повторно, исправлены или использованы после возвращения в систему поставок;

- <b)1)>: решение о выключении системы или элемента системы для подготовки ее к выводу из эксплуатации;

- <b)3)>: выбор знаний об эксплуатации для регистрации, которые относятся к безопасности, защищенности, секретности, экологическим стандартам, директивам и законам;

- <c)1)>: подтверждение того, что все факторы, вредные для здоровья, безопасности, защищенности и окружающей среды будут отсутствовать после вывода системы из эксплуатации.

- <c)3)>: Записи о выборе информации для архивирования должны быть зафиксированы в отчете для использования в качестве достоверной информации в [i)].

- <c)>: Завершение вывода из эксплуатации должно подтвердить, что у системы не осталось вопросов в области отчетности и ответственности [i)].

6.4 Анализ процесса реагирования на отказ

6.4.1 Цель

Цель анализа процесса реагирования на отказ состоит в том, чтобы обеспечить непрерывную работу системы с выполнением максимально возможного количества функций с наименьшим разрушением и ущербом самым целесообразным способом в условиях эксплуатации.

Цель анализа может быть достигнута с учетом следующего.

Отказы могут быть непредсказуемыми или предсказуемыми, но маловероятными или требующими слишком больших затрат для их предупреждения, или предсказуемыми, но не предотвращенными из-за непредвиденных событий.

Нельзя подготовить средства защиты от непредвиденных событий, вызывающих отказ. Однако могут быть подготовлены универсальные меры, которые могут быть быстро выполнены. Это процедуры, позволяющие быстро сформировать действия реагирования на отказ в данных условиях с изменением при необходимости. Защита от возможных отказов, независимо от их причин, также приводит к разработке универсальных мер.

Участие человека играет ключевую роль, так как не все отказы могут быть предупреждены или смягчены при помощи предварительно спланированных действий. Для быстрой и соответствующей реакции участие человека должно быть обеспечено поддержкой программных и аппаратных средств с целью оптимизации принятия решений и выполнения установленных действий.

Анализ процесса реагирования на отказ подготавливает средства управления последствиями нарушения работы системы. Действия после отказа включают меры по устранению идентифицированных последствий отказа, для которого не могут быть определены причины во время идентификации последствий. Подготовка к таким последствиям возможна, но ее можно сделать только после реализации последствий.

Анализ процесса реагирования на отказ идентифицирует действия, направленные на предотвращение возникновения неисправностей, ошибок, отказов и предшествующих им признаков. Реакция на отказ включает предупреждение отказа после обнаружения его предвестников, эксплуатацию в непредвиденных обстоятельствах после обнаружения отказов и корректирующее и предупреждающее техническое обслуживание.

Достижение цели включает следующее:

- подготовку к реагированию на отказ [6.4.2 результаты a)1) — a)8)];
- выполнение действий реакции на отказ при отказе [b)1) — b)8)];
- обеспечение ответственности относительно отказов и реакции на отказ [c)1) — c)4)];
- улучшение жизненного цикла системы с опытом возникновения отказов [d)1), d)2)].

Связь цели и результатов анализа описана в приложении В.4.

6.4.2 Результаты

a) Подготовлены действия реагирования на отказ.

1) Идентифицированы ключевые функции, нуждающиеся в защите для обеспечения непрерывной работы системы.

2) Идентифицированы цели защиты ключевых функций, необходимых для обеспечения непрерывной работы системы.

3) Идентифицированы неисправности, ошибки, отказы и предшествующие им признаки, которые воздействуют на ключевые функции.

Примечание 1 — Существуют неидентифицируемые неисправности, ошибки, отказы и предшествующие им признаки, включая те, которые не могут быть спрогнозированы и не признаны ни одной из заинтересованных сторон.

Примечание 2 — Ошибки взаимодействия указывают при идентификации и обнаружении неисправностей, ошибок, отказов и предшествующих им признаков.

4) Выполнен анализ последствий и вероятности возникновения идентифицированных неисправностей, ошибок, отказов и предшествующих им признаков.

Примечание 3 — Предположения, сделанные для анализа во время подготовки, проверены до реагирования на фактические отказы и т. д. См. b)2) ниже.

5) Для идентифицированных неисправностей, ошибок, отказов и предшествующих им признаков определены и согласованы цели обработки, необходимые для обеспечения непрерывной работы системы.

Примечание 4 — Данные цели включают в себя цели предотвращения ущерба.

6) Действия по обработке идентифицированных неисправностей, ошибок, отказов и предшествующих им признаков, выбраны из следующих вариантов:

I) мониторинг и предварительная обработка предусмотрены проектом системы;

II) мониторинг предусмотрен, а предварительная обработка не предусмотрена проектом системы;

III) мониторинг и предварительная обработка не предусмотрены проектом системы.

Примечание 5 — Слова «предусмотрен проектом системы» означают, что система разработана так, что в ней предусмотрен ряд определенных действий, которые обеспечивают непрерывность работы системы.

7) Разработаны установленные действия, защищающие ключевые функции системы от неисправностей, ошибок, отказов и предшествующих им признаков в соответствии с вариантом a)6)I) и невыполнения действий по реагированию на неисправности, ошибки, отказы и предшествующие им признаки в соответствии с вариантами a)6)II) и a)6)III).

Примечание 6 — Установленные действия реагирования должны быть основаны на результатах анализа последствий и вероятности неблагоприятных событий. Эти действия должны быть выполнены системой, а также персоналом, связанным с жизненным циклом системы.

Примечание 7 — Установленные реакции включают действия после появления отказа.

Примечание 8 — Рассматриваются также отказы действий, выполняемых после возникновения отказа. Действия для таких отказов могут быть представлены на нескольких уровнях и применены рекурсивно к их отказам.

8) Разработаны универсальные меры для сокращения вреда от отказов с неидентифицированными причинами.

Примечание 9 — Универсальные меры включают быструю идентификацию неисправных частей системы, изоляцию частей, работающих со сбоями, с целью защиты других частей, функционирующих исправно, поддержание оставшихся функций на уровне, оговоренном в соглашении заинтересованных сторон, и восстановление после отказа.

b) При необходимости выполнены действия реагирования на отказ.

1) Неисправности, ошибки, отказы и предшествующие им признаки обнаружены.

2) Выполнены анализ причин и анализ последствий фактических неисправностей, ошибок, отказов или предшествующих им признаков.

Примечание 10 — Анализ последствий после обнаружения отказов и т. д. проверяет предположения, сделанные при анализе до обнаружения отказов в отношении фактической ситуации, и подтверждает или изменяет результаты анализа.

3) Цель обработки обнаруженных неисправностей, ошибок, отказов и предшествующих им признаков усовершенствована для текущей ситуации.

4) При обнаружении выполнены установленные действия по реагированию на неисправности, ошибки, отказы и предшествующие им признаки в соответствии с вариантом a)6)I) и действия по умолчанию, предусмотренные вариантами a)6)II) и a)6)III).

5) После события разработаны действия по реагированию на фактические неисправности, ошибки, отказы и предшествующие им признаки в соответствии с a)6)II) и a)6)III).

Примечание 11 — Мониторинг в соответствии с вариантом a)6)II) позволяет более быстро распознавать отказы и т. д. с более подробными данными для действий реагирования по сравнению со случаем отсутствия мониторинга в соответствии с a)6)III).

6) Действия по реагированию на неисправности, ошибки, отказы и предшествующие им признаки не увеличивают вред и не повышают риск возникновения вреда в дальнейшем.

Примечание 12 — В некоторых случаях смягчающие действия наносят новый ущерб. Предполагается, что новый ущерб не превышает ущерб в ситуации, когда действия по снижению ущерба от неисправностей, ошибок, отказов не предпринимают.

7) Вред исследуемой системе и связанным с ней системам сокращен в целом.

8) Действия по реагированию на обнаруженные отказы проанализированы относительно цели, усовершенствованной в соответствии с b)3).

c) Обоснование действий по реагированию получено в результате анализа процесса обеспечения ответственности.

1) Ущерб, нанесенный отказами, компенсируют в соответствии с установленным соглашением.

2) Установлено доверие к системе.

Примечание 13 — Например, доверие может быть достигнуто с помощью распространения после каждого реагирования на отказ информации (1) в случае гарантии о том, что действия реакции достигли или достигнут своих целей (2) в случае пересмотра гарантии для жизненного цикла системы (пункт 5) о том, что будущие повторения отказа предотвращены.

3) Заинтересованные стороны и общественность информируют о результатах реагирования на отказ. Эта информация включает:

I) обоснование области идентифицированного набора неисправностей, ошибок, отказов и предшествующих им признаков;

II) обоснование планируемых действий по реагированию на обнаруженные неисправности, ошибки, отказы и предшествующие им признаки;

III) результаты анализа последствий обнаруженных неисправностей, ошибок, отказов или предшествующих им признаков;

IV) результаты действий по реагированию на отказ и их анализ.

4) Представлена необходимая информация для анализа процесса обеспечения ответственности.

Примечание 14 — Деструктивные изменения могут вызвать отказы, за которые не несет ответственность ни одна заинтересованная сторона, а также отказы, реагирование на которые невозможно. Предоставление необходимой информации для анализа процесса обеспечения ответственности позволяет быстро распознавать такие изменения и применять к ним анализ процесса аккомодации изменений, который исследует деструктивные изменения.

d) Жизненный цикл системы улучшен путем проведения анализа процесса согласования изменений на основе данных о фактических отказах и реакции на отказы.

1) Цель улучшения определена и согласована.

Примечание 15 — Цель включает предотвращение повторения отказов, улучшение стратегии эксплуатации системы, улучшение целей системы, улучшение процессов идентификации ошибок и менеджмента риска. Определение цели включает идентификацию фактических последствий отказа в соответствии с анализом последствий, оценкой вреда и оценкой значения работы системы.

2) Необходимая информация представлена для анализа процесса согласования изменений.

6.4.3 Процессы, действия и задачи

Анализ процесса реагирования на отказ должен быть выполнен при использовании действий и задач следующих процессов, установленных в *[1]*.

<6.1.1> Процесс приобретения

- <c)1)>: Соглашение между покупателем и поставщиком должно идентифицировать ключевые функции, которые должны быть защищены от отказов, и цели защиты [a)1), a)2), a)5)].
- <d)1)>: Оценка выполнения соглашения должна подтверждать, что цели защиты в соответствии с <c)1)> и результаты [b), c)] достигнуты и обеспечены.

<6.1.2> Процесс поставки

- <c)1)>: Соглашение между покупателем и поставщиком должно идентифицировать ключевые функции, которые должны быть защищены от отказов, и цели защиты [a)1), a)2), a)5)].
- <d)1)>: Оценка выполнения соглашения должна подтверждать, что цели защиты в соответствии с <c)1)> и результаты [b), c)] достигнуты и обеспечены.

<6.2.1> Процесс управления моделью жизненного цикла

- <a)5)>: Установленные модели жизненного цикла должны определять взаимосвязь процессов жизненного цикла, что обеспечивает получение всех результатов анализа процесса реагирования на отказ [a), b), c), d)].

<6.2.4> Процесс управления человеческими ресурсами

- <a)>: Навыки, которые должны быть идентифицированы, включают навыки, необходимые для понимания цели системы, и навыки, необходимые для применения понимания цели системы к разработке с участием человека, что обеспечивает результаты [a)7), a)8), b)].

<6.2.5> Процесс менеджмента качества

- <b)>: Оценка менеджмента качества должна анализировать обнаружение и обработку неисправностей, ошибок, отказов и предшествующих им признаков, идентифицированных в соответствии с [a)3)], как предполагается в [b), c)].

<6.3.2> Процесс оценки и управления проектом

- <a)>: Оценка проекта и стратегия управления проектом должны отражать общее понимание, установленное в [6.2.2 a)], чтобы поддерживать:
  - разработку общих мер противодействия отказам, не подготовленных в проекте, и отказам с не выявленными причинами [a)8)],
  - совершенствование целей обработки отказов [b)3)],
  - разработку действий реакции на отказы, не подготовленной при проектировании [b)5)].
- <c)>: Управление проектом должно включать в себя анализ процесса аккомодации изменений, связанных с адаптацией системы для предотвращения повторных отказов [d)].

<6.3.4> Процесс менеджмента риска

- <a)1), a)2), b)2), c), d)1), d)2), d)4), e)>: Процессы и процедуры менеджмента риска приведены в *ГОСТ Р ИСО 31000* и *ГОСТ Р ИСО/МЭК 31010*. Кроме того, должны быть идентифицированы в соответствии с [a), b)8)]:

- способы обмена информацией и консультаций в области риска, контроля и обработки риска;
- способы сокращения отказов с невыявленными причинами;
- способы сокращения ущерба от работы системы и связанных с ней других систем;
- результаты анализа последствий и анализа правдоподобия в письменной форме;
- перечень возможных событий, приносящих вред; перечень событий, приносящих вред, которые считают маловероятными, но за которыми установлен мониторинг; перечень событий, приносящих вред, которые считают маловероятными, но за которыми не установлен мониторинг;
- объективное обоснование адекватности набора средств для обнаружения неисправностей, ошибок, отказов и предшествующих им признаков;
- способы адаптации системы к изменениям в отношении отказов.

<6.4.2> Процесс определения требований и потребностей заинтересованных сторон

- <b)2)>: Потребности заинтересованных сторон должны быть идентифицированы вместе с потребностями в защите от отказов [a)1), a)2)]. Потребности заинтересованных сторон должны включать потребность в непричинении вреда исследуемой системе и связанным с ней системам [a)8), b)7)].
- <c)1)>: Анализ представительных сценариев должен помочь идентифицировать ключевые функции, требующие защиты [a)1)]. Этот анализ включает в себя анализ риска отказов для определения потребности в защите от отказов [a)2)] и анализ вреда, который исследуемая система может нанести связанным с ней системам [b)7)].
- <d)2)>: Идентификация требований и функций заинтересованных сторон включает обозначение ключевых функций, требующих защиты от отказов [a)1)], и цели защиты [a)2)]. Требования заинтересованных сторон должны включать требования непричинения вреда исследуемой системе и связанным с ней системам [b)7)].
- <e)1)>: Анализ полного набора требований заинтересованных сторон должен включать анализ риска отказов ключевых функций для определения цели их защиты [a)2)], рассмотрение общих мер противодействия отказам с невыявленными причинами [a)8)] и рассмотрение ущерба, который исследуемая система может нанести всем связанным с ней системам [b)7)]. Анализ должен идентифицировать неисправности, ошибки, отказы и предшествующие им признаки, которые воздействуют на ключевые функции, и их последствия [a)4), a)5)].
- <e)2)>: Критические показатели работы должны включать меры степеней защиты ключевых функций [a)2)], обработки отказов и т. д. [a)5)].
- <f)1)>: Соглашение по требованиям заинтересованных сторон должно включать перечень ключевых функций, требующих защиты [a)1)], цели защиты ключевых функций [a)2)], цели обработки отказов, воздействующих на ключевые функции [a)5)].

<6.4.3> Процесс определения требований к системе

- <b)1)>: Определение ключевых функций должно включать:
  - цели защиты от отказов [a)2)];
  - идентификацию неисправностей, ошибок, отказов и предшествующих им признаков, которые воздействуют на функцию, включая ошибки взаимодействия [a)3)];
  - цели обработки идентифицированных неисправностей, ошибок, отказов и предшествующих им признаков [a)5)];
  - классификацию обработки каждой идентифицированной неисправности, ошибки, отказа и предшествующих им признаков [a)6)].
- <b)3)>: Идентификация требований к системе, связанных с риском и т. д., должна допускать идентификацию ключевых функций, которые должны быть защищены от отказов [a)1)]. Необходимо идентифицировать:
  - требования защиты ключевых функций [a)2)];
  - требования обработки соответствующих неисправностей и т. д. [a)5)];
  - требование того, чтобы реакция на отказ не усугубляла вред от отказов и не увеличивала риск появления дальнейшего вреда [b)6)];
  - требования мониторинга будущих отказов и т. д. [b)1)];
  - требования сокращения ущерба, который исследуемая система может нанести связанным с ней системам [b)7)].
- <b)4)>: Определение требований к системе и их обоснование должно включать следующее:
  - требование защиты ключевой функции [a)2)] и функций обработки отказов и т. д. [a)5)];
  - прослеживаемость вышеупомянутых требований до исходных функциональных требований [c)].

- <c)1)>: Анализ полного набора требований к системе должен включать анализ последствий возможных отказов ключевых функций [a)4)], который допускает:

  - определение целей защиты ключевых функций [a)2)] и целей обработки идентифицированных ошибок и т. д. [a)5)];
  - разработку общих мер защиты от отказов с невыявленными причинами [a)8)];
  - исключение увеличения вреда и риска дальнейшего вреда от действий реакции на отказ [b)6)];
  - сокращение вреда, который исследуемая система может нанести себе и связанным с ней системам [b)8)].

- <c)2)>: Критические показатели деятельности должны включать показатели степени защиты ключевых функций [a)2)] и обработки неисправностей и т. д. [a)5)].

- <d)1)>: Соглашение о требованиях к системе должно включать перечень ключевых функций, требующих защиты [a)1)], цели защиты ключевых функций [a)2)], цели обработки неисправностей и т. д., которые воздействуют на ключевые функции [a)5)].

- <d)2)>: Прослеживаемость от требований к мониторингу до требований к ключевым функциям должна поддерживаться с целью обеспечения ответственности за реакцию на отказ [b)1), c)].

<6.4.4> Процесс определения структуры

- <a)2)>: Идентифицированные озабоченности заинтересованных сторон должны быть отражены в целях защиты ключевых функций [a)2)] и целях обработки неисправностей и т. д. [a)5)] в итерациях процесса определения структуры вместе с процессом определения требований и потребностей заинтересованных сторон и процессом определения требований к системе. Озабоченности заинтересованных сторон относительно вреда системам, связанным с исследуемой системой, должны быть идентифицированы [b)7)].

- <c)>: Должны быть разработаны модели и виды анализа, направленные на обработку неисправностей и т. д. [a)5), a)6)], их обнаружение [b)1)], частные и общие реакции на отказ [a)7), a)8)]. Взаимодействия между действиями реакции на отказ и другими функциями системы должны быть направлены на то, чтобы избежать увеличения вреда от действий реакции на отказ [b)7)].

- <c)2)>: Должны быть идентифицированы ключевые объекты структуры, связанные с ключевыми функциями и их защитой [a)1), a)7)].

- <d)1)>: Должны быть идентифицированы ключевые элементы системы, связанные с ключевыми объектами структуры, для защиты ключевых функций [a)1), a)7)].

- <d)2), d)3)>: Ошибки взаимодействия, их обнаружение и конкретные общие реакции на них должны быть учтены при определении интерфейсов между элементами системы и внешними объектами и при разделении требований по элементам системы [a)3), b)1), a)7), a)8)]. Взаимодействия между реакциями на отказы и другими функциями системы должны быть учтены во избежание увеличения вреда от действий реакции на отказ [b)6)].

- <f)2)>: Принятие структуры заинтересованными сторонами должно включать принятие структуры обработки неисправностей и т. д. [a)6)], конкретных реакций на отказ [a)7)], общих реакций на отказ [a)8)], обнаружения неисправностей и т. д. [b)1)].

- <f)6)>: Прослеживаемость от целей обработки неисправностей и т. д. [a)5)], структуры обработки неисправностей и т. д. [a)6)], конкретных реакций на отказ [a)7)], общих реакций на отказ [a)8)] и обнаружения неисправностей и т. д. [b)1)] до целей защиты [a)2)] должна поддерживаться для отчетности о реакции на отказ [c)].

<6.4.5> Процесс определения проекта

- <a)2)>: Должны быть определены характеристики проекта, связанные с общими мерами защиты от отказов с невыявленными причинами [a)8)].

- <a)3)>: Принципы разработки проекта должны обеспечивать руководство по анализу процесса аккомодации изменений после реагирования на отказ [d)].

- <b)1)>: Требования защиты ключевых функций [a)2)] и обработки неисправностей и т. д. [a)5)] должны быть распределены по элементам системы.

- <d)3)>: Прослеживаемость от характеристик проекта для обработки неисправностей и т. д. [a)6)], конкретной реакции на отказ [a)7)], общих реакций [a)8)] и обнаружения [b)1)] до объектов структуры для защиты ключевых функций [a)2)] и целей обработки ошибок [a)5)] должна поддерживаться для целей отчетности [c)].

<6.4.6> Процесс анализа системы

- <c)1)>: Прослеживаемость результатов анализа системы должна поддерживаться для обеспечения своевременного отчета о реакции на отказ [c)].

<6.4.7> Процесс изготовления

- <c)2)>: Прослеживаемость от перечисленного ниже до характеристик проекта должна поддерживаться для отчета о реакции на отказ [c)]:
  - изготовленных элементов системы для обработки неисправностей, ошибок, отказов и предшествующих им признаков [a)6)];
  - конкретных реакций на отказ [a)7)];
  - общих реакций [a)8)];
  - обнаружения неисправностей, ошибок, отказов и предшествующих им признаков [b)1)].

<6.4.8> Процесс интеграции

- <a)1)>: Для проверки правильной эксплуатации и целостности собранных интерфейсов и выбранных функций системы необходимо контролировать:
  - интерфейсы ключевых функций, идентифицированных в [a)1)];
  - интерфейсы функций защиты ключевых функций [a)2), a)5), a)7), b)1), b)5)];
  - ошибки взаимодействия элементов системы [a)2), a)8), b)7)];
  - общие меры защиты от отказов по всей системе [a)8), b)6), b)7)];
  - то, что реакции на отказ не увеличивают вред и риск дальнейшего вреда [b)6)];
  - возможный вред, который исследуемая система может нанести связанным с ней системам [b)8)].
- <b)3)>: Проверка интерфейсов, выбранных функций и критических характеристик качества включает следующее:
  - идентификацию возможных ошибок взаимодействия [a)3), a)7), b)7)];
  - проверку результативности общих мер защиты от отказов [a)8)];
  - проверку того, что реакция на отказ не увеличивает вред и риск дальнейшего вреда [b)6)];
  - проверку возможного вреда, который исследуемая система может нанести связанным с ней системам [b)8)].
- <c)2)>: Прослеживаемость интегрированных элементов системы должна поддерживаться способом, допускающим быстрое реагирование на отказ [b)] и своевременный отчет о реакции на отказ [c)].

<6.4.9> Процесс верификации

- <a)1)>: Область применения и действия верификации должны включать верификацию достижения целей защиты ключевых функций [a)2)] и обработки неисправностей и т. д. [a)5)].
- <c)2)>: Инциденты в эксплуатации должны быть зарегистрированы и прослежены до разрешения проблемы способом, допускающим своевременный отчет о реакции на отказ [c)].
- <c)3)>: Соглашение между заинтересованными сторонами о том, что установленные требования выполнены, должно включать соглашение о том, что цели обработки неисправностей и т. д. выполнены [a)5)].
- <c)4)>: Прослеживаемость результатов верификации должна поддерживаться способом, допускающим быструю реакцию на отказ [b)] и своевременный отчет о реакции на отказ [c)].

<6.4.10> Процесс перемещения

- <b)5)>: Обучение операторов и т. д. должно быть запланировано как часть общего реагирования на отказ и мер защиты от отказов [a)7), a)8)]. Обучение должно выработать у заинтересованных сторон навыки достижения [b)] посредством участия человека.
- <b)9)>: Анализ готовности к эксплуатации должен подтвердить, что достижение целей в соответствии с [a)2), a)5), a)8), от b)1) до b)7)] продемонстрирован.
- <c)2)>: Инциденты в эксплуатации должны быть зарегистрированы и прослежены до разрешения проблем способом, допускающим своевременный отчет о реакции на отказ [c)].
- <c)3)>: Прослеживаемость перемещенных элементов системы должна поддерживаться способом, допускающим быструю реакцию на отказ [b)] и своевременный отчет о реакции на отказ [c)].

<6.4.11> Процесс валидации

- <a)1)>: Область применения и действия валидации должны включать следующее:
  - валидацию защиты ключевых функций в отношении их целей [a)2)];
  - валидацию обработки неисправностей и т. д. в отношении их целей [a)5)];
  - валидацию общих мер защиты от отказов с невыявленными причинами [a)8), b)1), b)4) — b)7)].
- <c)2)>: Инциденты в эксплуатации должны быть зарегистрированы и прослежены до разрешения проблем способом, допускающим своевременный отчет о реакции на отказ [c)].

- <c)4)>: Прослеживаемость валидированных элементов системы должна быть поддержана способом, допускающим быструю реакцию на отказ [b)] и своевременный отчет о реакции на отказ [c)].

<6.4.12> Процесс эксплуатации

- <a)1)>: Стратегия эксплуатации должна включать следующие процедуры [b)]:

  - процедуры обнаружения неисправностей и т. д. [b)1)] и прогнозирования отказов по предшествующим им признакам;

  - процедуры мониторинга неисправностей и т. д. в классах I) и II) [a)6)];

  - процедуры в соответствии с [b)3)] и [b)5)], гарантирующие готовность быстрого участия человека в обнаружении неисправностей и т. д.

- <a)5)>: Обучение персонала должно быть запланировано как часть общих мер в соответствии с [a)8)] и должно подготовить у заинтересованных сторон способность достигать [b)] посредством участия человека в соответствии с пониманием целей системы. Требования квалификации должны включать требования к упомянутой выше способности.

- <b)3)>: Мониторинг эксплуатации системы должен включать мониторинг неисправностей, ошибок, отказов и предшествующих им причин в классах I) и II) [a)6)] для возможности их обнаружения в соответствии с [b)1)]. При обнаружении неисправностей и т. д. должны быть выполнены процедуры стратегии эксплуатации, обеспечивающие получение результатов [от b)2) до b)7)], а их результаты должны быть оценены [b)8)].

- <b)4)>: Идентификация неприемлемых результатов должна включать оценку реакции на отказ [b)8)] и инициировать анализ процесса согласования изменений для улучшения системы [d)].

- <b)5)>: Цели эксплуатации системы в непредвиденных обстоятельствах, необходимых для непрерывного выполнения функций, и условия, вызывающие эксплуатацию в непредвиденных обстоятельствах, должны быть включены в цели защиты ключевых функций в [a)2)] и цели обработки неисправностей и т. д. в [a)5)].

- <c)1)>: Результаты эксплуатации и аномалий должны быть зарегистрированы способом, допускающим отчет о реакции на отказ [c)] и улучшение системы [d)].

- <c)2)>: Инциденты и проблемы в эксплуатации должны быть зарегистрированы и прослеживаться способом, допускающим отчет о реакции на отказ [c)] и улучшение системы [d)].

- <c)3)>: Прослеживаемость эксплуатационных элементов должна поддерживаться способом, допускающим быструю реакцию на отказ [b)] и своевременный отчет о реакции на отказ [c)].

- <d)>: Поддержка потребителей должна активно обеспечивать отчет о реакции на отказ [c)].

<6.4.13> Процесс технического обслуживания

- <a)1)>: Стратегия технического обслуживания должна отражать цели защиты ключевых функций [a)2)] и цели обработки отказов и т. д. [a)5), b)].

- <b)1)>: Идентификация будущих потребностей технического обслуживания должна быть объединена с идентификацией и обнаружением неисправностей и т. д. [a)3), b)1)].

- <b)2)>: Инциденты при техническом обслуживании должны быть зарегистрированы и прослеживаться способом, допускающим отчет о реакции на отказ [c)] и улучшение системы [d)].

- <b)3), b)4)>: Обработка случайных ошибок должна быть объединена с анализом процесса реагирования на отказ [a), b), c), d)].

- <b)5)>: Предупреждающее техническое обслуживание может быть выбрано для достижения цели обработки идентифицированных неисправностей и т. д. [a)5), a)7)].

- <b)6)>: Действия идентификации отказа являются частью действий в соответствии с [b)1), b)2)].

- <c)>: Логистическая поддержка должна быть включена в реакции на предшествующие отказу признаки [a)7), b)4)].

- <d)1)>: Результаты технического обслуживания, результаты логистики и аномалии должны быть зарегистрированы способом, допускающим отчет о реакции на отказ и улучшение системы [c), d)].

- <d)2)>: Инциденты и проблемы в эксплуатации должны быть зарегистрированы и прослежены способом, допускающим отчет о реакции на отказ и улучшение системы [c), d)].

- <d)3)>: Идентификация тенденций инцидентов и проблем должна быть выполнена для улучшения жизненного цикла системы [d)].

- <d)4)>: Прослеживаемость элементов технического обслуживания должна поддерживаться способом, допускающим быструю реакцию на отказ [b)] и своевременный отчет о реакции на отказ [c)].

- <d)6)>: Контроль удовлетворенности потребителя должен быть объединен с оценкой реакции на отказ [b)8)] и улучшения жизненного цикла системы [d)].

<6.4.14> Процесс распоряжения (вывода из эксплуатации)

- <a)1)>: Должна быть определена стратегия вывода из эксплуатации для выполнения [b)7)].

6.5 Анализ процесса аккомодации изменений

6.5.1 Цель

Цель анализа процесса аккомодации изменений состоит в том, чтобы поддерживать статус «пригодности использования» системы, несмотря на изменения в требованиях, окружающей среде, задачах и/или целях.

Цель может быть достигнута при понимании следующего.

Анализ процесса обеспечивает взможность непрерывной работы системы в соответствии с решениями проблем, вызванных изменениями, и направлен на обеспечение того, чтобы отказы одного и того же вида не повторялись.

Существует много видов изменений, которые требуют адаптации. Изменения возникают в других системах, связанных с данной системой. Из-за быстрого темпа нововведений достаточно часто происходят изменения в технологической, деловой и социальной средах. Обнаружение непредвиденных событий указывает на изменения в предположениях, которые всегда являются неполными и неточными. Изменения могут быть неочевидными; часто их необходимо выявлять с помощью, например, периодического анализа. Необходимая адаптация не обязательно должна проходить непосредственно в исследуемой системе. При необходимости должен быть рассмотрен и приспособлен весь набор процессов жизненного цикла. Даже влияние и изменение окружающей среды могут быть адаптацией.

Анализ процесса аккомодации изменений требует выполнения действий по адаптации системы к изменениям, в том числе обнаружение изменений; их анализ; формирование и выполнение действий для продолжения выполнения, возможно, измененных функций системы и в случае, когда изменения являются причиной отказов, для предотвращения появления или повторения отказов.

Необходимо удостовериться, что планы являются не настолько жесткими, чтобы организация потеряла гибкость в случае возникновения незапланированной ситуации.

Достижение цели обеспечивают следующие действия:

- выполнение и анализ адаптации при наличии изменений [6.5.2 результаты a) — d)];
- постоянное улучшение жизненного цикла системы и обеспечение ответственности относительно адаптации к изменениям [e), f)].

Связь цели и результатов анализа описана в В.5.

6.5.2 Результаты

a) Изменения признаны и идентифицированы.

1) Идентифицированы изменения в области применения, предположениях, рисках и т. д., которые могут потребовать адаптации системы.

Примечание 1 — Изменения охватывают требования заинтересованных сторон; связанные системы; технологическую, деловую и социальную среду; восприятие заинтересованными сторонами функций системы; понимание заинтересованными сторонами консенсуса.

Примечание 2 — Изменения могут быть неочевидными; часто их необходимо активно выявлять, например при помощи периодического выполнения анализа.

2) До обнаружения непредвиденных событий, включая отказы, идентифицированы изменения в системе и/или окружающей среде, вызывающие отказы. Эта идентификация может быть инициирована анализом процесса реагирования на отказ.

Примечание 3 — Любое обнаружение непредвиденных событий, включая отказы, является обнаружением изменений. Изменение может быть фактическим или изменением понимания предполагаемых фактов.

3) Разрушающие изменения распознаны и являются управляемыми.

Примечание 4 — Разрушающими изменениями являются изменения, для которых существенная адаптация системы, по мнению существующих заинтересованных сторон, невозможна или невыполнима. Такая ситуация включает случаи, когда стоимость необходимой адаптации превышает устойчивость работы ответственных заинтересованных сторон в действующем соглашении. Менеджмент в таком случае может быть заранее запланирован в максимально возможной степени, например в отношении введения новых заинтересованных сторон, удаления неработающих заинтересованных сторон, восстановления консенсуса или раннего вывода системы из эксплуатации.

b) Адаптация системы подготовлена.

1) Оценены воздействия изменений на статус «пригодности использования» системы и документирована взаимосвязь изменений и их воздействий.

Примечание 5 — Оценка включает анализ причин.

2) Определена цель адаптации — сохранение статуса «пригодности использования» системы. Она включает следующее:

I) Заинтересованные стороны информируют о необходимости адаптации, вариантах адаптации и их последствиях.

II) Заинтересованные стороны получают необходимую поддержку на переговорах по соглашениям в измененных обстоятельствах.

III) Адаптация, вызванная анализом процесса реагирования на отказ, предотвращает повторение отказов.

IV) Цель адаптации определена.

3) Цель адаптации согласована и отражена в обновленном соглашении заинтересованных сторон с помощью анализа процесса достижения консенсуса.

Примечание 6 — Это включает принятие решения об адаптации системы.

Примечание 7 — Следует проявлять осторожность в случае адаптации к разрушающим изменениям.

c) Адаптация системы выполнена.

Примечание 8 — Адаптация может быть технической или нетехнической. Весь набор процессов жизненного цикла проанализирован и адаптирован при необходимости. Адаптация не обязательно связана непосредственно с системой. Даже влияние и изменение окружающей среды может быть адаптацией.

Примечание 9 — Рассмотрение адаптации включает предотвращение ошибок взаимодействия между частями системы, измененными после адаптации, и частями, которые остались неизменными.

1) Доступна техническая поддержка для необходимой адаптации.

2) Знания, полученные из прошлого опыта, эффективно использованы.

3) Определена адаптация, реализующая цель.

4) Адаптация разработана.

5) Адаптация выполнена так, чтобы разрушения существующих функций системы при эксплуатации и функций связанных систем были минимальны.

d) Выполнен анализ адаптированной системы в отношении цели адаптации.

e) Жизненный цикл системы непрерывно улучшается.

Примечание 10 — Ожидается, что постоянное улучшение обеспечивает возможность жизненному циклу системы соответствовать целевому состоянию системы. Это отличается от стремления к более высокой эффективности системы.

f) Адаптация учитывается при утверждении анализа процесса обеспечения ответственности.

1) Прослеживаемость от изменений в области применения и т. д. до адаптации поддерживается.

2) Заинтересованные стороны и общество в целом информируют о разработке и результатах адаптации.

6.5.3 Процессы, действия и задачи

Анализ процесса аккомодации изменений должен быть выполнен с использованием действий и задач следующих процессов *[1]*.

<6.1.1> Процесс приобретения

- <c)1), c)4)>: Заинтересованным сторонам должна быть обеспечена необходимая поддержка при обеспечении соглашения между покупателем и поставщиком с учетом измененного содержания [b)2)II)].
- <c)2), c)5)>: Для адаптации изменений должны быть идентифицированы необходимые изменения соглашения. Цель адаптации должна быть представлена как модификация соглашения [b)3)].
- <c)3)>: Результаты оценки воздействия изменений на соглашение следует рассматривать как обратную связь при определении цели адаптации [b)].
- <d)1)>: Большое отклонение фактического продвижения в выполнении соглашения от запланированного должно быть идентифицировано как изменение, которое также может требовать адаптации [a)1)].

<6.1.2> Процесс поставки

- <c)1), c)4)>: Заинтересованным сторонам должна быть обеспечена необходимая поддержка при обсуждении соглашения между покупателем и поставщиком с учетом измененного содержания [b)2)II)].

- <c)2), c)5)>: Для адаптации изменений должны быть идентифицированы необходимые изменения соглашения. Цель адаптации должна быть представлена как модификация соглашения [b)3)].

- <c)3)>: Результаты оценки воздействия изменений на соглашение следует рассматривать как обратную связь при определении цели адаптации [b)].

- <d)2)>: Большое отклонение фактического продвижения в выполнении соглашения от запланированного должно быть идентифицировано как изменение, которое также может потребовать адаптации [a)1)].

<6.2.1> Процесс управления моделью жизненного цикла

- <a)5)>: Установленные модели жизненного цикла должны устанавливать связи между процессами жизненного цикла, которые позволяют получить результаты анализа процесса аккомодации изменений [от a) до f)].

- <c)2)>: «Извлеченный урок» в одной итерации адаптации изменений должен быть включен в улучшение процесса для применения по отношению к будущим изменениям [e)].

<6.2.2> Процесс управления инфраструктурой: изменения в инфраструктуре проекта и требованиях к инфраструктуре должны быть идентифицированы как изменения, которые могут потребовать адаптации системы [a)].

<6.2.3> Процесс управления портфолио

- <a)1)>: Идентификация потенциально новых или измененных возможностей или назначения должна быть выполнена как часть идентификации изменений и оценки их воздействия [a)1), b)1)].

- <a)2)>: О расположении по приоритетам, выборе и установлении новых бизнес-возможностей и т. д. необходимо информировать для оценки статуса «пригодности использования» системы и определении целей адаптации в отношении других проектов в портфолио организации [b)1), b)2)].

- <a)3)>: Определение проекта в отношении системы, ответственностей и полномочий должно быть совместимо с целью адаптации системы [b)2), b)3)].

- <a)4)>: Ожидаемые цели, задачи и результаты выполнения проекта должны обеспечивать основу для оценки статуса «пригодности использования» системы и определения цели адаптации в отношении других проектов в портфолио [b)1), b)2)].

- <a)8)>: Должно быть получено разрешение на начало адаптации системы с определенной целью с учетом воздействия адаптации на другие проекты из портфолио организации [b)3), c)].

- <b)1)>: Оценка жизнеспособности проекта должна быть выполнена как часть изменения идентификации и оценки статуса «пригодности использования» системы [a)1), b)1)].

- <b)2)>: Действия по продолжению или переадресации проекта, относящиеся к системе, включают принятие решений о необходимости адаптации системы и определении цели адаптации [b)3), b)2)].

<6.2.5> Процесс менеджмента качества

- <a)>: Менеджмент качества должен быть запланирован с учетом того, что цели менеджмента качества изменяются, когда цель системы и т. д. также изменяются [от a) до d)].

- <b)1)>: Сбор и анализ результатов оценки обеспечения качества должны быть выполнены как часть признания и идентификации соответствующих изменений [a)].

- <b)2)>: Оценка удовлетворенности потребителя должна быть использована при оценке статуса «пригодности использования» системы [b)1)].

- <b)4)>: Мониторинг статуса улучшения качества должен быть выполнен как часть признания и идентификации соответствующих изменений [a)] и оценки адаптированной системы [d)].

- <c)1), c)2)>: Планирование корректирующих и предупреждающих действий в менеджменте качества должно быть объединено с определением цели адаптации [b)2)].

- <c)3)>: Мониторинг корректирующих и предупреждающих действий должен быть использован при оценке адаптированной системы по отношению к цели адаптации [d)].

<6.2.6> Процесс менеджмента знаний должен поддерживать информацию об «извлеченных уроках» из каждой итерации адаптации изменений, чтобы обеспечить ее применение по отношению к будущим изменениям [c)2), e)].

<6.3.1> Процесс планирования проекта

- <a)1)>: Задачи проекта должны быть идентифицированы и обоснованы, что составляет основу оценки статуса «пригодности использования» при изменении [b)1)] и определении цели адаптации [b)2)].

- <a)2)>: Область применения проекта должна включать действия по получению всех результатов анализа данного процесса [от a) до f)]. Планирование действий по управлению проектом (см. <a)2) примечание>) должно предусматривать ситуацию изменения цели проекта [a)]. Изменения действий в пределах области применения проекта должны быть признаны и идентифицированы [a)].

- <a)3)>: Модель жизненного цикла данного проекта должна определять связи процессов жизненного цикла, позволяющие получить все результаты анализа процесса аккомодации изменений [от a) до f)].

- <b)2)>: Критерии достижения в точке принятия решения на стадии жизненного цикла должны включать критерий решения о выходе из стадии использования, которое инициирует анализ процесса аккомодации изменений [a)].

- <b)4)>: Функции, обязанности, ответственность и полномочия для выполнения анализа процесса аккомодации изменений должны быть определены способом, допускающим отчет об аккомодации изменений [f)].

- <b)5)>: Изменения инфраструктуры и услуг, необходимых для выполнения проекта, должны быть признаны и идентифицированы [a)].

- <b)7)>: Обмен информацией о плане адаптации изменений должен позволять разработку соглашения о цели адаптации [b)3)] и должен быть использован при выполнении адаптации [f)].

<6.3.2> Процесс оценки и управления проектом должен допускать получение всех результатов анализа процесса аккомодации изменений [от a) до f)]. В частности, этот процесс должен быть направлен на изменение технических целей, требований и бизнес-задач в целом. Это включает поддержку разработчиков вариантов адаптации, идентификации изменений проекта, предположений, рисков и других изменений, которые требуют адаптации системы и идентификации соответствующих технических или нетехнических средств.

<b)>: Оценка проекта должна включать признание и идентификацию изменений [a)]. Проект должен быть исследован в отношении возможных изменений содержания, целей и планов проекта для оценки статуса «пригодности использования» системы [b)1)] и определять цель адаптации [b)2)].

- <b)7)>: Менеджмент проекта, технический анализ, аудит и контроль должны определить потребность и готовность к выполнению адаптации системы [a), b)].

- <b)8)>: Мониторинг критических процессов и новых технологий необходимо выполнять как часть признания и идентификации изменений [a)].

- <b)9)>: Анализ результатов измерений должен обеспечить идентификацию изменений и разработку рекомендаций по выполнению адаптации [a), b)2)].

- <b)11)>: Большое отклонение фактических результатов от плана должно быть идентифицировано как изменение, которое, в свою очередь, может потребовать адаптации [a)1)].

- <c)>: Средства управления проектом включают инициирование адаптации системы в соответствии с [b), c)].

- <c)1)>: Действия начала управления проектом включают определение цели адаптации [b)2)].

- <c)2)>: План проекта должен быть переработан в соответствии с согласованными целями адаптации и обновленным соглашением [b)3)].

- <c)4)>: Проект должен иметь разрешение на выполнение адаптации системы в соответствии с определенными целями [b)3), c)].

<6.3.3> Процесс менеджмента принимаемых решений

- <a)1), c)>: Стратегия менеджмента принимаемых решений должна быть направлена на изменения критериев решений в соответствии с изменениями содержания, предположений, рисков и т. д. проекта. Менеджмент принимаемых решений должен включать анализ прошлых решений, если они признаны и идентифицированы [b)1), b)2)].

<6.3.4> Процесс менеджмента риска: процедуры и процессы менеджмента и оценки риска приведены в *ГОСТ Р ИСО 31000* и *ГОСТ Р ИСО/МЭК 31010*. Кроме того, необходимо рассмотреть следующее:

- <a)1)>: Стратегия менеджмента риска должна быть направлена на изменения в менеджменте риска и включать процедуры анализа применяемых средств контроля риска, когда изменения признаны и идентифицированы [a), b)1), b)2)].

- <a)2)>: Условия применения менеджмента риска и процесс идентификации риска должны учитывать риск, связанный с изменениями [a)]:
  - требований заинтересованных сторон;
  - связанных систем;
  - технологической, деловой и социальной среды;

- восприятия заинтересованными сторонами функций системы;
- понимания заинтересованными сторонами консенсуса.

- <b)1)>: Пороги и критерии принятия риска, связанного с изменениями, должны отражать воздействие изменений на статус «пригодности использования» системы [b)1)].

- <b)3)>: Представление данных о риске заинтересованным сторонам должно быть выполнено как часть согласования целей адаптации и действий по адаптации [b)2), f)2)].

- <c)1)>: Идентификация риска, связанного с изменениями, должна быть выполнена как часть признания и идентификации изменений [a)1)].

- <c)2), c)3)>: Оценка последствий риска, связанного с изменениями, и ее сопоставление с пороговым риском должны быть выполнены как часть оценки статуса «пригодности использования» системы [b)1)].

- <c)4)>: Определение рекомендуемых стратегий обработки риска и действий по снижению риска, связанного с изменениями и не соответствующего пороговому значению риска, является частью определения цели адаптации [b)2)] и определения действий по адаптации [c)3)].

- <d)1)>: Идентификация рекомендуемых альтернативных вариантов обработки риска, связанного с изменениями, является частью определения цели адаптации [b)2)].

- <d)2)>: Определение заинтересованными сторонами необходимости воздействия на риск, связанный с изменениями, должно быть зафиксировано в обновленном соглашении заинтересованных сторон [b)3)]. Выполнение обработки риска, связанного с изменениями, является частью выполняемой адаптации [c)3)], [c)4)].

- <e)1)>: Непрерывный мониторинг всех видов риска и условий менеджмента риска в отношении изменений и повторную оценку риска при выявлении изменений необходимо выполнять как часть признания и идентификации изменений [a)1)] и оценки статуса «пригодности использования» системы [b)1)].

- <e)2)>: Меры оценки результативности обработки риска должны допускать оценку адаптированной системы [d)]. Мониторинг этих мер является частью признания и идентификации изменений [a)].

<6.3.5> Процесс управления конфигурацией

- <b)1)>: Идентификация элементов конфигурации крайне важна для признания и идентификации изменений в системе [a)]. Элементы системы, изменение которых может потребовать адаптации системы, должны быть идентифицированы как элементы конфигурации. Элементы конфигурации могут быть компонентами, представляемыми в виде черного ящика.

- <b)2)>: Идентификация структуры информации о системе должна учитывать вероятность того, что сама структура системы может быть непреднамеренно изменена вследствие неопределенности и неполноты системы или сознательно в процессе адаптации [a), f)].

- <b)3)>: Установление идентификаторов элементов конфигурации должно обеспечивать прослеживаемость между введенными или измененными в процессе адаптации элементами конфигурации и изменениями, которых требует адаптация [f)].

- <b)4)>: Исходное состояние должно допускать признание и идентификацию изменений в системе в течение всего жизненного цикла системы [a)].

- b)5)>: Соглашение между покупателем и поставщиком, которое устанавливает исходное состояние, должно быть использовано для определения цели адаптации будущих изменений как обновлений исходного состояния [b)3)].

- <c)>: Управление изменениями конфигурации должно включать следующее:
  - анализ воздействия изменений на статус «пригодности использования» системы [b)1)];
  - информирование заинтересованных сторон о возможности адаптации [b)2)I)];
  - поддержка заинтересованных сторон в обсуждении и согласовании цели адаптации [b)2)II), b)3)].

- <c)4)>: Прослеживание и управление утвержденными изменениями следует выполнять с учетом адаптации [f)]. Обоснование адаптации должно быть зарегистрировано как «извлеченные уроки» для применения по отношению к будущим изменениям [c)2)].

- <d)>: Отчет о статусе конфигурации должен обеспечивать поддержку прослеживаемости элементов конфигурации, а также обоснование изменений этих элементов [f)].

- <e)2)>: Верификация конечной конфигурации должна поддерживать признание и идентификацию случайных изменений в системе вследствие неопределенности и неполноты системы [a)].

- <f)1)>: Одобрение внедрения системы должно соответствовать тому, что внедрение системы обеспечит минимальные нарушения в существующем обслуживании системы и в других связанных системах [c)5)].

<6.3.6> Процесс управления информацией должен обеспечивать:

- признание и идентификацию изменений за счет доступа к прошлой и настоящей информации об элементах, зависящих от изменений [a)];
- представление заинтересованным сторонам информации о возможной адаптации системы [b)2)I)];
- представление информации об опыте прошлого в разрабатываемых адаптациях [c)2)];
- отчет об адаптации для заинтересованных сторон [f)].

<6.3.7> Процесс измерений

- <a)3)>: Потребности в информации должны быть идентифицированы для признания и идентификации изменений [a)] и оценки статуса «пригодности использования» системы [b)1)].
- <b)4)>: Результаты измерений в отношении значимости изменений следует сообщать заинтересованным сторонам [a), b)].

<6.3.8> Процесс обеспечения качества

- <b)>: Оценка продукции и услуг должна быть выполнена как часть оценки адаптированной системы по отношению к цели адаптации [d)].
- <c)1)>: Сравнительная оценка процессов жизненного цикла проекта должна допускать непрерывное усовершенствование жизненного цикла системы [e)].
- <e)>: Для каждого рассматриваемого инцидента и проблемы необходимо исследовать существование изменения, которое может потребовать адаптации системы [a)2)].

<6.4.1> Процесс анализа деятельности или назначения

- <от a) до e)>: Процесс анализа деятельности или назначения следует проводить для выполнения [a), b)] (см. <6.4.1.1, примечание 2>). Условия принятия включают следующее:
  - изменения обнаружены в процессе эксплуатации и процессе технического обслуживания;
  - анализ процесса реагирования на отказ определяет цель улучшения жизненного цикла после действий реакции на отказ;
  - изменения в исходных данных к этому процессу идентифицированы.

Примечание 1 — Исходные данные для процесса анализа деятельности или назначения, которые могут изменяться, включают стратегию организации, идентифицированные проблемы и их возможности, цели и задачи организации, обеспечение использования систем или функций [a)1), примечание 1].

Результат процесса анализа деятельности или назначения должен включать четкие соглашения между заинтересованными сторонами относительно возможности начала адаптации системы и целях адаптации в соответствии с [b)3), b)2)].

- <a)1)>: Стратегия организации должна определять стартовые механизмы для периодического анализа проблем и возможности признания изменений, особенно в случае соответствующих событий [a)].
- <b), c)>: Определение проблемы, пространства возможностей и пространства характеристик решения должны сформировать основу для анализа воздействия изменений на статус «пригодности использования» системы и должны быть частью возможных целей адаптации [b)1), b)2)].
- <d)>: сравнительная оценка вариантов альтернативных решений должна дать информацию для принятия решения о начале адаптации системы [b)3)] и для определения возможных целей адаптации, как предпочтительных вариантов альтернативных решений [b)2)].
- <e)1)>: Прослеживаемость результатов анализа деятельности или назначения до и после изменений должна поддерживаться в дополнение к прослеживаемости между результатами анализа деятельности или назначения и артефактами в последующих стадиях жизненного цикла [d), e), f)].

<6.4.2> Потребности заинтересованных сторон и процесс определения требований

- <a) — f)>: Процесс определения требований и потребностей заинтересованных сторон должен быть утвержден всякий раз, когда это необходимо. Условия утверждения процесса такие же, как у процесса анализа деятельности или назначения.

Примечание 2 — Исходные данные для процесса определения требований и потребностей заинтересованных сторон, которые могут изменяться, включают выходные данные процесса анализа деятельности или назначения, определенное количество идентифицированных заинтересованных сторон, потребности заинтересованных сторон и условия, которые рассматривают для определения представительных сценариев.

- <a)1)>: Идентификация заинтересованных сторон должна поддержать менеджмент деструктивных изменений, в которых существующий список заинтересованных сторон может быть изменен [a),3)].
- <a)2)>: Стратегия определения требований и потребностей заинтересованных сторон должна включать план проведения анализа, который признает изменения у идентифицированных заинтересованных

сторон и определенные требования и потребности заинтересованных сторон. Такой анализ следует проводить периодически и всякий раз при необходимости [a)].

- <b), c)>: Определение потребностей заинтересованных сторон, обоснование (<b)>) и разработка концепций эксплуатации и других концепций жизненного цикла (<c)>) должны учитывать, что выходы формируют основу следующих действий, если изменения произойдут в будущем:
  - анализ воздействия изменений на статус «пригодности использования» системы [b)1)];
  - решение о продолжении адаптации системы [b)3)];
  - определение и согласование цели адаптации [b)2), b)3)].

Потребности заинтересованной стороны и их обоснование должны быть зарегистрированы способом, который помогает в будущей адаптации как «извлеченные уроки» [c)2)].

- <e)2)>: Критические показатели работы, которые поддерживают оценку адаптации, должны быть определены [d)].
- <e)4), f)1)>: Цели адаптации и соглашение по ним должны быть представлены как обновление определения требований заинтересованных сторон и четкого соглашения по требованиям заинтересованных сторон [b)3)].
- <f)2)>: Прослеживаемость между требованиями к системе до и после адаптации должна поддерживаться [f)1)].

<6.4.3> Процесс определения требований к системе

- <от a) до d)>: При необходимости должен быть выбран процесс определения требований к системе. Условия выбора такие же, как у процесса анализа деятельности или назначения.

Примечание 3 — Исходные данные для процесса определения требований к системе, которые могут меняться, включают требования заинтересованной стороны, условия использования, сценарии эксплуатации, особенности окружающей среды, ограничения для внедрения.

- <a)1), a)2), b)c)>: Определение функциональной границы (<a)1)>), стратегии определения требований к системе (<a)2)>), требований к системе (<b)>) и анализ требований к системе (<c)>) должны быть выполнены, чтобы их выходные данные поддерживали анализ воздействия будущих изменений на статус «пригодности использования» системы [b)1)] и определение цели адаптации [b)2)].
- <b)2)>: Необходимо выполнять мониторинг соблюдения ограничений для выявления изменений статуса этих ограничений как части распознавания возможных изменений оценки проекта и процесса управления [a)].
- <b)3)>: Должны быть идентифицированы требования к системе, которые относятся к риску, связанному с изменениями [a), b)1)].
- <b)4)>: Цель адаптации должна быть представлена как обновление определения требований к системе и обоснования, отражающего изменения окружающей среды, включая системы, связанные с исследуемой системой [b)2)]. Обоснование должно быть зарегистрировано, поддерживать оценку статуса «пригодности использования» системы [b)1)]; это помогает будущим адаптациям в качестве «извлеченных уроков» [c)2)].
- <c)1)>: Цель адаптации необходимо анализировать вместе с исходным набором требований к системе с точки зрения возможного нарушения функций системы и систем, связанных с исследуемой системой [c)5)], и результативностью предотвращения повторения отказов [b)3)].
- <c)2)>: Должны быть определены критические показатели работы, допускающие оценку адаптированной системы по отношению к цели [d)].
- <c)3)>: Обратная связь с компетентными заинтересованными сторонами относительно проанализированных требований должна допускать обмен информацией с заинтересованными сторонами, поддержку заинтересованных сторон при переговорах и отчет об адаптации [b)2)I), b)2)II), f)].
- <d)1)>: Соответствие цели адаптации должно быть отражено при обновлении четкого соглашения относительно требований к системе [b)3)].
- <d)2)>: Необходимо поддерживать прослеживаемость между требованиями к системе до и после адаптации [f)].

<6.4.4> Процесс определения структуры разрабатывает адаптацию изменений [c)4)].

- <от a) до f)>: При необходимости процесс определения структуры должен быть утвержден. Условия утверждения такие же, как и для процесса анализа деятельности или назначения.

Примечание 4 — Исходные данные процесса определения структуры, которые могут изменяться, включают требования к системе, условия рынка, регулирующие и правовые ограничения, назначение и бизнес-концепцию эксплуатации, технологические дорожные карты, обеспокоенность заинтересованных сторон, интерфейсы связанных систем и другие факторы, воздействующие на пригодность системы по всем стадиям жизненного цикла.

- <a)1), a)2), b), c)>: Идентификация ключевых факторов структуры и озабоченностей заинтересованных сторон (<a)1), a)2)>), разработка точек зрения на структуру и модели рассматриваемых структур (<b), c)>) должны быть выполнены таким образом, чтобы выходные данные поддерживали анализ воздействия будущих изменений на статус «пригодности использования» системы [b)1)].

- <a)4), b), c), e)>: Определенные критерии оценки структур, разработанных точек зрения на структуру, моделей рассматриваемых структур, результаты оценки рассматриваемых структур должны допускать определение цели адаптации и согласование ее [b)2), b)3)].

<6.4.5> Процесс определения проекта разрабатывает адаптацию изменений в соответствии с [c)4)].

- <от a) до d)>: При необходимости должен быть утвержден процесс определения проекта. Условия утверждения выбора такие же, как и для процесса анализа деятельности или назначения.

Примечание 5 — Исходные данные процесса определения проекта, которые могут изменяться, включают результат процесса определения структуры, доступные технологии, озабоченности заинтересованных сторон, прогноз устаревания элементов системы, интерфейсы с внешними юридическими лицами и доступные «технические объекты, не связанные с разработкой».

- <a)1), a)2), c)>: Определение необходимых технологий и типов необходимых характеристик проекта (<a)1), a)2)>) и оценка альтернатив получения элементов системы (<c)>) должны быть выполнены так, чтобы их выходные данные поддерживали анализ воздействия будущих изменений на статус «пригодности использования» системы [b)1)].

- <b), c)>: Установленные характеристики проекта, возможности проекта и результат оценки альтернатив получения элементов системы должны допускать определение цели адаптации и ее согласование [b)2)].

<6.4.6> Для оценки статуса «пригодности использования» системы должен быть использован процесс анализа системы [b)1)] и статус системы, адаптированной относительно цели адаптации [d)].

<6.4.7> Процесс внедрения осуществляет адаптацию к изменениям [c)4)]. Процесс внедрения вступает в действие, когда процесс определения проекта выполняет обновление проекта после изменений и когда ошибки изготовления идентифицированы при анализе процесса реагирования на отказ.

<6.4.8> Процесс интеграции реализует адаптацию к изменениям [c)4)]. Процесс интеграции вступает в действие, когда реализация элементов системы обновлена после изменений, а ошибки интеграции идентифицированы после отказов в процессе реагирования на отказ.

<6.4.9> Процесс верификации должен использоваться для оценки адаптированной системы по отношению к цели адаптации [d)] и для признания и идентификации изменений [a)] при выполнении различных видов анализа или оценки проекта и процесса управления, проводимых периодически.

<6.4.10> Процесс перемещения размещает адаптированные функции или систему [c)5)], оценивает адаптированную систему относительно цели адаптации [d)] и учитывает адаптацию до эксплуатации [f)]. Это включает идентификацию ответственных лиц или объектов, размещение адаптированных функций с наименьшим количеством нарушений в существующих функциях системы при эксплуатации и в других связанных системах. Процесс перемещения вступает в действие, когда адаптированная система интегрирована после изменений и когда требуется переустановка системы после изменений на место эксплуатации и в другую среду.

<6.4.11> Процесс валидации должен быть использован для оценки адаптированной системы относительно цели адаптации [d)] и для признания и идентификации изменений [a)] в различных видах анализа, проводимых периодически или при оценке проекта и процесса управления.

<6.4.12> Процесс эксплуатации контролирует эксплуатацию системы и ее окружающую среду таким образом, чтобы гарантировать признание и идентификацию изменений, которые могут потребовать адаптации системы [a)] и инициирования адаптации [b), c), d), e)] при помощи соответствующих процессов. Этот процесс учитывает адаптацию при выполнении анализа процесса обеспечения ответственности [f)].

<6.4.13> Процесс технического обслуживания помогает процессу оценки и управления проектом в управлении анализом процесса адаптации изменений, если проект системы стабилен и изменения в значительной степени прогнозируемы.

- Следующие действия должны быть выполнены как часть признания и идентификации изменений [a)]:

  - <a)2)>: идентификация ограничений системы для адаптации технического обслуживания;
  - <b)1)>: анализ инцидента и составление отчета о проблеме для идентификации будущих потребностей технического обслуживания;

- <b)6)>: действия по идентификации отказа при обнаружении несоответствия;
- <b)7)>: идентификация при необходимости адаптивного или перспективного технического обслуживания;
- <d)1)>: идентификация аномалий в техническом обслуживании и действиях логистики;
- <d)3)>: идентификация тенденций в инцидентах, проблемах, техническом обслуживании и действиях логистики;
- <d)6)>: мониторинг удовлетворенности потребителя системой и поддержкой технического обслуживания.
- Следующие действия должны быть выполнены как часть подготовки к адаптации [b)]:
- <a)2)>: идентификация ограничений системы для адаптации технического обслуживания;
- <a)3)>: идентификация компромиссных решений в системе, техническом обслуживании и действиях логистики;
- <b)1)>: анализ инцидента и составление отчета о проблеме для идентификации будущих потребностей технического обслуживания;
- <d)3)>: идентификация тенденций инцидентов, проблем, технического обслуживания и действий логистики.
- <b)2), d)2)>: Проблемы технического обслуживания и эксплуатации должны быть решены при помощи выбора соответствующих процессов [b), c), d), e)].

<6.4.14> Процесс распоряжения (вывода из эксплуатации)

- <b)3)>: Для адаптации изменений в будущем и улучшения жизненного цикла системы [e)] должна быть использована регистрация знаний об эксплуатации [c)2)].
- <c)1)>: Подтверждение того, что вредные для здоровья факторы и т. д. после утилизации элементов системы отсутствуют, должно быть учтено при адаптации [f)].
- <c)3)>: Архивированная информация, собранная за весь период функционирования системы, должна быть учтена при адаптации [f)] и зарегистрирована для использования в будущем при изменениях [c)2)].

Приложение А
(справочное)

Пример моделей жизненного цикла для обеспечения надежности открытых систем

А.1 Общие положения

В настоящем стандарте приведено четыре вида анализа процесса жизненного цикла, но не приведены модели жизненного цикла, использующие эти виды анализа процесса. В данном приложении приведены две модели жизненного цикла в качестве примера: модель жизненного цикла «обеспечение надежности открытых систем» и модель жизненного цикла «управление гарантийной цепочкой».

В приложении А угловые скобки (< >) использованы для обращения к номеру пункта процесса в *[1]*.

А.2 Модель жизненного цикла «обеспечение надежности открытых систем»

Модель жизненного цикла «обеспечение надежности открытых систем» (*[5]*) рассматривает следующие группы заинтересованных сторон:

- пользователи функций или продукции системы (общество в целом в случае систем социальной инфраструктуры);
- поставщики услуг или продукции;
- орган по сертификации функций (услуг) или продукции;
- поставщики систем, включая:
  - проектировщиков и разработчиков;
  - специалистов в области технического обслуживания и ремонта;
  - поставщиков аппаратных средств.

Модель жизненного цикла «обеспечение надежности открытых систем» организована в виде двух итеративных последовательностей действий, названных далее «циклами» (см. *[5]* и рисунок А.1): цикла адаптации изменений (внешняя петля) и цикла реагирования на отказ (внутренняя петля). В каждом цикле выполняют анализ одного и того же процесса, устанавливая последовательность и/или порядок работ, необходимых для анализа процесса. Эти два цикла также выполняют часть анализа процессов достижения консенсуса и обеспечения ответственности относительно аккомодации изменений и реагирования на отказ соответственно. Оба цикла начинаются со стадии эксплуатации.

a) Цикл адаптации изменений начинают, если система должна быть модифицирована в соответствии с изменением ее целей, задач, окружающей среды или фактического изготовления, цикл охватывает стадию достижения консенсуса, стадию разработки и стадию обеспечения ответственности.

b) Цикл реагирования на отказ начинают, если отказ произошел или спрогнозирован, цикл состоит из стадии реагирования на отказ и стадии обеспечения ответственности.

c) При необходимости после анализа причин отказа цикл реагирования на отказ может инициировать цикл адаптации изменений для модификации системы.

d) В базе данных с описанием соглашений хранятся свидетельства надежности и подлинники программы, которые автоматизируют мониторинг, действия реакции на отказ и обеспечение ответственности, основанные на свидетельствах надежности. Данные свидетельства надежности используют при эксплуатации системы. Эксплуатация системы интегрирована в процесс разработки, а свидетельства надежности непрерывно обновляются.

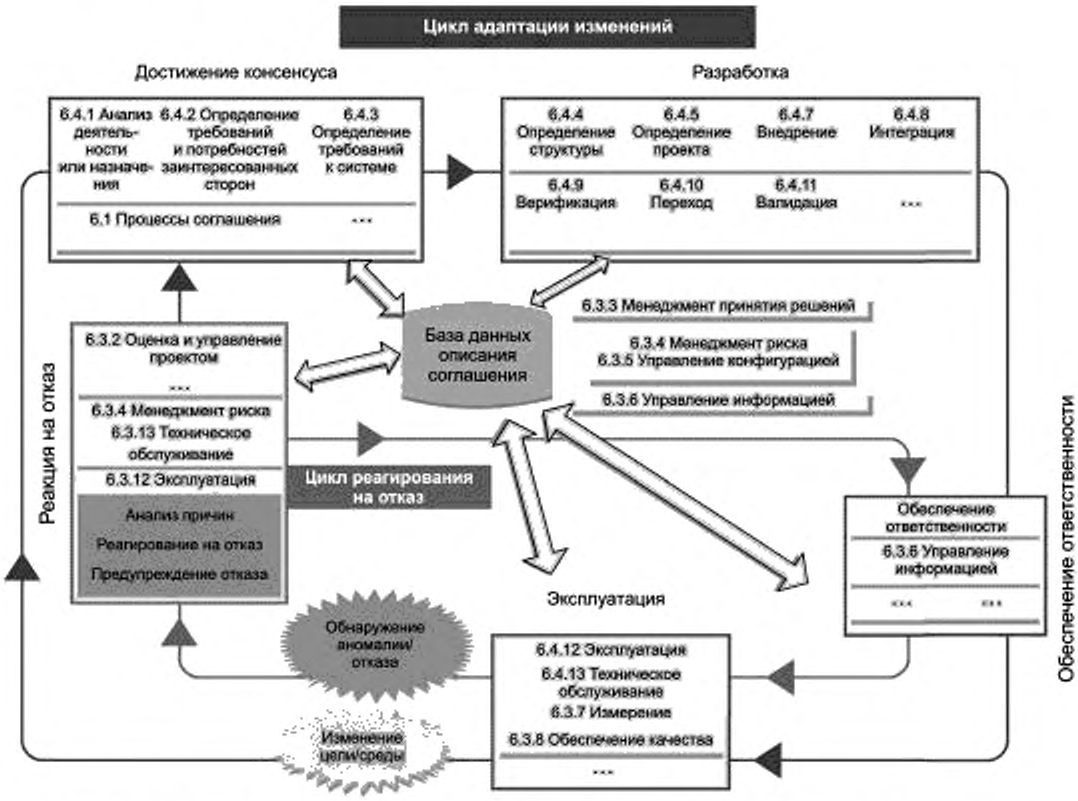

Рисунок А.1 — Модель жизненного цикла «обеспечение надежности открытых систем» (*[5]*, измененная)

У модели жизненного цикла «обеспечение надежности открытых систем» существует пять стадий. Далее перечислены результаты анализа и процессы жизненного цикла в соответствии с *[1]*, наиболее подходящие для каждой стадии.

- Стадия достижения консенсуса охватывает:
  - анализ процесса достижения консенсуса [6.2.2 a), b)];
  - начальные части анализа процесса обеспечения ответственности [6.3.2 от a) до e), g)];
  - начальные части анализа процесса реагирования на отказ [6.4.2 a)1), a)2)] и обновление консенсуса после отказов [6.4.2 d)];
  - начальные части анализа процесса аккомодации изменений [6.5.2 a), b)].

Соответствующие процессы жизненного цикла включают <6.1.1> процесс приобретения, <6.1.2> процесс поставки, <6.4.1> процесс анализа деятельности или назначения, <6.4.2> процесс определения требований и потребностей заинтересованных сторон, <6.4.3> процесс определения требований к системе.

Примечание 1 — Процессы жизненного цикла *[1]* применены одновременно, итеративно и рекурсивно к системе и на определенных этапах к ее элементам (см. <1.3> и <5.7>). Это особенно характерно для открытых систем. Так как открытая система непрерывно обновляется и изменяется, процессы, упомянутые выше, должны быть повторены несколько раз после того, как система была введена в эксплуатацию.

- Стадия разработки охватывает:
  - поддержку и мониторинг ответственности, так как приняты более детальные решения и результаты решений становятся доступными (6.3.2);
  - разработку реагирования на отказ [6.4.2 от a)3) до a)8)];
  - разработку и оценку адаптации [6.5.2 c), d)].

Соответствующие процессы жизненного цикла включают <6.4.4> процесс определения структуры, <6.4.5> процесс определения проекта, <6.4.7> процесс выполнения, <6.4.8> процесс интеграции, <6.4.9> процесс верификации, <6.4.10> процесс перемещения, <6.4.11> процесс валидации.

- Стадия обеспечения ответственности охватывает:
  - сбор необходимой информации, включая информацию о реагировании на отказ и адаптации к изменениям [6.3.2 f), g), 6.4.2 c), 6.5.2 f)];
  - выполнение обязательств ответственных заинтересованных сторон для обеспечения согласованных действий по запросам неответственных заинтересованных сторон [6.3.2 e), h)];
  - предоставление информации заинтересованным сторонам и обществу в целом [6.3.2 i)].

Соответствующие процессы жизненного цикла включают <6.3.6> процесс управления информацией.

- Стадия эксплуатации охватывает:
  - обнаружение отказов [6.4.2 b)1)];
  - выявление изменений [6.5.2 a)];
  - мониторинг для обеспечения ответственности и отчетности [6.3.2 f)].

Соответствующие процессы жизненного цикла включают <6.4.12> процесс эксплуатации, <6.4.13> процесс технического обслуживания, <6.3.7> процесс измерений, <6.3.8> процесс обеспечения качества.

- Стадия реагирования на отказ охватывает:
  - непосредственную реакцию на обнаруженные отказы [6.4.2 b)];
  - предоставление информации об отказах для обеспечения ответственности и постоянного улучшения [6.4.2 c), d)2)].

Соответствующие процессы жизненного цикла включают <6.3.2> процесс оценки и управления проектом, <6.3.4> процесс менеджмента риска, <6.4.12> процесс эксплуатации, <6.4.13> процесс технического обслуживания.

Примечание 2 — Упомянутое выше является упрощением и не является исчерпывающим. Каждая стадия затрагивает результаты анализа процесса, связанные со стадией, и каждый результат зависит от выполнения стадий, связанных с результатом.

Соответствие конкретного примера модели жизненного цикла «обеспечение надежности открытых систем» настоящему стандарту может быть установлено при помощи свидетельств надежности, демонстрирующих, что четыре вида анализа процесса, представленные в разделе 6, выполнены с помощью набора соответствующих процессов, действий и задач, показанных на рисунке А.1.

А.3 Модель жизненного цикла «управление гарантийной цепочкой»

Управление гарантийной цепочкой является менеджментом процесса циклической деятельности. Один цикл начинается при отказе, продолжается проведением анализа всех данных обратной связи и анализа первопричины (RCA), предоставлением потребителю пересмотренной продукции, которая соответствует его ожиданиям, и переходит на следующий цикл. Помимо отказов, в управлении гарантийной цепочкой рассматривают другие события, которые происходят в эксплуатации, а также на стадии разработки для начала цикла, так как открытая система непрерывно обновляется и изменяется. Управление гарантийной цепочкой включает превентивные действия, которые предназначены для сокращения количества отказов в будущем.

Процессы жизненного цикла, к которым применяют данную модель, разделяют на четыре группы: обслуживание потребителей, анализ отказов, разработка и цепочка поставок (см. рисунок А.2).

Обслуживание потребителей непрерывно использует техническое обслуживание продукции, в процессе которого принимают заявки потребителей, оказывают потребителям услуги по восстановлению продукции и фиксируют информацию о ее эксплуатации для дальнейшего анализа. Процесс анализа отказов осуществляет контроль информации об эксплуатации продукции и идентифицирует первопричины отказов и корректирующие действия. Процесс разработки охватывает технический менеджмент продукции, включая разработку продукции, технологии ее производства и управление портфолио. Цепочка поставок охватывает источники, производство, распределение и отвечает за производство и поставку продукции потребителю.

Управление гарантийной цепочкой объединяет четыре процесса жизненного цикла при помощи цикла Деминга — Шухарта: «Планирование — Выполнение — Проверка — Действие».

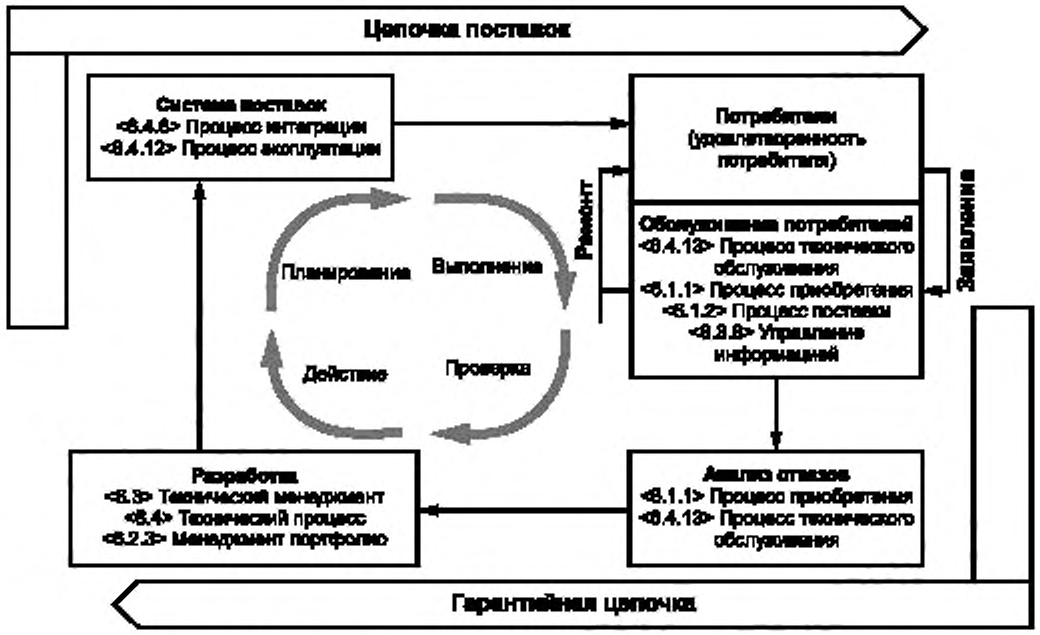

Рисунок А.2 — Модель жизненного цикла «управление гарантийной цепочкой»

Обслуживание потребителей (внутренний цикл) описывает части анализа процесса реагирования на отказ и анализа процесса обеспечения ответственности, которые непосредственно связаны с потребителем [6.4.2 b), 6.4.2 c), 6.3.2 h) и 6.3.2 i)]. Анализ отказов связан с начальной частью анализа процесса адаптации изменений, когда изменения в форме непредвиденных отказов обнаружены, проанализированы и идентифицированы корректирующие действия [6.5.2 a)2) и b)]. Разработка формирует адаптацию [6.5.2 c)4)]. Цепочка поставок развивает адаптацию [6.5.2 c)5)], так же как выполнение анализа процесса обеспечения консенсуса (6.2.2) между поставщиком и потребителем для формирования новых адаптированных функций (услуг) системы. Аналогично модель жизненного цикла обеспечивает цели, которые отображают результаты анализа других процессов.

Соответствие конкретного примера модели жизненного цикла «управления гарантийной цепочкой» настоящему стандарту может быть установлено с помощью свидетельств надежности, демонстрирующих, что четыре вида анализа процесса, представленные в разделе 6, выполнены с использованием набора соответствующих процессов, действий и задач, приведенных на рисунке А.2.

Приложение В
(справочное)

Образец свидетельства надежности

В.1 Общие положения

Ниже приведен образец структуры доказательств свидетельства надежности, связанный с обеспечением надежности открытых систем в соответствии с разделом 5. Структура доказательств приведена в *[10]*.

Примечание — В приложении В цели, приведенные в рамочках с пунктирными границами, должны быть проработаны далее в отдельных диаграммах.

Результаты анализа процесса являются целями; все неделимые цели являются результатами. Если результаты имеют иерархическую структуру, результаты верхних уровней становятся промежуточными целями. Промежуточная цель, которая не является результатом более высокого уровня, описывает установленный смысл группы целей более низкого уровня. Стратегии описывают обоснование декомпозиции цели.

Конкретный пример доказательства для данного жизненного цикла системы получен при помощи дальнейшей разработки и конкретизации целей и обеспечения свидетельств (решений) выполнения неделимых целей. Описания целей и стратегий должны быть исследованы на соответствие и достаточность в данной ситуации, структуру доказательств необходимо изменить и увеличивать при необходимости. Данный пример не содержит образцы текста и доказательств, которые также должны быть добавлены при необходимости.

Цель высшего уровня — «обеспечение непрерывности и ответственности функционирования постоянно изменяющейся системы» разделяют согласно четырем видам анализа процессов, представленным в настоящем стандарте. Декомпозиция цели означает идентификацию подцелей, достижение которых подразумевает достижение основной цели (см. рисунок В.1).

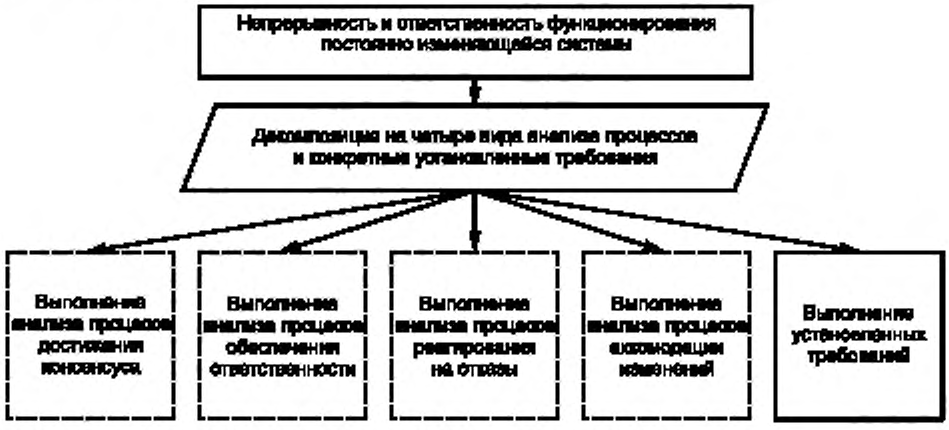

Рисунок В.1 — Общие доказательства

В.2 Доказательство достижения консенсуса

Описание цели «Выполнение анализа процесса достижения консенсуса» означает, что цель данного анализа процесса выполнена и, таким образом, расширена до следующего утверждения в соответствии с 6.2.1.

Общее понимание с четкими соглашениями о системе, ее целях, задачах, окружающей среде, фактической работе, жизненном цикле и их изменениях установлены и поддерживаются.

Доказательство разделено на установление понимания и соглашений и их поддержку (см. рисунок В.2). В пользу установления приведены доводы с точки зрения подготовки [6.2.2 a)1), a)2), a)4)], содержания [a)3), a)5)] и оценки результатов [a)6), a)7)] (см. рисунок В.3). Цели поддержки разделены на группы, в одной из которых приведены цели, связанные с действиями, необходимыми для поддержки [b)1), b)2), b)3)], а в другой — цели, обеспечивающие связь между действиями поддержки и поддержкой свидетельств надежности [b)4), b)5)] (см. рисунок В.4).

Рисунок В.2 — Достижение консенсуса 1

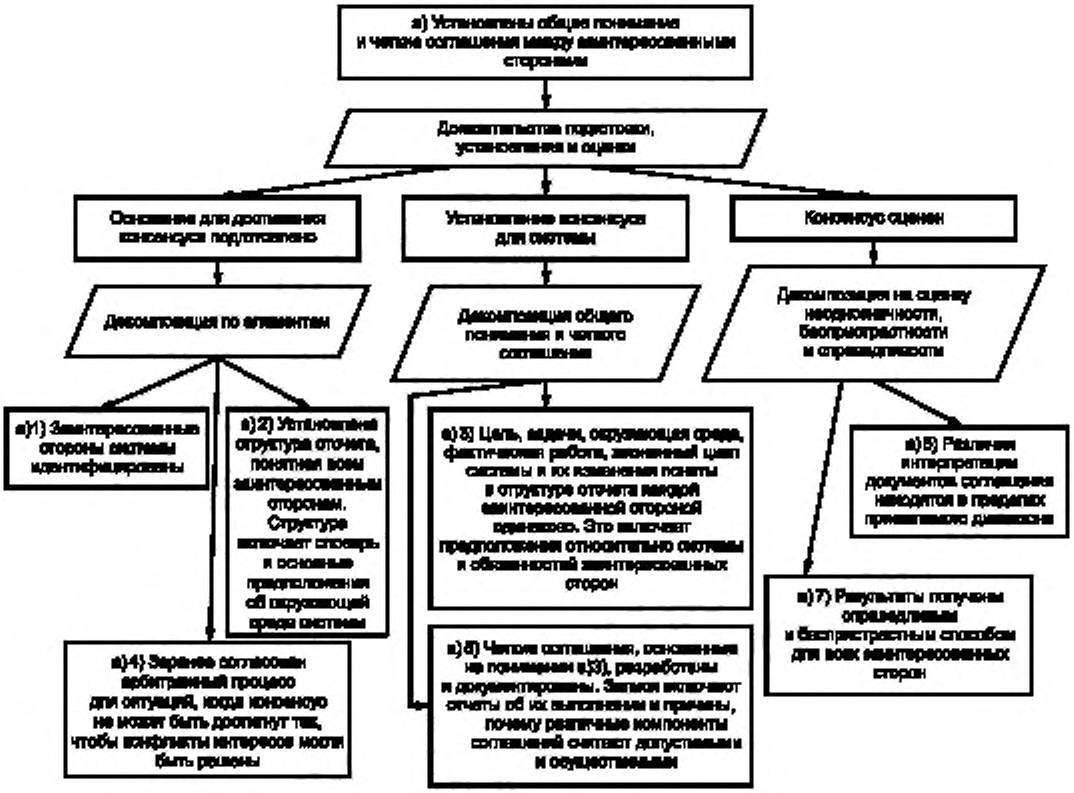

Рисунок В.3 — Достижение консенсуса 2

Рисунок В.4 — Достижение консенсуса 3

В.3 Доказательство обеспечения ответственности

Цель «Выполнение анализа процесса обеспечения ответственности» расширена до следующего утверждения в соответствии с целью анализа процесса (см. 6.3.1).

Установлены взаимосвязь между нарушением четкого соглашения и его последствиями для заинтересованных сторон и общества в целом. Они включают обязательства ответственных заинтересованных сторон способствовать реализации консенсуса в отношении системы для поддержки уверенности и доверия к системе и обеспечения доступности защиты от потенциальных повреждений.

Эта цель обоснована с точки зрения подготовки, которая происходит до возникновения событий, которые нужно учитывать, и фактического выполнения при возникновении событий, включая мониторинг (см. рисунок В.5). Подготовка, которая определяет, какой должна быть взаимосвязь, включает идентификацию и определение необходимых элементов [6.3.2 от a) до e)] (см. рисунок В.6). Цели выполнения разделены на две группы: цели, которые в пределах системы [от f) до h)] (см. рисунок В.7), и цели, которые должны быть получены за пределами системы [i), i)1), i)2), i)3), i)4), i)5)] (см. рисунок В.8).

Рисунок В.5 — Обеспечение ответственности 1

Рисунок В.6 — Обеспечение ответственности 2

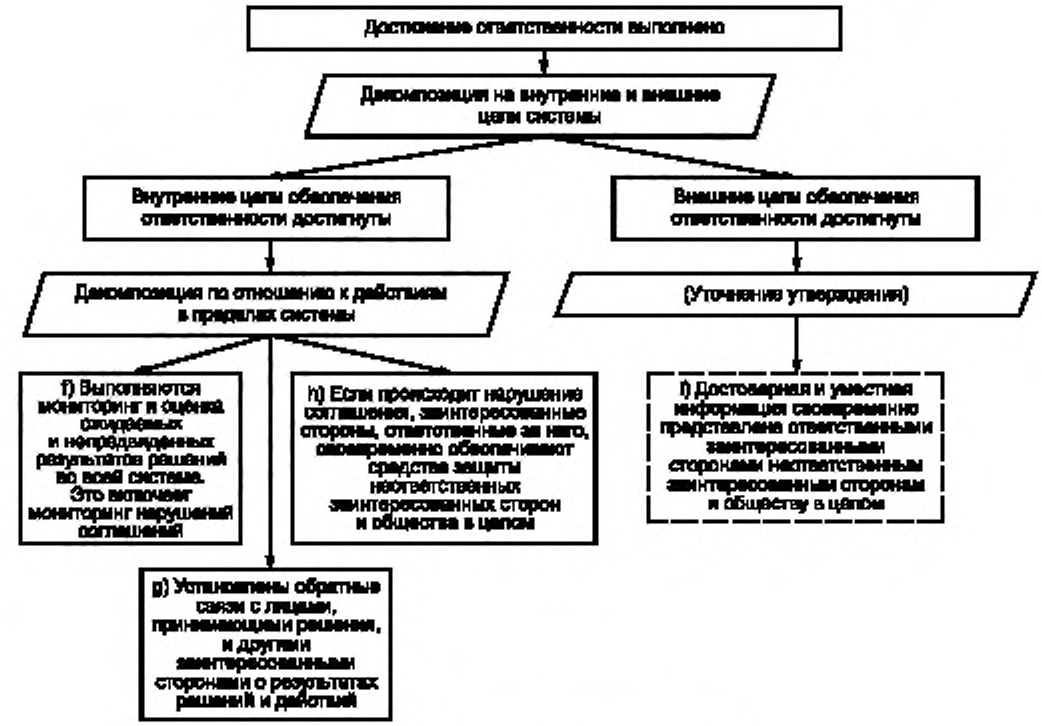

Рисунок В.7 — Обеспечение ответственности 3

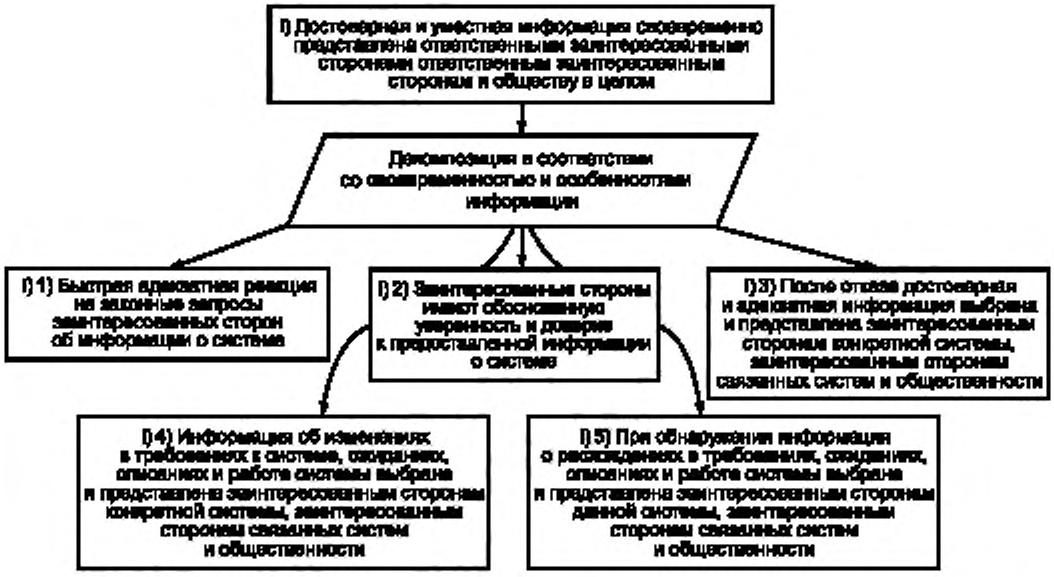

Рисунок В.8 — Обеспечение ответственности 4

В.4 Доказательство реагирования на отказ

Цель «Выполнение анализа процесса реагирования на отказ» расширена до следующего утверждения (см. 6.4.1).

Выполнение функций системы продолжается в полном объеме с наименьшими нарушениями и ущербом самым целесообразным способом.

Цель разделена на цель снижения вреда непосредственно от отказов и цель снижения последствий отказов (см. рисунок В.9). Доказательством снижения вреда непосредственно от отказов является подготовка до возникновения отказа [6.4.2 a)] и фактические действия при появлении отказа [b)]. Подготовка состоит из установления целей реагирования на отказ и разработки вариантов действий, обеспечивающих достижение целей. Установление целей реагирования на отказ включает идентификацию объектов защиты, причин отказа и определение этих целей для предотвращения отказов [a)1) — a)5)] (см. рисунок В.10). При разработке реакции на отказ рассматривают случаи, когда причины отказа идентифицированы, и случаи, когда они не идентифицированы. В первом случае разработка включает решение для каждой идентифицированной причины отказа независимо от того, установлена конкретная реакция на отказ или достаточно универсальной реакции в [a)6), a)7)] (см. рисунок В.11). В случае, когда причины отказа не идентифицированы, разрабатывают универсальные действия [a)8)]. Цель реагирования на отказ разделена на цель выполнения ответных действий и на цель оценки этих действий. Выполнение действий реакции на отказ демонстрируют: обнаружение, анализ отказа, улучшение действий в текущей ситуации и реагирование на отказ [от b)1) до b)5)]. Цели оценки реагирования на отказ включают оценку по отношению к цели анализа процесса [b)6), b)7)] и оценку относительно цели, установленной при анализе [b)8)] (см. рисунок В.12). Цель снижения последствий отказов разделяют на поддержку уверенности и доверия общества к системе, что является случаем обеспечения ответственности [c)], и непрерывного улучшения жизненного цикла системы, что является случаем адаптации изменений [d)] (см. рисунок В.9). Первый необходим для цели анализа процесса (см. 6.3.1) и состоит из целей ответственности после возникновения отказа [c)1) — c)4)] (см. рисунок В.13). Последний состоит из определения целей улучшения, включая предотвращение повторения отказа и соответствующие действия анализа процесса адаптации изменений [d)1), d)2)] (см. рисунок В.14).

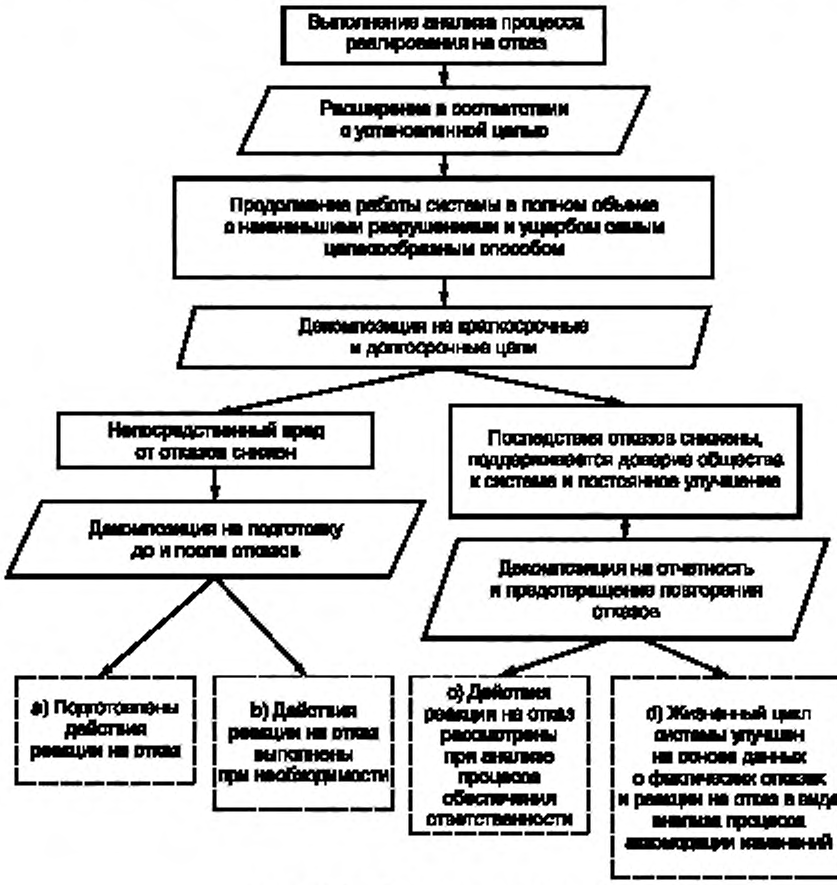

Рисунок В.9 — Реагирование на отказ 1

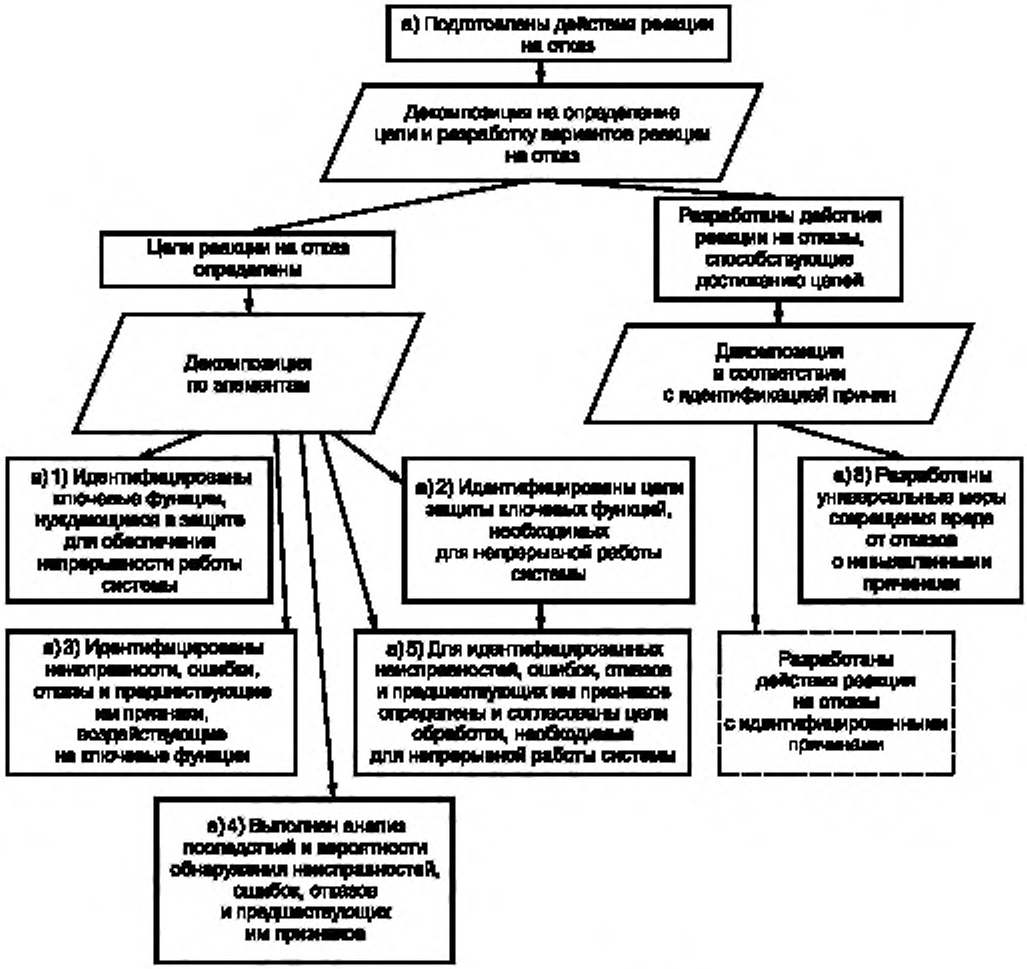

Рисунок В.10 — Реагирование на отказ 2

Рисунок В.11 — Реагирование на отказ 3

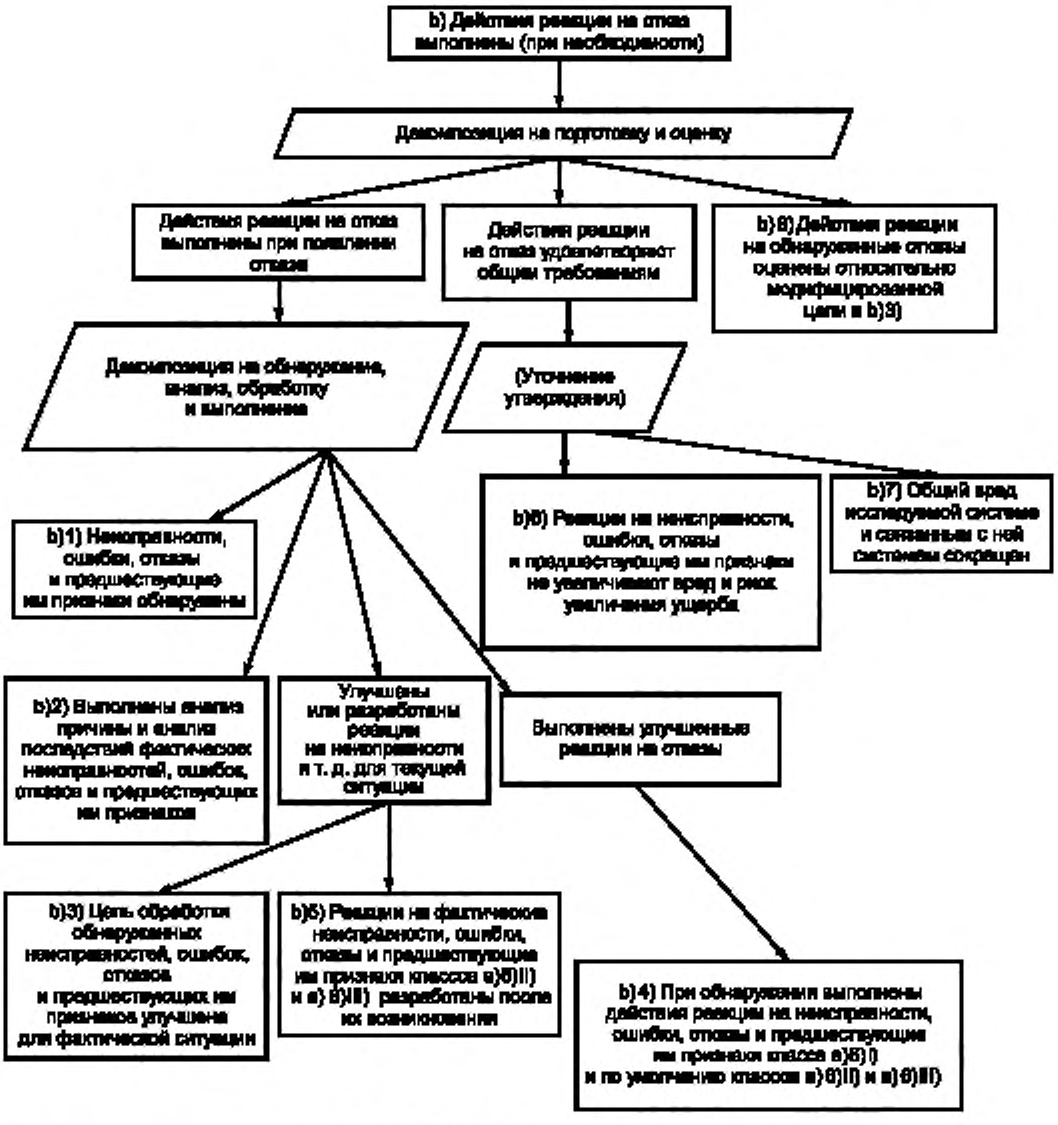

Рисунок В.12 — Реагирование на отказ 4

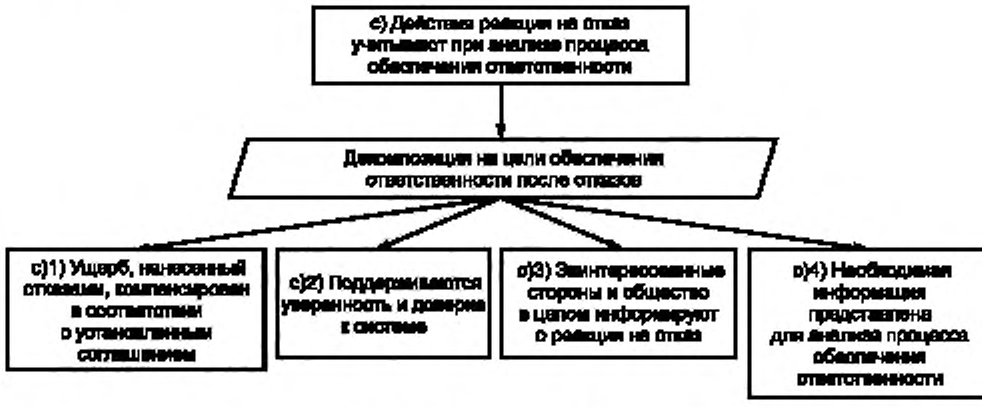

Рисунок В.13 — Реагирование на отказ 5

Рисунок В.14 — Реагирование на отказ 6

В.5 Доказательство адаптации изменений

Цель «Выполнение анализа процесса адаптации изменений» расширена до следующего утверждения согласно цели, приведенной в 6.5.1.

Статус «Пригодности использования» системы поддерживается, несмотря на изменения требований, окружающей среды, задач и/или целей.

Эту цель разделяют на цель адаптации системы к изменениям и на цель долгосрочной поддержки постоянного улучшения жизненного цикла системы, уверенности и доверия общества к системе. Доказательством первой цели являются идентификация изменений [6.5.2 a)], подготовка к адаптации [b)], выполнение адаптации [c)] и оценка [d)] (см. рисунок В.15). Цель идентификации изменений разделяют на цели идентификации типов изменений для наблюдений [a)1) — a)3)] (см. рисунок В.16). Доказательством выполнения цели подготовки к адаптации являются выполнение необходимых действий [b)1) — b)3)] (см. рисунок В.17). Цель выполнения адаптации рассмотрена с двух точек зрения: доступности необходимой поддержки [c)1), c)2)] и выполнения необходимых действий адаптации [c)3) — c)5)] (см. рисунок В.18). Первая часть цели постоянного улучшения оставлена неразработанной, но она должна быть разработана в условиях конкретной модели жизненного цикла, включая подробное описание, каким образом одна итерация анализа процесса адаптации изменений достигает длительных воздействий на будущие улучшения. Другая часть цели поддержка уверенности и доверия общества к системе является примером обеспечения ответственности для адаптации [f)], доказательством является доступность выполнения входных данных для анализа процесса обеспечения ответственности и то, что эти данные фиксируют в отчете об адаптации [f)1), f)2)] (см. рисунок В.15).

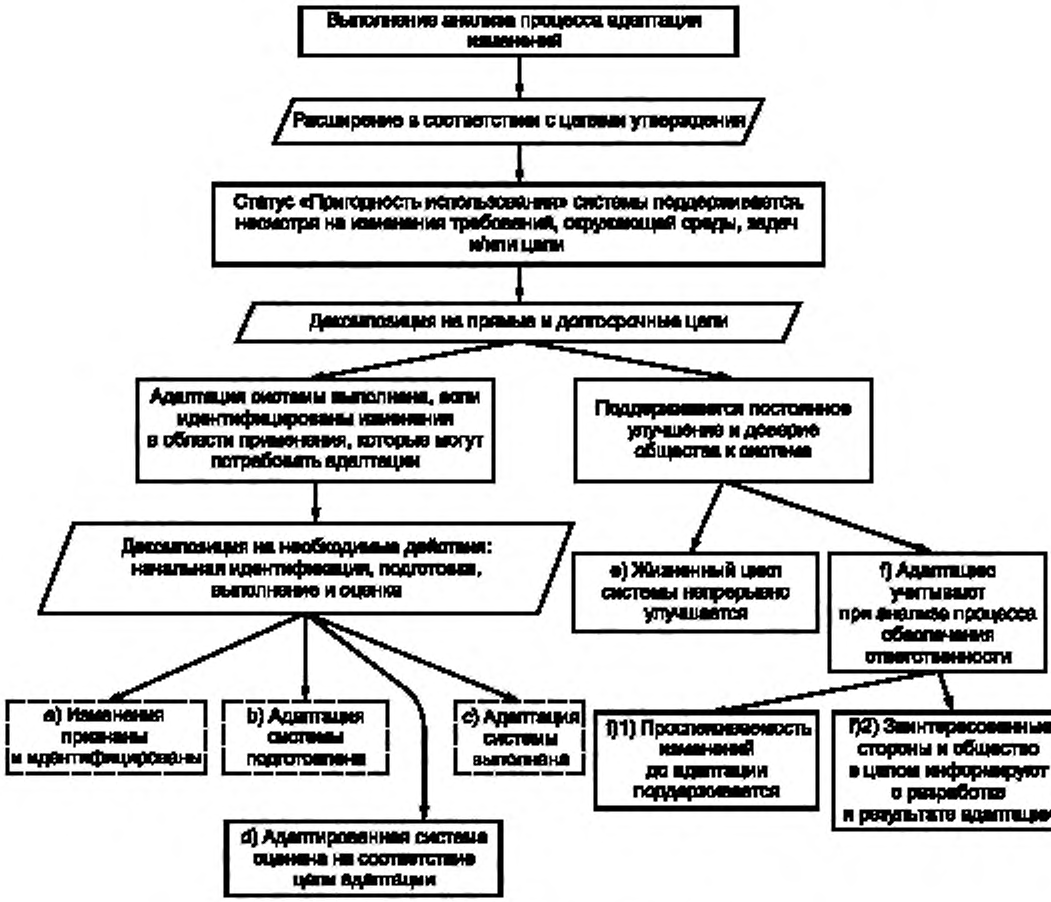

Рисунок В.15 — Адаптация изменений 1

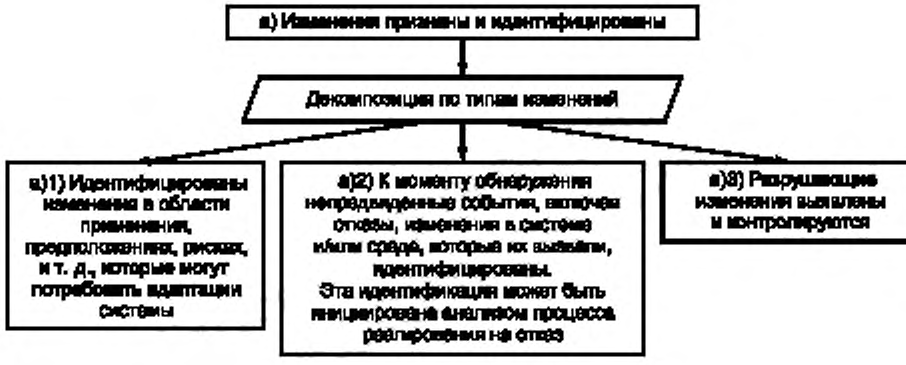

Рисунок В.16 — Адаптация изменений 2

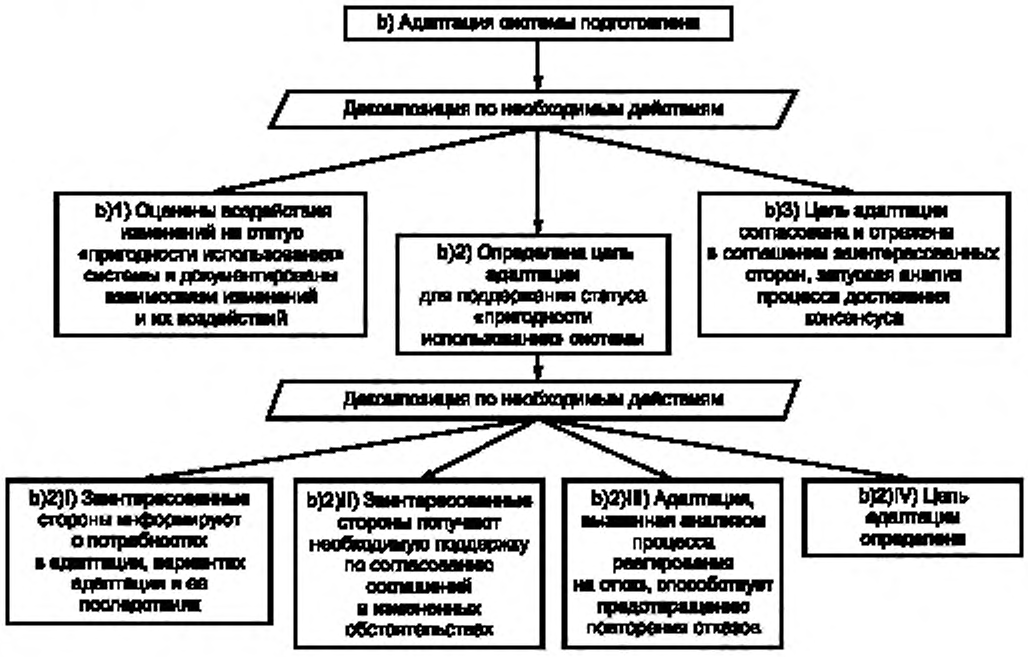

Рисунок В.17 — Адаптация изменений 3

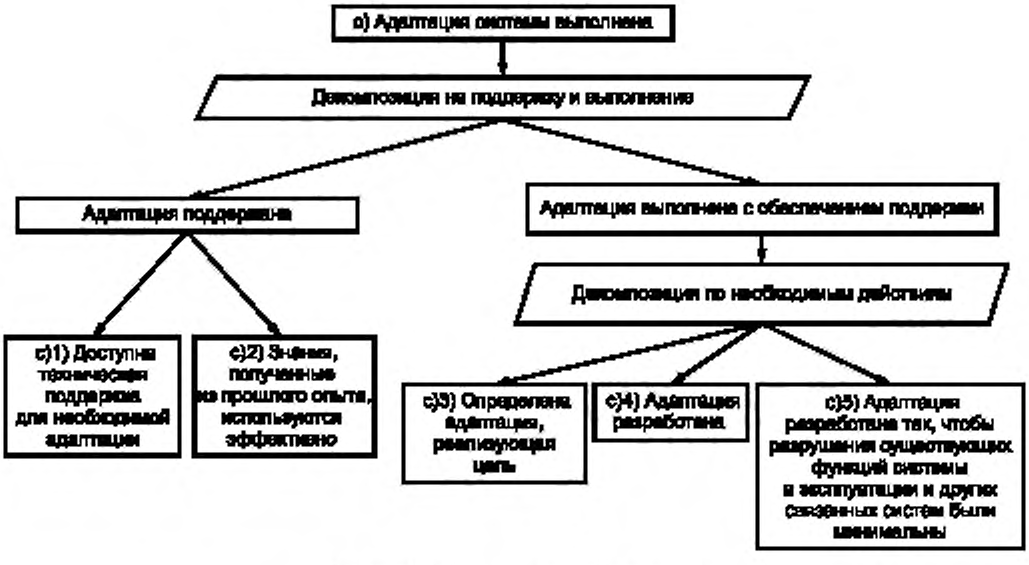

Рисунок В.18 — Адаптация изменений 4

Приложение С
(справочное)

Интеллектуальная электросеть

С.1 Общие положения

В данном приложении в качестве примера открытой системы приведено описание «интеллектуальной электросети» и показаны способы обеспечения надежности открытых систем. В качестве основы использована модель жизненного цикла «обеспечение надежности открытых систем», приведенная в приложении А.2. В С.3 показано построение свидетельств надежности интеллектуальной электросети в соответствии с положениями С.5. В С.4 описан цикл аккомодации изменений модели «обеспечения надежности открытых систем» жизненного цикла интеллектуальной электросети, которое реализует анализ процесса адаптации изменений (см. 6.5). В С.5 описан цикл реагирования на отказ, который реализует анализ процесса реагирования на отказ (см. 6.4). Оба цикла обеспечивают анализ процесса обеспечения ответственности в 6.3 и анализ процесса достижения консенсуса (см. 6.2) по изменению адаптации интеллектуальной электросети и реагированию на отказ соответственно. Пример основан на системе электросети Дании.

С.2 Предпосылки

Устойчивое и надежное электроснабжение имеет большое значение в современном обществе. Меры по энергосбережению и возобновляемым источникам энергии, такие как ветряные турбины и солнечные батареи, усложняют эксплуатацию и регулирование энергосистемы. Наиболее важными требованиями энергосистемы являются надежность (готовность и ее вклад в безотказность, ремонтопригодность) и обеспеченность технического обслуживания.

Собственность на системы распределения электроэнергии и собственность на производство и продажу электроэнергии принадлежит различным владельцам. Дистрибьюторы платят за использование электросетей для поставки электроэнергии, которую они покупают у поставщиков. Вместе с несколькими большими электростанциями, работающими на угле, и атомными электростанциями теперь существует большое количество небольших электростанций, производящих тепло и продающих электроэнергию. Потребители электроэнергии также во многих случаях являются производителями электроэнергии при помощи ветряных турбин или солнечных батарей. Изменение спроса и предложения в дневное и ночное время заставило установить цену на электроэнергию, которая изменяется каждый час. Поэтому было введено понятие интеллектуальной электросети. Оно включает в себя счетчики электроэнергии каждого потребителя с удаленным доступом для организации, эксплуатирующей сети. В то же время потребитель может заплатить цену за электроэнергию в зависимости от цены на рынке, которая изменяется каждый час. Потребитель может также продавать избыточное количество электроэнергии на рынке.

Электроэнергию очень трудно хранить. Это означает, что цена может быть отрицательной в периоды чрезмерной поставки, то есть поставщик должен заплатить, чтобы поставлять электроэнергию.

Программное обеспечение, которое управляет интеллектуальной системой электросети, является частью открытой системы, так как эта система постоянно изменяется с приходом новых потребителей, распространителей и производителей. Программное обеспечение связано с тысячами потребителей, многие из которых управляют программным обеспечением, чтобы управлять своими ветряными двигателями и солнечными батареями. Так как эти системы связаны с общественными электросетями, вся интеллектуальная электросеть является открытой системой и может оказаться под влиянием вредоносных программ. Поэтому необходима «межсетевая защита» как для потребителей, так и для поставщиков электроэнергии.

С.3 Построение свидетельств надежности интеллектуальной электросети

С.3.1 Общие положения

Для жизненного цикла интеллектуальной электросети должны быть созданы и поддерживаться свидетельства надежности, соответствующие 5. В С.3 показан возможный набор этапов этой работы, а также вопросы, которые должны быть рассмотрены на каждом этапе в случае интеллектуальной электросети. Ниже приведены девять этапов из описания свидетельств надежности в *[5]*.

С.3.2 Этапы построения свидетельств надежности интеллектуальной электросети

С.3.2.1 Этап 1: Определение жизненного цикла системы и идентификация входной и выходной документации для каждого этапа

Документы, обеспечивающие входные и выходные данные для всего жизненного цикла интеллектуальной электросети, формируют основу свидетельств надежности. Эти документы включают нормативные документы, правила управления и договора компании.

У оператора сети имеется своего рода концессия или собственность на энергосистему (опоры, кабели, трансформаторные станции высокого напряжения и распределительные сети низкого напряжения). Собственность может быть основана на законе или на собственности общественной или частной компании.

У оператора сети должны быть контракты со многими поставщиками и дистрибьюторами электроэнергии. Это могут быть крупные электростанции (угольные, атомные или гидроэлектрические) в их собственной стране или за рубежом. У них также могут быть контракты с операторами сети в разных странах. Оператор сети может покупать электроэнергию через дистрибьюторов у частных владельцев ветряных двигателей и парков солнечных батарей. Поставщик может быть потребителем или консорциумом. Все эти контракты содержат требования, которым должно соответствовать программное обеспечение. Например, требования о том, кто может поставлять электроэнергию, когда и по какой цене. Эта цена может быть различной для дня, ночи, времени года.

Оператор сети также имеет контракт с дистрибьюторами, покупающими электроэнергию на рынке (по постоянной или по переменной цене) и продающими электроэнергию потребителям. Это также должно быть отражено в программном обеспечении интеллектуальной электросети.

Жизненный цикл программного обеспечения интеллектуальной электросети состоит из следующих этапов:

- На этапе достижения консенсуса исходные данные поступают из консультации с органами, предоставляющими концессию, контролирующими органами, поставщиками и потребителями, а также документов и контрактов определяющих требования, до установки умных счетчиков по адресам потребителей. Этап начинается снова после реагирования на отказ или обнаружения изменений окружающей среды для улучшения и адаптации сети.

Этап разработки включает в себя следующие действия:

- Выполнение разработки структуры проекта после утверждения определения требований. Программное обеспечение разделено на подсистему, поддерживающую устойчивость энергосети (в пределах спецификаций), подсистему, покупающую и продающую электроэнергию и управляющую платежами, подсистему, управляющую контрактами, и подсистему, выполняющую мониторинг безопасности системы.

- Данные об определении требований и структуры проекта выполнены и проверены отдельно и вместе в системе программного обеспечения электросети последовательным объединением и процессом испытаний объединения. Система программного обеспечения испытана с прецедентами, сопровождаемыми испытаниями с моделируемыми данными эксплуатации. Наконец, безопасность, защита и испытания на перегрузку (испытания на скачки) выполнены на программном обеспечении. Программные коды, журналы разработки, результаты испытаний и другие данные являются выходной информацией.

- Этап обеспечения ответственности обеспечивает данные о соответствии требованиям до получения лицензии на эксплуатацию. Свидетельства и доказательства для контролирующих органов, поставщиков и потребителей гарантируют, что разработанная интеллектуальная электросеть удовлетворяет требованиям и контракты продолжают соблюдаться. Жизненный цикл снова переходит на этот этап после отказа или адаптации сети для составления отчета о реакции на отказ, улучшения установления компенсационных положений контрактов и обеспечения улучшения сети.

- На этапе эксплуатации внедряют окончательное программное обеспечение сначала в небольшой области, прежде чем оно будет внедрено на всем запланированном пространстве. Сеть и среда проверены на отказы и наличие изменений, которые могут потребовать восстановления консенсуса.

- На этапе реагирования на отказ происходит непосредственное реагирование на обнаруженные отказы в соответствии с планом, который требуется и/или определен в инструкциях и контрактах. Этот план устанавливает интерфейсы с чрезвычайными действиями многих служб, зависящих от сети. План не является совершенным, этап имеет встроенную гибкость для приспособления к ситуации и для увеличения реакций, требующих незапланированного участия лиц с более высокими полномочиями. На этом этапе регистрируют результаты реакции для использования на стадии обеспечения ответственности и следующей итерации стадии достижения консенсуса.

С.3.2.2 Этап 2: Классификация выходных документов

Далее показано, каким образом документы, идентифицированные на этапе 1, использованы при формировании свидетельств надежности и классифицированы соответственно. Ниже приведены возможные категории документов и международных стандартов.

- Стандарты по проблемам, отнесенным к интеллектуальной электросети включают *[11]*, *ГОСТ IEC 61000-4-30* и *[12]*.

- Результаты анализа риска интеллектуальной электросети получены при применении *ГОСТ Р 51901.12*, *ГОСТ Р 27.302* и *[13]*.

- Требования надежности для интеллектуальной электросети сформулированы на основе настоящего стандарта, *[2]* и *[14]*, *ГОСТ Р МЭК 60300-1*, *ГОСТ Р 27.003*, *[15]*, *ГОСТ Р 27.014* и *[16]*.

- Документы жизненного цикла, устанавливающие жизненный цикл интеллектуальной электросети, разработаны на основе настоящего стандарта, *ГОСТ Р МЭК 60300-1*, *[1]*, *ГОСТ Р 57098*, руководства *[17]*, *ГОСТ Р 57102*, *ГОСТ Р 56923*, *ГОСТ Р 58607*, *[18]* и *[19]*.

- Модели структуры системы сформулированы на основе *ГОСТ Р 57100*, *ГОСТ Р 51901.14* и других.

- Информация, связанная с эксплуатацией, приведена в *[11]*, *ГОСТ IEC 61000-4-30* и *[12]*.

- Информация, связанная с окружающей средой, классифицирована в соответствии с *[20]*.

- Результаты проверки и верификации соответствуют *[9]*.

- Программные коды. Программное обеспечение кодируют при помощи определенного языка. Коды — модули программного обеспечения, которое необходимо для поддержки постоянных напряжения и частоты в сети, контроля нагрузок и реакции на отказы, а также программного обеспечения для эксплуатации «системы защиты»

потребителей, дистрибьюторов, поставщиков и контроля необычных действий в сети (чрезмерные вариации потребления, необычные платежи, необычный поток данных и возможные вредоносные программы).

С.3.2.3 Этап 3: Установление требования высшего уровня «обеспечение непрерывности обслуживания и ответственности в постоянно изменяющейся системе»

После подготовки этапов 1 и 2 основная часть формирования свидетельств надежности начинается с определения требования высшего уровня. Использованная формулировка показывает связь с надежностью открытых систем. Чтобы определить это требование, надо установить его интерпретацию для интеллектуальной электросети посредством определений терминов (таких как «система», «непрерывность обслуживания») и разработки четкого текста. Энергосистема должна иметь наименьшую продолжительность неработоспособного состояния, сохранять установленные напряжение и частоту в сети при всех условиях нагрузки. Эти цели кодируют в виде формулировки требований высшего уровня.

С.3.2.4 Этап 4: Установление требований надежности, информации об окружающей среде и определений терминов для требования высшего уровня

Детали, установленные на этапе 3, и их связь с требованием высшего уровня четко зарегистрированы в свидетельствах надежности. Если *[10]* используется как в приложении В, свидетельства обеспечивают ссылки на документацию о деталях. Для интеллектуальной электросети: «энергосистема обязана иметь готовность 0,99997»; «в 98 % случаев периоды неработоспособного состояния должны быть менее 1 ч»; «напряжение, частота, их скачки и перебои должны удовлетворять установленным требованиям в течение 99,8 % времени»; «определения терминов в соответствии с *[2]* и *[14]*»; «географическим районом, охваченным энергосистемой, является Северная Европа с температурой, осадками, ветром и солнечным излучением в соответствии с *[21]*».

С.3.2.5 Этап 5: Планирование общей структуры свидетельств надежности

Планирование общей структуры начинается с образца, приведенного в приложении В. Пояснения образца для интеллектуальной электросети, т. е. его превращение в конкретное структурированное утверждение включает декомпозицию целей на подцели, определенные для интеллектуальной электросети, и формирование и/или улучшение стратегий обоснования новых и старых целей. Далее приведены примеры стратегий обоснования высших целей, установленных для интеллектуальной электросети.

a) Стратегии обоснования, основанные на жизненном цикле, подходят для целей, включающих:

1) концессию (юридический текст),

2) владение энергосистемой, документы свидетельства регистрации земельного налога, контракты,

3) трансформаторные станции, их спецификации и чертежи,

4) распределительные сети, схемы расположения кабелей и линий электропередач, соединения и мощности,

5) контракты с фермами ветряных двигателей и солнечных батарей.

b) Стратегии обоснования, основанные на функционировании системы, подходят для целей, включающих:

1) производительность поставщиков, жесткость сети.

c) Стратегии обоснования, основанные на технологическом процессе, подходят для целей, включающих:

1) вариации нагрузки и поставки,

2) вариации цен.

d) Стратегии обоснования, основанные на отказе и снижении риска, являются подходящими для целей, включающих:

1) прогноз нагрузки и поставки,

2) резервную мощность и резервирование,

3) процедуру отключения для уменьшения нагрузки,

4) процедуру подключения после отключения,

5) процедуру эксплуатации на небольшой территории,

6) процедуру защиты от вредоносных программ в системе управления,

7) процедуру защиты от вредоносных программ в согласовании цен и системе учета.

Примечание — Прогноз потребления может быть основан на хронологических данных для вариации нагрузки в течение дня и ночи, рабочих дней и праздников, лета и зимы. Прогноз объема поставки может быть основан на времени дня (солнечные батареи не работают ночью). Прогноз погоды может сообщать об облачности для солнечных батарей и скорости ветра для ветряных двигателей. Например, при большом шторме ветряные двигатели Дании производят достаточно электроэнергии для потребления всей страны. Однако через короткий промежуток времени ветряные двигатели выбывают из строя один за другим из-за слишком сильного ветра.

С.3.2.6 Этап 6: Приложение необходимых документов в качестве свидетельств

После того как общая структура доказательств определена, документы, необходимые для каждого довода, должны быть приложены. Классификацию документов исходной и выходной информации за весь жизненный цикл интеллектуальной электросети проводят на этом этапе.

С.3.2.7 Этап 7: Элементы свидетельств надежности могут быть получены из документов

Должны быть разработаны доказательства в контексте приложенных документов в соответствии с этапом 6. Стратегии обоснования часто включают обычные процедурные проверки сложного текста и свидетельств. Указания,

какая стратегия использована, часто недостаточно, чтобы восполнить расхождения между целью стратегии и ее подцелями и/или свидетельствами. В таком случае стратегии обоснований расширяют до элемента свидетельств надежности, который объясняет результат выполнения процедуры, в данном случае свидетельство надежности, основанное на содержании документов. Эти элементы свидетельств надежности часто получают автоматически, если документы хорошо структурированы.

С.3.2.8 Этап 8: Использование установленной структуры доказательств невыводимых элементов свидетельств надежности и свидетельств надежности в целом

Оставшиеся части общей запланированной структуры доказательств, которые не могут быть выведены на основе документов, представляют собой утверждения на основе мнений экспертов, принятых норм, согласованных предположений и мнений, неизбежных воздействий и т. п. Эти элементы свидетельств разрабатывают индивидуально. Это хорошая практика создания структуры доказательств, когда они успешно применены в аналогичных ситуациях. Разъяснение соответствующих стандартов и инструкций может создать хорошую структуру доказательств. Использование установленных структур доказательств помогает избежать трудностей при оценке других доказательств.

С.3.2.9 Этап 9: Повторение вышеупомянутых этапов столько раз, сколько необходимо

Свидетельства надежности должны часто обновляться, так как система является открытой.

Конфигурация сети изменяется, поскольку создают или выводят из эксплуатации кабели линий электропередач и трансформаторные станции.

Происходят изменения в количестве и возможностях поставщиков, особенно ферм ветряных двигателей и солнечных батарей. Потребители (заводы, офисы и частные хозяйства) часто изменяются, так же как и дистрибьюторы, которых они выбирают для поставки. Оператор сети обычно имеет концессию, которая требует, чтобы он поставлял энергию любому клиенту в указанном географическом районе.

Изменяются поставка и соглашение о цене.

Ниже рассмотрен цикл адаптации изменений и цикл реагирования на отказ (см. рисунок А.1).

Эти девять этапов представлены и рассмотрены в *[5]*.

С.4 Цикл адаптации изменений

Цикл адаптации изменений в модели «обеспечение надежности открытых систем» интеллектуальной электросети в целом осуществляет анализ процесса аккомодации изменений в соответствии с 6.5 относительно адаптации интеллектуальной электросети, а также анализ процесса обеспечения ответственности в соответствии с 6.3 и анализ процесса достижения консенсуса в соответствии с 6.2 (см. приложение А.2). После сбора информации о требованиях и анализе риска получено согласие заинтересованных сторон в соответствии с рисунком А.1. После этого начальная версия программного обеспечения открытой системы разработана, скомпонована, проверена и тестирована в соответствии с С.3.2.1. После лабораторного тестирования и проверки на ограниченной территории программное обеспечение принято к использованию. Отчетность четко выполнена для свидетельств надежности, которые сопровождают заявление для получения лицензии на эксплуатацию интеллектуальной электросети. Во время эксплуатации выполняют мониторинг результатов и задач. Проблемы и события разделяют на аномалии и отказы, с которыми работает цикл реагирования на отказ (см. С.5), и на изменения в задачах и/или окружающей среде, с которыми работает цикл адаптации изменений. Изменения в целях могут иметь более высокое значение для возобновляемого источника энергии, например пониженное выделение CO_2, большая прозрачная концессия и ценовая политика. Изменения в окружающей среде могут быть вызваны изменениями в структуре поставок, как, например, вывод из эксплуатации атомной электростанции, введение новых международных линий элекропередач, оборудования для аккумулирования энергии (водохранилища или емкости сжатого воздуха и т. п.). Изменениями в окружающей среде могут быть засуха и меньшее количество снега в областях с большими гидроэлекростанциями. Цикл адаптации изменений завершают новым сбором информации о требованиях и обновленным анализом риска, приводящими к обновлению соглашения заинтересованных сторон, которые вместе выполняют новый проект, его реализацию, верификацию и испытание. В этом отношении надежность открытых систем подобна спиральной модели разработки программного обеспечения с тем отличием, что для открытых систем спиральные процессы продолжаются в течение всей эксплуатации открытой системы, а не только во время начальной разработки как для программного обеспечения.

С.5 Цикл реагирования на отказ

Цикл реагирования на отказ в модели «обеспечение надежности открытых систем» интеллектуальной электросети в целом осуществляет анализ процесса реагирования на отказ в соответствии с 6.4, анализ процесса обеспечения ответственности относительно действий реакции на отказ в соответствии с 6.3 и анализ процесса достижения консенсуса в соответствии с 6.2 (см. приложение А.2). Цикл реагирования на отказ начинается с отказа или обнаружения аномалии. Отказом может быть, например, потеря мощности в одной из областей вследствие короткого замыкания в сети или на трансформаторной станции. Причиной могут быть удар молнии, перегрузка линий высокого напряжения от ветра, повреждения кабелей при земляных работах или повреждение подводных кабелей якорем судна. Такие отказы имеют тенденцию происходить внезапно, даже при наличии прогноза, например оценки вероятности отказа трансформатора на основе его срока службы и условий работы.

Первым действием при нарушении электроснабжения должна быть изоляция проблемы таким образом, чтобы она не распространилась дальше по системе. Может потребоваться отключение части системы для уменьшения нагрузки. В крайних случаях может возникнуть необходимость замены сети на определенном участке, то есть управления системой как обычной системой без поставки или доставки в закрытой области. Цель действий реакции на отказ состоит в том, чтобы восстановить электроснабжение всех потребителей за самое короткое время.

Это требует повторного контролируемого подключения поставщиков и потребителей. Основная часть этих действий может быть выполнена автоматически или полуавтоматически при наличии программных модулей контроля эксплуатации. Обнаружение (или прогнозирование) отказа начинает этап реакции на отказ, который состоит из предотвращения отказа, реакции на отказ и анализа причин отказа. Реакция на отказ описана выше. Анализ причин отказа — это действия по определению причин отключения электроснабжения (см. *[22]*). Некоторые типичные причины описаны выше. Предотвращение отказа включает, например, переход от линий электропередач на опорах к кабелям, профилактическому обслуживанию трансформаторных станций. Предотвращению отказа также помогает создание карт соединений кабелей для учета при земляных работах и запрет на постановку судов на якорь около подводных кабелей.

Для открытой системы обнаружение аномалии является очень важным действием. Модуль наблюдения за программным обеспечением должен непрерывно выявлять аномальные действия. Такое наблюдение должно прежде всего обнаруживать попытки проникновения в сеть и управления программным обеспечением при помощи вредоносных программ. Это может произойти через потребителей, у которых есть соединение сети с Интернетом, домашними устройствами, потребляющими мощность и производящими мощность, а также связь с согласованием цен, поставок и бухгалтерской подсистемой. Обнаружение аномалии также должно искать некорректный бухгалтерский учет, такой как чрезмерный денежный перевод и внезапные изменения в потреблении или поставке от потребителя. Это непрерывное обнаружение аномалии также очень важно для открытых систем, для закрытых систем со встроенным программным обеспечением это менее важно.

Операторы открытой системы должны поддерживать круглосуточную готовность к изоляции потенциальных вредоносных программ, анализу и удалению угрозы. Эти действия могут включать размещение некоторых адресов, например адресов потребителей, в карантин до тех пор, пока проблема не будет проанализирована и решена. Решение может включать соединение с циклами адаптации изменений посредством сбора информации о требовании анализа риска, согласования с заинтересованными сторонами и разработки блоков программного обеспечения (проект, реализация, проверка и тестирование).

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ IEC 61000-4-30—2017	IDT	IEC 61000-4-30:2015 «Электромагнитная совместимость (ЭМС). Часть 4-30. Методы испытаний и измерений. Методы измерений качества электрической энергии»
ГОСТ Р 27.003—2011	NEQ	IEC 60300-3-4:2007 «Управление надежностью. Часть 3. Руководство по применению. Раздел 4. Руководство по заданию технических требований к надежности»
ГОСТ Р 27.014—2019 (МЭК 62347:2006)	MOD	IEC 62347:2006 «Руководство по установлению требований к надежности систем»
ГОСТР 27.302—2009	NEQ	IEC 61025:2006 «Надежность в технике. Анализ дерева неисправностей»
ГОСТ Р ИСО 15489-1—2019	IDT	ISO 15489-1:2016 «Информация и документация. Управление документами. Часть 1. Понятия и принципы»
ГОСТ Р ИСО 26000—2012	IDT	ISO 26000:2010 «Руководство по социальной ответственности»
ГОСТ Р ИСО 31000—2019	IDT	ISO 31000:2018 «Менеджмент риска. Принципы и руководство»
ГОСТ Р ИСО/МЭК 31010—2011	IDT	ISO/IEC 31010:2009 «Менеджмент риска. Методы оценки риска»
ГОСТ Р 51897—2011	IDT	ISO Guide 73:2009 «Менеджмент риска. Словарь. Руководство по использованию в стандартах»
ГОСТ Р 51901.12—2007 (МЭК 60812:2006)	IDT	IEC 60812:2006 «Методы анализа надежности систем. Метод анализа видов и последствий отказов (FMEA)»
ГОСТ Р 51901.14 (МЭК 61078:2006)	MOD	IEC 61078:2006 «Методы анализа надежности систем. Структурная схема надежности и булевы методы»
ГОСТ Р 56923—2016/ ISO/IEC TR 24748-3:2011	IDT	ISO/IEC TR 24748-3:2011 «Информационные технологии (ИТ). Системная и программная инженерия. Управление жизненным циклом. Часть 3. Руководство по применению ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)»
ГОСТ Р 57098—2016/ ISO/IEC TR 24774:2010	IDT	ISO/IEC TR 24774:2010 «Системная и программная инженерия. Управление жизненным циклом. Руководство для описания процесса»
ГОСТ Р 57100—2016/ ISO/IEC/IEEE 42010:2011	IDT	ISO/IEC/IEEE 42010:2011 «Системная и программная инженерия. Описание архитектуры»
ГОСТ Р 57102—2016/ ISO/IEC TR 24748-2:2011	IDT	ISO/IEC TR 24748-2:2011 «Информационные технологии (ИТ). Системная и программная инженерия. Управление жизненным циклом. Часть 2. Руководство по применению ИСО/МЭК 15288»
ГОСТ Р 58607—2019/ ISO/IEC/IEEE 24748-4:2016	IDT	ISO/IEC/IEEE 24748-4:2016 «Системная и программная инженерия. Управление жизненным циклом. Часть 4. Планирование системной инженерии»
ГОСТ Р МЭК 60300-1—2017	IDT	IEC 60300-1:2014 «Менеджмент надежности. Часть 1. Руководство по управлению и применению. Руководство по применению менеджмента надежности»

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

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

Библиография

[1] *ISO/IEC/IEEE 15288:2015 Systems and software engineering — System life cycle processes*

[2] *IEC 60050-192, International Electrotechnical Vocabulary — Part 192: Dependability (available at http://www.electropedia.org/)*

[3] United Nations International Strategy for Disaster Reduction (UNISDR). Terminology on Disaster Risk Reduction, 2009

[4] Laprie, Jean-Claude. «From dependability to resilience». 38th IEEE/IFIP Int. Conf. On Dependable Systems and Networks, 2008

[5] Tokoro, Mario, ed. Open Systems Dependability — Dependability Engineering for Ever — Changing Systems. Second edition, CRC Press, 2015

[6] Bloomfield, Robin and Gashi, Ilir. Evaluating the resilience and security of boundaryless, evolving socio-technical systems of systems. Research report to DSTL, Centre for Software Reliability, City University, London, 2008

[7] Jamshidi, Mohammad, ed. System of systems engineering: innovations for the twenty-first century. John Wiley & Sons, 2011

[8] *ISO/IEC 15026-2:2011 Systems and software engineering — Systems and software assurance — Part 2: Assurance case*

[9] *IEC 62741:2015, Demonstration of dependability requirements — The dependability case*

[10] Origin Consulting LLC. GSN Community Stsndsrd Version 1 November 2011 [viewed 2016-01-14]. Available as www.goalstructuringnotation.info/documents/GSN_Standard.pdf

[11] *IEC 61850:2020 SER Series Communication networks and systems for power utility automation — ALL PARTS*

[12] *IEC TR 62351-12:2016 Power systems management and associated information exchange — Data and communications security — Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems*

[13] *IEC 62551(2012) Analysis techniques for dependability — Petri net techniques*

[14] *IEC 60050-692:2017 International electrotechnical vocabulary — Part 692: Generation, transmission and distribution of electrical energy — Dependability and quality of service of electric power systems*

[15] *IEC 61907:2009 Communication network dependability engineering*

[16] *IEC 62673:2013 Methodology for communication network dependability assessment and assurance*

[17] *ISO/IEC/IEEE 24748-1:2018 Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management*

[18] *ISO/IEC/IEEE 24748-5:2017 Systems and software engineering — Life cycle management — Part 5: Software development planning*

[19] *ISO/IEC TS 24748-6:2016 Systems and software engineering — Life cycle management — Part 6: System integration engineering*

[20] *IEC 60721 Classification of environmental conditions — ALL PARTS*

[21] *IEC 61721:1995 Susceptibility of a photovoltaic (PV) module to accidental impact damage (resistance to impact test)*

[22] *IEC 62740:2015 Root cause analysis (RCA)*

УДК 621.745.552:006.354

МКС 03.100.40
03.120.01
21.020

Ключевые слова: надежность, надежность открытых систем, менеджмент надежности, система, жизненный цикл системы, открытые системы

БЗ 9—2020/23

Редактор *В.Н. Шмельков*
Технические редакторы *В.Н. Прусакова, И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Половой*

Сдано в набор 10.08.2020. Подписано в печать 04.09.2020. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 7,44. Уч.-изд. л. 7,16. Тираж 40 экз. Зак. 669.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
www.jurisizdat.ru y-book@mail.ru

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ»,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru