ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15026-1— 2016

СИСТЕМНАЯ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

Гарантирование систем и программного обеспечения

Часть 1

Понятия и словарь

(ISO/IEC 15026-1:2013, IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 апреля 2016 г. № 281-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15026-1:2013 «Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 1. Понятия и словарь» (ISO/IEC 15026-1:2013 «Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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

Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) образуют специализированную систему для всемирной стандартизации. Национальные органы по стандартизации, которые являются членами ИСО или МЭК, участвуют в разработке международных стандартов через технические комитеты, созданные соответствующей организацией для определенных областей технической деятельности. Технические комитеты ИСО и МЭК сотрудничают в сферах, представляющих взаимный интерес. Другие международные правительственные и неправительственные организации, связанные с ИСО и МЭК, также принимают участие в работе по разработке стандартов. В сфере информационной технологии ИСО и МЭК учредили совместный технический комитет ИСО/МЭК СТК 1.

Международные стандарты разрабатываются в соответствии с правилами, приведенными в Директивах ИСО/МЭК, Часть 2.

Основная задача совместного технического комитета состоит в подготовке международных стандартов. Проекты международных стандартов, принятые совместным техническим комитетом, распространяются среди национальных органов по стандартизации для вынесения решения. Для публикации в качестве международного стандарта требуется одобрение по крайней мере 75 % национальных органов по стандартизации, участвующих в голосовании.

Следует обратить внимание на тот факт, что отдельные элементы настоящего стандарта могут являться объектами патентного права. ИСО и МЭК не несут ответственность за установление какого-либо или всех подобных патентных прав.

ИСО/МЭК 15026-1 был подготовлен Подкомитетом 7 «*Системная и программная инженерия*» совместного технического комитета ИСО/МЭК СТК 1 «*Информационные технологии*».

Первая редакция настоящего стандарта отменяет действие и заменяет пересмотренный документ ИСО/МЭК ТО 15026-1:2010.

ИСО/МЭК 15026 с общим названием «*Системная и программная инженерия. Гарантирование систем и программного обеспечения*» состоит из следующих частей:

- *Часть 1. Понятия и словарь*;
- *Часть 2.Гарантийный случай*;
- *Часть 3. Уровни целостности системы*;
- *Часть 4. Гарантии жизненного цикла.*

В разработке международных стандартов ИСО/МЭК 15026 вместе с ИСО/МЭК СТК 1 принимало участие компьютерное сообщество ИИЭР. В качестве базовых документов для настоящего стандарта использовались стандарты: ИИЭР Std 1228—1994 и ИИЭР для плана обеспечения безопасности.

В областях, относящихся к гарантированию качества программного обеспечения и систем, а также в связанных с ним областях применяют одни и те же понятия, однако пользуются разными словарями и концепциями. Настоящий стандарт представляет унифицированный набор базовых понятий и однозначное толкование терминов во всех таких областях. Таким образом, обеспечивается основа для уточнения, обсуждения, соглашения о записи и обоснования унифицированных понятий и словаря, единообразно используемых во всех частях ИСО/МЭК 15026.

Настоящий стандарт разъясняет понятия, необходимые для описания гарантирования качества программного обеспечения и систем, и в частности основные понятия, используемые в стандартах, начиная с ИСО/МЭК 15026-1 до ИСО/МЭК 15026-4. Этим обеспечивается совместное использование понятий, концепций и терминологии, которые могут быть использованы для множества различных свойств, областей приложения и технологий.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМНАЯ И ПРОГРАММНАЯ ИНЖЕНЕРИЯ

Гарантирование систем и программного обеспечения

Часть 1

Понятия и словарь

Systems and software engineering. Systems and software assurance. Part 1.Concepts and vocabulary

Дата введения — 2017—06—01

1 Область применения

Настоящий стандарт определяет относящиеся к гарантии термины и представляет упорядоченный набор понятий и отношений между ними, обеспечивая основы единого понимания гарантии в пользовательских сообществах. Кроме того, предоставлена информация по использованию других частей ИСО/МЭК 15026, в том числе по совместному использованию нескольких частей. Для «гарантийного случая» существенным понятием, из представленных в ИСО/МЭК 15026, является понятие «претензия» (требование) и поддержка такой претензии посредством «аргументации» и «доказательств». Эти претензии тесно связаны с гарантированием свойств систем и программного обеспечения в процессах жизненного цикла системного или программного продукта.

ИСО/МЭК 15026 не применим для гарантирования службы, которая эксплуатируется и управляется непрерывно.

2 Применимость

2.1 Целевая аудитория

Среди множества потенциальных пользователей ИСО/МЭК 15026, в число которых входят разработчики и специалисты по обслуживанию гарантийных случаев, имеются те, кто хочет разработать, поддерживать, оценить или заказать систему с определенными требованиями к конкретным свойствам, чтобы быть более уверенным в этих свойствах и требованиях к ним. В ИСО/МЭК 15026 используются понятия и термины, соответствующие ИСО/МЭК 12207 и ИСО/МЭК 15288 и в общем случае серии стандартов ИСО/МЭК 25000. Однако потенциальные пользователи ИСО/МЭК 15026 должны представлять различия между этими понятиями и терминами и, возможно, привычными для них понятиями и определениями. В настоящем стандарте эти различия разъяснены.

2.2 Область применимости

Основная цель настоящего стандарта состоит в том, чтобы помочь использовать другие части ИСО/МЭК 15026, представив контекст, понятия и определения следующих терминов: гарантия, гарантийный случай и уровень целостности. Однако такие важные для практического использования точные детали гарантии, как, например, измерение, демонстрация или анализ конкретных свойств, выходят за рамки настоящего стандарта. Эти детали являются предметом других специализированных стандартов, на которые имеются ссылки и которые включены в элемент «Библиография».

3 Термины и определения

В настоящем стандарте использованы следующие термины и определения, данные в ИСО/МЭК 15026, а также перечисленные ниже термины с соответствующими определениями.

Издание официальное

Примечание — Во всех частях ИСО/МЭК 15026 использованы единые термины.

3.1 Термины, относящиеся к гарантии и свойствам

3.1.1 **гарантия, гарантирование** (assurance):Основание для утверждения, что требование выполнено или будет выполнено.

3.1.2 **претензия, требование** (claim):Утверждение типа «истина/ложь» о выполнении ограничений на значения однозначно определенных свойств (называемых связанными с претензией свойствами), а также ограничений на неопределенность значений свойств в пределах этих ограничений в случае применимости претензии при указанных условиях.

Примечания

1 Неопределенность также может быть связана с продолжительностью применимости и заданными условиями.

2 Претензия может включать в себя следующее:

- свойство, относящееся к претензии;
- ограничения на значение свойства, связанного с претензией (например, диапазон значений);
- ограничения на неопределенность значения свойства, удовлетворяющего ограничениям;
- ограничения на продолжительность применимости претензии;
- связанная с продолжительностью неопределенность;
- ограничения на условия, связанные с претензией;
- связанная с условием неопределенность.

3 Термин «ограничения» используется для соответствия многим возможным ситуациям. Значением могут быть как единственная величина, так и множество величин, диапазон значений или множество диапазонов значений. Значения могут быть многомерными. В некоторых случаях границы этих ограничений нечетко выражены. Например, они могут быть заданы вероятностным распределением, а также могут быть инкрементными.

3.1.3 **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 — 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.

3.1.4 **функциональная надежность** (dependability):Собирательный термин, используемый для описания эксплуатационной готовности и влияющих на нее факторов: показатель надежности, показатель ремонтопригодности и показатель технического обслуживания.

Примечания

1 Термин «надежность» применяется только для общего неколичественного описания.

2 В ИСО/МЭК 25010 [99] отмечено, что «характеристики функциональной надежности включают в себя готовность и свойственные ей или внешние факторы влияния, такие как надежность, отказоустойчивость, восстанавливаемость, целостность, защищенность, сопровождаемость, долговечность и поддержка технического обслуживания». Надежность рассматривается в нескольких стандартах (например, [64] и [69]), а кроме того, многие стандарты посвящены качеству надежности. В МЭК 60050-191 [63]приводятся соответствующие определения.

[МЭК 60300-1:2003]

3.2 Термины, относящиеся к продуктам и процессам

3.2.1 **процесс** (process): Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующих входы в выходы.

[ИСО/МЭК 15288:2008 и ИСО/МЭК 12207:2008]

3.2.2 **представление процесса** (process view):Описание того, как указанная цель и совокупность результатов могут быть достигнуты с использованием действий и задач существующих процессов.

[ИСО/МЭК 15288:2008, D.3]

3.2.3 **продукт** (product):Результат процесса.

Примечания

1 Результатами могут быть компоненты, системы, программное обеспечение, службы, правила, документы или многое другое.

2 В качестве результата в некоторых случаях может быть множество связанных между собой отдельных результатов. Однако претензии, как правило, связаны с конкретными версиями продукта.

[ИСО/МЭК 15288:2008 и ИСО 9000:2005]

3.2.4 **система** (system):Комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей.

Примечания

1 Систему можно рассматривать как продукт или предоставляемые услуги.

2 На практике интерпретация значения термина часто уточняется посредством ассоциативного существительного, например «система самолета». Кроме того, слово «система» может быть заменено просто контекстно-зависимым синонимом, например «самолет», хотя подобная замена может скрыть аспекты системных принципов.

[ИСО/МЭК 15288:2008]

3.2.5 **требование** (requirement):Утверждение, которое отражает или выражает потребность и связанные с ней ограничения и условия.

Примечание —Требования существуют на различных уровнях и выражают потребность в высокоуровневой форме (например, требование компонента программного обеспечения).

[ИСО/МЭК/ИИЭР 29148:2011]

3.2.6 **элемент системы** (system element):Представитель совокупности компонентов, образующих систему.

Примечание — Элемент системы — это дискретный компонент системы, который может быть реализован для выполнения определенных требований. Элемент системы может представлять собой аппаратные средства, программное обеспечение, данные, людей, процессы (например, процессы для предоставления услуг пользователям), процедуры (например, инструкции оператору), средства, материалы и естественные объекты (например, вода, организмы, полезные ископаемые) или любую их комбинацию.

[ИСО/МЭК 15288:2008]

3.3 Термины, относящиеся к уровню целостности

3.3.1 **уровень целостности** (integrity level):Требования системы, продукта или элемента, содержащие в себе ограничения значений свойства, область применения требований и допустимую неопределенность достижения требований.

Примечания

1 Как правило, целью является поддержка ограничений значений свойств, связанных с соответствующими аспектами, что приводит к удержанию системных рисков в определенных рамках.

2 Адаптировано из ИСО/МЭК 15026:1998.

3.3.2 **требования уровня целостности** (integrity level requirements): Набор определенных требований, предъявляемых к характеристикам системы, продукта или элемента, и связанных с ними аспектов, необходимых для достижения заданного уровня целостности (то есть выполнения условий) при удовлетворении ограничений на неопределенности, включая получение необходимых доказательств.

Примечания

1 Так как уровень целостности определен как требования, то «достижение заданного уровня целостности» эквивалентно «выполнению требований».

2 В ИСО/МЭК 15026:1998 (пункты 3.3.1 и 3.3.2) использованы понятия «уровень целостности» и «требования целостности» соответственно. Для большей ясности и в целях использования той же терминологии, что применяется в области безопасности, последнее понятие было заменено на «требования уровня целостности».

3 ИИЭР 1012:2004 определяет уровень целостности как «значение, представляющее уникальные для проекта характеристики (например, сложность программного обеспечения, критичность, риск, уровень защищенности, уровень безопасности, требуемая производительность, надежность), которые и определяют важность программного обеспечения для пользователя». То есть уровень целостности является значением свойства целевого программного обеспечения. Поскольку и требование, и утверждение того, что свойство имеет определенное значение, могут рассматриваться в качестве характеристики системы или программного обеспечения, то оба определения уровней целостности, в сущности, одинаковы.

3.4 Термины, относящиеся к условиям и последствиям

3.4.1 **последствие** (consequence):Эффект (изменение или отсутствие изменения), как правило, связанный с событием, состоянием или системой и, как правило, допускаемый, обусловленный, предотвращенный или измененный событием, состоянием или системой либо способствующий им.

Примечание — Следствием эффекта может быть выгода, ущерб либо ни то, ни другое.

3.4.2 **негативное последствие** (adverse consequence):Нежелательное последствие, связанное с ущербом.

3.4.3 **желательное (или положительное) последствие** (desirable (or positive) consequence):Последствие, результатом которого является выгода или преимущество либо предотвращение негативного последствия.

3.4.4 **дефект** (error): Недопустимое состояние системы.

3.4.5 **ошибка** (fault): Недостаток в системе или ее представлении, при активации (при выполнении) которого система может перейти в недопустимое состояние.

Примечание — Дефекты могут быть и в спецификациях в случае наличия в них ошибок.

3.4.6 **атака** (attack):Злонамеренное воздействие на систему или взаимодействие с системой или ее средой при наличии потенциала проявления дефекта или ошибки (а следовательно, и возможного отказа) или другого негативного последствия.

3.4.7 **нарушение** (violation):Поведение, действие или событие системы, выходящие за рамки требуемых свойств или требований.

Примечание — В области безопасности термин «нарушение» использован для описания преднамеренного нарушения процедуры или правила человеком.

3.4.8 **отказ** (failure):Прерывание способности объекта выполнять требуемую функцию или невозможность выполнения им заданной функции в заранее установленных границах.

3.4.9 **систематический отказ** (systematic failure):Отказ, который определенным образом относится к конкретной причине, которая может быть устранена только путем изменения проекта, производственного процесса, операционных процедур, документации или других связанных с ними факторов.

3.4.10 **риск** (risk):Функция вероятности возникновения заданной угрозы и потенциально неблагоприятных последствий возникновения этой угрозы.

Примечания

1 Обычно термин «риск» используется только в случаях, когда есть, по крайней мере, возможность негативных последствий.

2 В некоторых случаях риск связан с вероятностью отклонения от ожидаемого результата или события.

3 По вопросам, связанным с безопасностью, следует обратиться к Руководству ИСО/МЭК 51.

[ИСО/МЭК 16085]

3.5 Термины, относящиеся к организациям

3.5.1 **организация** (organization):Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений.

Примечания

1 Объединения людей, организованные для некоторой определенной цели, такие как клуб, объединение, корпорация или сообщество, являются организацией.

2 Идентифицированная часть организации (даже совсем маленькая, вплоть до одного человека),так же как и идентифицированная группа организаций, может рассматриваться как организация в том случае, если они наделены ответственностью, полномочиями и отношениями.

[ИСО/МЭК 15288:2008]

3.5.2 **ответственный за систему** (approval authority):Человек (люди) и/или организация (организации), ответственные за утверждение действий, артефактов и других аспектов системы во время ее жизненного цикла.

Примечания

1 Объект «ответственный за систему» может включать в себя множество объектов, например людей или организации, которые могут отличаться друг от друга разными уровнями утверждения и/или различными предметными областями.

2 В ситуации участия двух сторон ответственность за систему зачастую лежит на приобретателе. В спорных ситуациях ответственным за систему может быть третье лицо, такое как государственная организация или ее агент.

В других ситуациях, например при покупке стандартных продуктов, разработанных одной стороной, независимость ответственного за систему может быть существенным вопросом для приобретателя.

3.5.3 **ответственный проектировщик** (design authority):Человек или организация, которые отвечают за проектирование продукта.

3.5.4 **ответственный за обеспечение целостности** (integrity assurance authority):Независимый человек или организация, ответственные за сертификацию соответствия требованиям уровня целостности.

Примечание — Адаптировано из ИСО/МЭК 15026:1998, в котором дано следующее определение. «Независимый человек или организация, ответственные за оценку соответствия требованиям целостности».

4 Структура стандарта

В разделе 5 настоящего стандарта рассмотрены фундаментальные понятия, такие, как гарантия, заинтересованные стороны, системы и продукты, неопределенности и последствия. В разделе 6 представлены некоторые аспекты, о которых должны заранее знать пользователи ИСО/МЭК 15026-2, ИСО/МЭК 15026-3 и ИСО/МЭК 15026-4. В разделах 7, 8 и 9 представлены термины, понятия и аспекты, особенно важные для пользователей ИСО/МЭК 15026-2, ИСО/МЭК 15026-3 и ИСО/МЭК 15026-4 соответственно. Однако пользователям каждой части может быть полезна информация других частей.

Библиография размещена в конце стандарта. Ссылки на пронумерованные элементы библиографии везде далее приведены в квадратных скобках.

5 Фундаментальные понятия

5.1 Введение

В настоящем разделе приведены понятия и термины, базовые для всех частей ИСО/МЭК 15026.

5.2 Гарантия

В ИСО/МЭК 15026 использовано специфическое определение гарантии как основания для обоснованной уверенности. Обычно заинтересованным сторонам необходимо основание для обоснованной уверенности до того момента, как они станут зависимы от системы, особенно в случаях сложных, новых систем или технологии с проблемной историей (например, программного обеспечения). Чем больше степень зависимости от системы, тем сильнее необходимость в веских основаниях для уверенности. Для получения рациональной основы обоснованной уверенности в соответствующих требованиях к свойствам системы необходимы соответствующие веские аргументы и доказательства. Свойства могут включать в себя такие аспекты, как будущие затраты, поведение и последствия. Соответствующие основания для обоснованных решений, относящихся к обеспечению разработки и производства, отвечающих требованиям систем, и к уверенности в этих системах, должны присутствовать на протяжении всего жизненного цикла.

Гарантия — это термин, который используется различными сообществами по-разному. Однако в любом случае использование термина имеет отношение к установке ограничений или уменьшению неопределенности в таких аспектах, как измерения, результаты измерений, оценки, прогнозы, информация, выводы или воздействие неопределенных факторов с конечной целью удовлетворить требования и/или продемонстрировать их выполнение. Снижение неопределенности может обеспечить лучшую основу для обоснованной уверенности. Даже в том случае, если оценка значения свойства остается неизменной, усилия, потраченные на уменьшение неопределенности ее значения, могут быть зачастую экономически оправданы, поскольку полученное уменьшение неопределенности улучшает основание для принятия решений.

Гарантия относится к вопросам:1) будет ли система или программное обеспечение в том виде, как это задано в спецификации, отвечать реальным нуждам и соответствовать ожиданиям; 2) будет ли соответствовать или соответствует ли система в том виде, как она построена и как эксплуатируется, спецификации; либо к обоим случаям, 1) и 2).

Спецификации могут быть заданы в виде представления статических и/или динамических аспектов системы. Зачастую в спецификации включают описания возможностей, функциональности, поведения, структуры, служб и ответственности, включая аспекты, связанные со временем и ресурсами, а также ограничения на частоту или серьезность отклонений продукта и связанные с ними неопределенности.

Спецификации могут представлять собой как предписания, так и/или ограничения (например, для поведения продукта), а также включать в себя критерии, оценки и предписания относительно компро-

миссов. Как правило, в спецификации помещают и некоторые ограничения на условия применимости, такие как внешняя среда и ее условия (например, температура) и, возможно, состояние продукта (например, возраст или степень износа).

5.3 Заинтересованные стороны

На протяжении всего жизненного цикла систем и программного обеспечения заинтересованные стороны либо влияют на процессы жизненного цикла систем, либо испытывают их влияние на себе. Заинтересованные стороны могут получать выгоду, терпеть убытки, накладывать ограничения или, иными словами, испытывать интерес к системе, следовательно, именно они предъявляют требования к системе. К заинтересованным сторонам можно отнести лиц, не являющихся непосредственными пользователями, чьи действия, результаты или другие требования могут быть затронуты, например лиц, программное обеспечение которых выполняется на тех же или подключенных к общей сети компьютерах.

Другой важный вид заинтересованной стороны — злоумышленник, который, несомненно, налагает ограничения или испытывает интерес к системе. В настоящем стандарте злоумышленник включен в число заинтересованных сторон; однако в сообществах по безопасности и некоторых других сообществах термин «заинтересованные стороны» не включает в себя злоумышленника.

Влиятельными заинтересованными сторонами, требования которых необходимо учитывать, являются не только владельцы и пользователи системы, но также разработчики и операторы, которые должны определять требования к разработке и эксплуатации системы. В зависимости от условий и последствий для разных заинтересованных сторон необходимо основание для обоснованной уверенности в свойствах системы, требования для которой они определили.

5.4 Система и продукт

В целях соответствия ИСО/МЭК 15288 и ИСО/МЭК 12207 в ИСО/МЭК 15026 широко используется термин «система». Потребители настоящего стандарта и других частей ИСО/МЭК 15026, хорошо знакомые с использованием термина «продукт», должны отметить, что термин «система» включает в себя как продукты и услуги, которые являются результатами процессов, так и программное обеспечение, системы, элементы или компоненты программного обеспечения. Несмотря на то что настоящий стандарт и другие части ИСО/МЭК 15026 в первую очередь ориентированы на системы, произведенные в результате процессов, хотя бы частично управляемых человеком или искусственно, его также допускается использовать для уменьшения неопределенности зависимости системы от природных явлений.

5.5 Свойство

Настоящий стандарт связывает гарантию с требованиями к свойствам системного или программного продукта. Свойство может включать в себя условие, характеристику, атрибут, качество, особенность, измерение или последствие. Свойства могут быть неизменными или зависимыми от времени, ситуации или предыстории. Для целей настоящего стандарта предполагается, что свойство прямо или косвенно относится к системе или системам и поэтому связано с соответствующими требованиями.

Требования к свойствам могут быть требованиями к свойствам в прошлом, настоящем или будущем.

Как правило, последнее является наиболее важным с учетом требований ИСО/МЭК 15026. Поскольку подобная информация связана с предсказанием будущего, то зачастую получить ее трудно, а, кроме того, достоверность ее сомнительна. В связи с этим поведение системы в будущем и последствия (см. 5.8) зачастую являются принципиальными вопросами гарантии системы.

Многие из свойств, к которым предъявляются требования, являются показателями качества системы. Списки и определения показателей качества, которые могут быть предметом гарантии, представлены в ряде стандартов и отчетов: ИСО/МЭК 9126-1, ИСО/МЭК 25010 и связанные с ними серии, ИСО/МЭК 2382-14, ИСО 9241, ИСО/ТО 18529 и ИСО/ТС 25238.

Применение термина «свойство» в настоящем стандарте вытекает из повсеместного использования этого термина в ИСО/МЭК 25010 и согласовано с ним. В ИСО/МЭК 25010 этот термин охватывает свойства, которые являются присущими или нет, внутренними или внешними, явными или подразумеваемыми.

Производители и другие заинтересованные стороны могут наделять приоритетом такие свойства, как эффективность и надежность, и искать компромисс между этими свойствами и связанными с ними требованиями. Для решения таких задач было разработано множество методов, описанных в [25], [64], [122], [157] и [40]. Определение требования верхнего уровня к свойству в некоторых случаях является результатом анализа, включая и анализ компромиссных решений.

5.5.1 Свойства как поведение

Часто свойство определяют как поведение. Во время выполнения операций связанные с поведением свойства могут быть формально определены как комбинация следующих факторов:

- ограничение на разрешенные состояния системы (иногда называемое «свойством безопасности»);
- состояния системы, которые должны быть достигнуты и требуют прогресса или завершения («свойство живучести»);
- ограничения на потоки или взаимодействия, требования на ограничения разделения.

Такие свойства могут быть заданы как условия или ограничения, которые для системы должны выполняться[1]. На практике они нетривиальны и имеют модульную структуру, связаны со временем и начальным состоянием (состояниями), а также с изменениями состояния, связанными с взаимодействием системы или программного обеспечения со средой.

Предметами возможного интереса являются многие виды потоков, такие как потоки газов, жидкостей, трафика или информации, так же как и поддерживаемые ограничения на них, например невмешательство и разделение. Кроме того, ограничения потоков зачастую удобны или необходимы для определения аспектов информационной безопасности [135], таких как механизмы управления доступом, политики и ограничения на информацию, передаваемую по открытым или закрытым каналам.

5.6 Неопределенность и уверенность

В ИСО/МЭК 15026 термин «неопределенность» используется как объединяющий термин, который включает в себя отсутствие уверенности в том, что можно вероятностно смоделировать неопределенность. Неопределенность может включать в себя нечеткие понятия, которые могут быть смоделированы без использования вероятности. Некоторые сообщества ограничивают использование этого термина прогнозами будущих событий, реализованными или физическими измерениями с неизвестными результатами. Ввиду того что такое ограниченное использование термина может быть удобным для целей этих сообществ, использование ИСО/МЭК 15026 охватывает многие сообщества.

Степень уверенности, которая могла бы возникнуть или уже возникла на основе конкретного гарантийного случая, может быть различной для разных людей, организаций и ситуаций. Чем меньше неопределенность в претензии для гарантийного случая, тем выше степень обоснованной уверенности. Однако для конкретных приложений преобразование степени неопределенности в степень обоснованной уверенности в пригодности либо не является прямым, либо неизвестно. По этой и ряду других причин в гарантийный случай иногда включаются последствия. Несмотря на то что это логично, остается необходимость принятия решения относительно степени обоснованной уверенности лицом, принимающим решения.

5.7 Условия и инициирующие события

Гарантийный случай должен учитывать все условия, которые могут оказать существенное негативное влияние на результат и неопределенность требования верхнего уровня. Изначально может оказаться сложным идентифицировать потенциально значимое множество условий и событий [2], и, кроме того, без их учета может оказаться затруднительным в самом начале гарантийного случая выявить те из них, влияние которых может быть значительным.

Исторически сложилось так, что одним из условий, считающимся самым важным, является системный отказ. Системному отказу посвящено множество инструкций, практик и публикаций (например, [2], [71] и [14, глава 18, с. 475—524]).Несмотря на то что преимущественно эти разработки были сделаны в сообществах, занимающихся безопасностью, защитой или человеческими ошибками, системный отказ может привести к снижению достижения положительного свойства или последствиям, а также может стать причиной отрицательных свойств или убытков.

Опасность поведения системы может быть различной для различных условий ее среды. Для того чтобы определить, закончатся ли негативные последствия, зачастую необходимо во время анализа рассматривать комбинацию поведения и условий. Фактические условия среды, в которой находится система, могут быть известны или неизвестны в зависимости от датчиков, значения входных величин и их обработки.

Разработчики системы могут знать, а могут и не знать обо всех инициирующих условия событиях в среде. Однако, возможно, потребуется принять во внимание опасные условия, несмотря на то, что не все инициирующие их события известны или распознаваемы.

---

[1] Если определено формально, то возможен статический анализ соответствия проекта и кода, что потенциально увеличивает надежное обоснование гарантии.

5.8 Последствия

Вне системы обоснование в основном базируется на условиях, которые могут привести к негативным последствиям, на инициирующих их событиях или предварительных условиях. Внутри системы обоснование опирается на условия, которые могут привести к опасному поведению системы, на инициирующие события или предварительные условия.

На практике требования могут выходить за рамки системы или ее поведения. В частности, требования могут накладывать ограничения на последствия поведения системы и/или связанные с системой события, действия и/или условия, особенно на значимость последствий.

Последствие может быть желательным или нежелательным с учетом позиции, точки зрения или интересов заинтересованной стороны. Последствие может иметь место в любой момент жизненного цикла системы.

В сложных социально-технических системах интерпретацию неудач или нарушений требований нельзя ограничивать лишь отказами компонентов. Негативные последствия могут быть следствием нормальной изменчивости поведения, а также непреднамеренных или непредвиденных взаимодействий [57], [54].Независимо от того, как они возникают, опасные условия и негативные последствия являются предметом изучения для смягчения отрицательных последствий.

Злоумышленники могут обладать возможностями, ресурсами, мотивацией и намерениями, которые позволяют им инициировать и приложить вредоносные усилия для нарушения требований. Нарушители используют свои преимущества, чтобы воспользоваться в своих интересах предоставленными системой и/или средой возможностями, называемыми «уязвимостями», то есть «слабыми местами, которые могут быть использованы или инициированы источником угрозы»[150][1)].

В некоторых случаях не уделяется должного внимания тому, что злонамеренные и подрывные действия становятся проблемой, даже если они не затрагивают никаких связанных с защищенностью свойств системы. Злонамеренные разработчики могут повлиять практически на любое свойство.

В нескольких стандартах и отчетах рассматриваются последствия, относящиеся к системам в определенных предметных областях. Такими стандартами являются ИСО 14620 [79], ИСО 19706 [81] и ИСО/ТС 25238 [121]. Кроме того, в стандартах менеджмента рисков также рассматриваются последствия, например в ИСО/МЭК 16085 [91] и ИСО 31000.

6 Применение нескольких частей ИСО/МЭК 15026

6.1 Введение

ИСО/МЭК 15026 или его части могут использоваться сами по себе либо совместно с другими стандартами или руководствами. Части ИСО/МЭК 15026 могут быть распространены на большинство стандартов жизненного цикла, и в них можно использовать любой из наборов строго определенных качеств или свойств.

6.2 Начальное руководство по использованию

При использовании ИСО/МЭК 15026 выбор свойств и/или требований полностью лежит на пользователе стандарта в соответствии с потребностями и требованиями заинтересованных сторон системы. Для гарантийного случая может быть выбрано любое свойство или любое требование независимо от его важности или связанного с ним риска. Однако ИСО/МЭК 15026 ориентирован прежде всего на свойства, которые считаются критически важными с точки зрения одной или нескольких основных заинтересованных сторон. В ИСО/МЭК 15026-4 термин «критические свойства» используется именно для таких приоритетов и требований заинтересованной стороны.

В то время как ИСО/МЭК 15026-3 в общем случае совместим «сверху вниз» с ИСО/МЭК 15026:1998, переход к ИСО/МЭК 15026-3 имеет некоторые особенности. ИСО/МЭК 15026-3 открывает новые возможности инженерии и принятия решений, так как он дает не только автономную концепцию, но также и ту, в которую включены соответствующие гарантийному случаю уровни целостности. ИСО/МЭК 15026-3 концентрируется больше на самой системе и ее уровнях целостности, а не на внешнем анализе рисков. Кроме того, в нем также рассмотрено создание уровней целостности. Уровни целостности рассмотрены в разделе 8 настоящего стандарта.

[1)] В большинстве случаев смысловая значимость и необходимость отделения уязвимости от других слабых мест могут быть низки либо вообще отсутствовать. Кроме того, вопрос всегда рассматривается в контексте настоящего и будущего, что очень важно для утверждения «... могут быть использованы или инициированы».

6.3 Взаимосвязь частей ИСО/МЭК 15026

ИСО/МЭК 15026 состоит из следующих частей:

- ИСО/МЭК 15026-1 «Понятия и словарь», в которой объясняются понятия и термины, базисные для всех частей этого стандарта;
- ИСО/МЭК 15026-2 «Гарантийный случай», в которой рассмотрены требования к содержанию и структуре гарантийного случая;
- ИСО/МЭК 15026-3 «Уровни целостности системы», которая связывает уровни целостности с гарантийным случаем и включает в себя требования использования уровней целостности с гарантийным случаем и без него (пересмотр ИСО/МЭК 15026:1998);

ИСО/МЭК 15026-4 «Гарантии жизненного цикла», в которой приводятся указания и рекомендации по конкретным, связанным с гарантией действиям для всех процессов жизненного цикла систем и программного обеспечения.

ИСО/МЭК 15026-2, ИСО/МЭК 15026-3 и ИСО/МЭК 15026-4 образуют связанный набор и в то же время обеспечивают разделение тем гарантии, поэтому они могут использоваться как раздельно, так и вместе. Настоящий стандарт обеспечивает общие сведения, понятия и терминологию, которые применимы к любой из трех частей, и, кроме того, далее представлены специальные введения для ИСО/МЭК 15026-2, ИСО/МЭК 15026-3 и ИСО/МЭК 15026-4.

Гарантийный случай в большей или меньшей степени рассматривается во всех частях, однако в ИСО/МЭК 15026-4 обсуждаются достижение выполнения требований, свидетельство выполнения требований и то, содержит ли артефакт, называемый «гарантийным случаем», такое свидетельство.

ИСО/МЭК 15026-2 концентрируется на содержании и структуре гарантийного случая. ИСО/МЭК 15026-3 связывает уровни целостности и гарантийные случаи. В ней описано, как уровни целостности и гарантийные случаи могут взаимодействовать, особенно при определении спецификаций для уровней целостности или при использовании уровней целостности в пределах области гарантийного случая. Эта взаимосвязь определяется уровнем риска и зависимостями в системе.

В тех случаях, когда риски или обработка рисков не достаточно хорошо изучены, неизвестна структура зависимостей системы в целом или непонятен выбор подходящих требований, то целесообразнее использовать гарантийный случай, а не уровни целостности. Это особенно актуально для новых видов рисков или при использовании новых методов обработки риска. В подобных случаях важным для гарантийного случая является обоснование выбора требований верхнего уровня.

В случаях известных рисков и их обработки разработчики должны не обосновывать выбор требований верхнего уровня, а всего лишь выбирать надлежащие требования для их условий из известного набора, то есть надлежащий уровень целостности из совокупности уровней целостности. В таких ситуациях общие аргументы, задаваемые при определении уровня целостности, обеспечивают обоснование того, что соответствие требованиям уровня целостности адекватно соответствию уровню целостности. Такое обоснование (например, обобщенный гарантийный случай) обычно создается в отдельной организации один раз, а затем многократно используется в разных проектах.

ИСО/МЭК 15026-4 содержит методические материалы, относящиеся к гарантии, и рекомендации по мероприятиям для всех процессов жизненного цикла, включая действия, которые выходят за пределы деятельности, непосредственно связанной с гарантийным случаем, например при планировании проекта для относящихся к гарантии разработок.

6.4 Ответственные

Во всех частях ИСО/МЭК 15026 используется термин «ответственный», определенный в разделе 3 «Термины и определения» настоящего стандарта. Например, в ИСО/МЭК 15026-3 входит заключение соглашения между ответственным проектировщиком и ответственным за обеспечение целостности. Кроме того, для новой системы нужен ответственный за приобретение, который возьмет на себя ответственность за анализ процесса создания гарантийных случаев совместно с ответственным проектировщиком и ответственным за обеспечение целостности со стороны поставщика.

Однако для гарантийного случая совсем не обязательно «ответственный за систему» должен оценивать соответствие частям ИСО/МЭК 15026. По мере возможности требования соответствия частям ИСО/МЭК 15026 оцениваются по более простым и трудно оспариваемым аспектам, нежели качество артефактов и решений, оцененных в контексте системы или проекта. На практике в контракте может быть указано, что приобретатель является лицом, ответственным за систему, или лицом, подтверждающим соответствие частям ИСО/МЭК 15026.

7 ИСО/МЭК 15026 и гарантийный случай

7.1 Введение

ИСО/МЭК 15026-2 раскрывает структуру и содержание гарантийного случая. Здесь описаны пять основных компонентов гарантийного случая: требования, параметры, доказательство, обоснования и предположения. Цель гарантийного случая состоит в улучшении обратной связи с заинтересованной стороной, обеспечив ее информацией, необходимой для принятия решений, и предоставив обоснование для необходимой уверенности заинтересованной стороны. В общем случае гарантийный случай должен предоставить гарантию свойств системы сторонам, не вовлеченным тесно в процессы технического развития системы. Такими сторонами могут быть стороны, привлеченные для сертификации системы, ее настройки, приобретения или аудита. Как правило, гарантийный случай рассматривает причины ожидания и подтверждения успешного изготовления системы, а также возможности и риски, идентифицированные как трудности или препятствия при разработке и поддержке этой системы.

В отличие от логических проверок дедукции претензий из доказательства, которое покрывается аспектами абсолютной истины, или истины с точки зрения Платона, гарантийный случай имеет дело с диалектическими аспектами системы, где истина всегда относительна или даже субъективна. Другими словами, даже если логические доказательства представлены в соответствии с конкретной логической теорией, то в гарантийных случаях они могут быть опровергнуты на основании того, что была выбрана несоответствующая базовая логическая теория. Потребность в гарантийных случаях возникает и тогда, когда становится понятно, что свойства систем в реальном мире никогда не могут быть полностью формализованы в соответствии с логической теорией, а всегда есть что-то, что не поддается никакой логической формализации.

Примечание — В случае если требования верхнего уровня относятся к безопасности, защищенности, надежности или RAM (надежность, готовность и сопровождаемость), то гарантийные случаи, связанные с этими требованиями, называют случаями безопасности, случаями защищенности, случаями надежности или случаями RAM соответственно. См. элемент «Библиография»: [139], [142], [143], [146], [154], [155], [168], [74], [22], [23], [24].

Гарантийный случай, рассматриваемый как артефакт, наделен такими относящимися к качеству аспектами, как природа содержания, его форма или структура (например, метод аргументации или модульности), семантическими аспектами, такими как полнота, создание и обслуживание, включая поддержку инструментальных средств, удобство использования и презентабельность, целостность, законность, понятность и наличие четких заключений с явными степенями неопределенности. В одной из статей [164] приведен достаточно полный перечень относящихся к качеству характеристик для гарантийных случаев. Относящиеся к качеству аспекты гарантийного случая не покрываются ни ИСО/МЭК 15026-2, ни другими частями ИСО/МЭК 15026.

Любые независимые изменения в системе, среде или требованиях верхнего уровня гарантийного случая требуют внесения изменений в гарантийный случай. Таким образом, гарантийный случай обычно содержит прогрессивно расширяющуюся доказательную базу, созданную во время разработки и на более поздних этапах жизненного цикла, которая должна отражать все соответствующие изменения [139, с. 5].

Примечание — Претензии гарантийного случая к значениям свойств могут включать в себя весь набор требований системы в целом для свойства, представляющего интерес. Например, в одном случае требования верхнего уровня могут состоять из следующего:

1) требуемые ограничения на последствия;
2) функциональность и свойства самой системы (например, требования обязательности функциональности).

Показатели качества, определенные в ряде стандартов серии ИСО/МЭК 25000, включают в себя также показатели качества, связанные с функциональностью и ограничениями. С обеих точек зрения интерес представляет работа «Общие Критерии v.3.1 Пересмотр 2» [30].

7.2 Обоснование метода доказательства

Аргументация имеет соответствующее обоснование для правильности или ценности ее метода обоснования. Метод аргументации может быть дополнительным источником неопределенности.

Для аргументации и анализа в гарантийном случае может быть использовано множество подходов, которые отличаются друг от друга их применимостью, правомочностью, получаемыми точностью, неопределенностью и простотой использования. Объекты и подходы к доказательству различны для разных сообществ, отличающихся мотивацией, мышлением и зачастую множеством методов доказательств.

В методы доказательств входят:

количественные:

- детерминированные (например, формальные доказательства);
- недетерминированные формальные системы доказательства:

a) вероятностные,

b) теоретико-игровые (например, минимакс),

c) другие основанные на неопределенности формальные системы доказательств (например, нечеткие множества);

- качественные (например, оценки результатов деятельности персонала, решений суда и качественные оценки причинной связи событий).

Текущее состояние науки не позволяет получать четкие и точные количественные прогнозы для сложных продуктов и ситуаций, а также для ситуаций с участием людей. В условиях отсутствия доступных, подходящих, более объективных методов и технологий или при необходимости добавить или оценить результаты таких методов используются субъективные оценки. Широко используется и общепринято дополнение количественных методов экспертной оценкой и обоснованием. Как и в случаях с другими формами аргументации, субъективные оценки принимают форму требований и их обеспечения. Несмотря на то что в некоторых случаях использование субъективного доказательства необходимо или предпочтительно, оно может привести к дополнительной неопределенности, следовательно, обычно (так же, как и с допущениями) менее критичное доказательство является лучшим.

Случаи «естественных» событий и обычного незлонамеренного человеческого поведения обычно описываются вероятностно. Тем не менее имеются возможности интеллектуальных, вредоносных действий, вероятность которых не определена или не понятна и которые могут стать проблемой в случае, если квалифицированный и мотивированный противник намеренно нарушает законы вероятности, чтобы сделать свое поведение непредсказуемым для достижения, например внезапности. Эта особенность является основным различием в обоснованиях безопасности и защищенности.

7.3 Средства получения доказательств и управления ими

Для любого свойства существуют много способов получения доказательства. К ним относятся: опыт, история, результаты измерений и непосредственно измерения, тесты, оценка соответствия и ее результаты, исследования, дефекты и выводы. Доказательство должно достигнуть целей, заявленных в аргументации гарантии (см. [139,часть 3, 9.1]).

Доказательная база может стать довольно большой, быть организованной и управляться некоторой структурой, обеспечивающей неизменность и отслеживаемость доказательства, для того чтобы обеспечить пользователю уверенность в ее источнике, содержании и правильности. В источнике [150] указано следующее:

- доказательство должно быть однозначно определено таким образом, чтобы аргументация могла бы однозначно сослаться на доказательство;
- доказательство должно обеспечивать возможность проверки и аудита;
- доказательство должно быть защищено и контролироваться при управлении конфигурацией;
- доказательство должно сопровождаться метаданными, необходимыми для должного использования их в гарантийном случае.

Последний пункт — это просто повторение того, что предполагается получить в результате тестирования, связанного с гарантийным случаем.

7.4 Сертификации и аккредитации

Каждый аспект, потенциально имеющий значительные последствия для удовлетворения требований верхнего уровня или для достижения уверенности ключевых заинтересованных сторон, потенциально присутствует в полном доказательстве гарантийного случая. Этим должно обеспечиваться не только ожидаемое доверие заинтересованных сторон, но и достаточность информации для использования сертифицирующими и аккредитующими органами.

Авиационная и атомная промышленность имеют длинную историю стандартов и сертификаций, а сообщество безопасности в подкомитете ИСО/МЭКСТК 1/Подкомитет 27 работало над темой гарантии на протяжении многих лет. Базой для сертификации операционных систем системы менеджмента информационной безопасности (ISMS) являются: Общие Критерии, FIPS 140 для криптологии, ИСО/МЭК 27002 «Информационные технологии. Свод правил для менеджмента информационной безопасности» в сочетании с ИСО/МЭК 27001 (ранее британский стандарт BS 7799-2:2002). Министерство обороны Великобритании и Управление гражданской авиации также разработали эффективные стандарты, включая рассматривающие гарантийные случаи стандарты для надежности, сопровождаемости и безопасности, например [139], [142], [143], [22] и [23]. В библиографии указаны и другие стандарты.

Сообщество безопасности (например, гражданская авиация) использовало сертификацию ведущих специалистов (назначаемый агент или выдача разрешений) как часть своего подхода. На практике существует большое количество разных сертификаций безопасности и компьютерной безопасности, от ориентированных на управление до технических для определенных продуктов, например сертификация международного консорциума, сертификации систем безопасности информационных систем (ISC) и сертификация института SANS.

8 ИСО/МЭК 15026 и уровни целостности

8.1 Введение

Уровни целостности применимы для использования при определенных уровнях риска или при поддержке гарантийных случаев, а также для задания критериев, характерных для проекта, собранных доказательств и систем. Уровень целостности можно рассматривать как представление степени уверенности, которую используют для достижения соглашения о рисках, связанных с системой, заинтересованными в этой системе сторонами.

ИСО/МЭК 15026-3 прежде всего устанавливает структуру уровня целостности. Далее в стандарте определяются уровни целостности, их применение, определение уровней целостности системы или продукта, использование анализа рисков, присвоение уровня целостности элементу системы, удовлетворение требованиям уровня целостности, применение доказательств, соглашений и одобрений, включая полномочия (см. 6.4).

Требования уровня целостности отражают то, что должно быть достигнуто, при том, что доказано, что система или элемент системы имеют (имели или будут иметь) свойства, отвечающие его уровню целостности. Уровень целостности системы подтверждает соответствие с точки зрения свойств всей системы. Таким образом, доказательство свойств играет ведущую роль в доказательстве выполнения более высоких требований, предъявляемых к системе, включая среду, желательные или нежелательные последствия. Если такие, более высокие требования не предъявлены, то достижение и доказательство уровней целостности элемента системы представляют собой основную часть доказательства выполнения требований верхнего уровня относительно самой системы.

На практике уровни целостности часто обсуждаются в терминах, подчеркивающих доказательства, необходимые для удовлетворения требований к уровню целостности и, тем самым, обеспечивающие доказательства для аргументов, поддерживающих требования к свойствам самой системы. Тем не менее из-за влияния качества на неопределенности важно также и качество аргументов, удовлетворяющих требованиям к уровню целостности, как доказательство достижения соответствующего уровня целостности. Неопределенности, относящиеся к аргументации, доказательствам и допущениям, являются частью установления требований к уровню целостности.

Примечание — Уровни целостности и связанные с ними стандарты, особенно в области безопасности, имеют богатую историю. Уровни целостности в стандартах, связанных с безопасностью, определены в виде многоуровневых наборов, относящихся к различным степеням строгости и/или неопределенности в их достижении более высоких уровней, обеспечивающих более высокую строгость и более низкую неопределенность. В качестве примера можно рассмотреть стандарт безопасности МЭК 61508 «Функциональная безопасность электрических/электронных/программируемых электронных связанных с безопасностью систем» [70]. В других источниках подобные схемы используются в рамках другой терминологии, например «классы соответствия».

8.2 Анализ рисков

Анализ рисков устанавливает требуемый уровень целостности для всей системы. Анализ рисков — это непрерывный и итеративный процесс, который должен сбалансировать то, что еще непонятно, с тем, что должно быть известным. Уровень целостности, полученный в результате анализа рисков, является трансляцией значений последствий в события и синхронизацию условий или поведения системы. Такая трансляция имеет место для внутренних по отношению к системе уровней целостности и их зависимостей, поскольку они также являются предметом событий и синхронизации. Таким образом, уровень целостности представляет собой кодирование того, что необходимо сделать и доказать для различных диапазонов и уровней серьезности ограничений на значения свойств и связанную с ними неопределенность.

ИСО/МЭК 15026 не рассматривает подробно анализ рисков. Многие стандарты и руководящие документы предлагают руководства для анализа рисков и могут помочь в идентификации потенциальных негативных последствий.

Например, МЭК 61508 [70] и МЭК 31010, редакция 1.0 (2009-11-27) «Менеджмент рисков. Методы менеджмента рисков», описывают подходы к анализу рисков. В МЭК 300-3-9 используется специфичная

для безопасности терминология, поэтому термины «опасность» (hazard)и «вред» (harm) должны быть интерпретированы как «опасное условие» (dangerous condition) и «негативное последствие» (adverse consequence) соответственно. Общее представление дается и в МЭК 60300 «Менеджмент надежности» [64].

Другие специализированные стандарты и документы применимы в различных областях: ИСО 13849 [78] — для машинного оборудования, ИСО 14620 [79] — в космических системах, ИСО 19706 [81] — в пожарном деле, ИСО/ТС 25238 [121] — в медицинской информатике, ИСО/МЭК 27005 [110] — в области информационной безопасности, UK CAP 760760 [24] — на воздушном транспорте и в аэропортах. Возможный интерес могут представить более общие стандарты менеджмента рисков ИСО/МЭК 16085[91] и ИСО 31000.

9 ИСО/МЭК 15026 и жизненный цикл

9.1 Введение

ИСО/МЭК 15026-4 «Гарантии жизненного цикла» представляет процессы для гарантирования систем и программного обеспечения в виде информации о целях и результатах, подходящих для целей гарантирования систем и программного обеспечения. Понятие представления процесса сформулировано и описано в приложении к стандарту ИСО/МЭК 15288 «Системная и программная инженерия. Процессы жизненного цикла систем». Описание представления процесса содержит информацию о целях и результатах процесса. В отличие от самого процесса описание представления процесса не включает в себя действия и задачи. Вместо этого описание содержит руководство и рекомендации, объясняющие, каким образом могут быть достигнуты результаты с использованием действий и задач различных процессов, описанных в ИСО/МЭК 15288 и ИСО/МЭК 12207 «Системная и программная инженерия. Процессы жизненного цикла программного обеспечения».

В ИСО/МЭК 15288 и ИСО/МЭК 12207описаны все процессы жизненного цикла, несмотря на то, что в ИСО/МЭК 12207 процессы специализированы к программному обеспечению и, в некоторых случаях, имеют отличные наименования, отражающие такую специализацию. В ИСО/МЭК 12207 входят процессы, не включенные в ИСО/МЭК 15288, связанный с процессами реализации программного обеспечения: процессы поддержки и процессы повторного использования.

Все процессы, действия, задачи, методические материалы и рекомендации должны быть представлены в контексте модели жизненного цикла. Состоящий из нескольких частей технический отчет ИСО/МЭК ТО 24748 «Системная и программная инженерия. Менеджмент жизненного цикла» предназначен для того, чтобы упростить для описания процесса совместное использование содержания двух стандартов процесса жизненного цикла. ИСО/МЭК ТО 24748 обеспечивает объединенное и консолидированное руководство по менеджменту жизненного цикла систем и программного обеспечения. Его цель состоит в том, чтобы обеспечить непротиворечивость в концепциях системы и понятиях жизненного цикла, моделях, этапах, процессах, приложениях процесса, итерации и рекурсии процессов во время жизненного цикла, ключевых понятиях представления, адаптации и использовании в различных областях. ИСО/МЭК 24748-1 показывает применение модели жизненного цикла для систем в контексте ИСО/МЭК 15288 и приводит соответствующий пример использования модели жизненного цикла для программного обеспечения в контексте ИСО/МЭК 12207.

ИСО/МЭК 15026-4 дает пользователю свободу выбора: использовать ли специфический артефакт, называемый «гарантийный случай», или оформить относящуюся к гарантии информацию в виде иного документа. Суть заключается в удовлетворении требований верхнего уровня и последующем доказательстве удовлетворения требования к значению критического для соответствующей заинтересованной стороны свойства. Необходимо, чтобы процессы жизненного цикла, действия и задачи отражали как реализацию надлежащей системы, так и уверенность в том, что система соответствует доказательству достижения уровня уверенности, требуемого заинтересованными сторонами.

Пользователям ИСО/МЭК 15026-4 могут потребоваться оценка степени риска и менеджмент рисков, измерения и требования к процессам, разработанные более досконально, чем это предоставлено в ИСО/МЭК 15288 и ИСО/МЭК 12207. Для обеспечения большего числа деталей этих трех процессов совместно со стандартами ИСО/МЭК 15288 и ИСО/МЭК 12207 можно использовать три международных стандарта: ИСО/МЭК 16085 «Менеджмент рисков», ИСО/МЭК 15939 «Измерение» и ИСО/МЭК/ИИЭР 29148 «Инженерия требований». Другими стандартами, в которых представлены полезные требования и методические материалы по специфическим процессам, является ИСО/МЭК/ИИЭР 15289 для документирования результатов выполнения процессов жизненного цикла и ИСО/МЭК/ИИЭР 16326 для процесса управления проектами.

ИСО/МЭК 15026 совместим с этими стандартами процессов жизненного цикла. Цели гарантии, выбор гарантируемых требований, относящееся к гарантии планирование, разработка и обслуживание гарантийных случаев взаимозависимы во всех процессах жизненного цикла.

9.2 Мероприятия гарантии в жизненном цикле

Чтобы обеспечить основание для уверенности в свойствах системы, необходимо выполнить запланированную и систематическую совокупность гарантийных мероприятий. Такая совокупность действий разработана для обеспечения соответствия процессов и систем требованиям к ним, стандартам, методическим материалам и определенным процедурам [145].«Процессы» в данном контексте включают в себя все действия, связанные с проектированием, разработкой и техническим обслуживанием системы. Для программного обеспечения понятие «программный продукт» включает в себя само программное обеспечение, связанные с ним данные, его документацию, поддерживающие и отчетные документы, произведенные как часть программного процесса (например, результаты испытаний и аргументы гарантии), а также все то, что необходимо для завершения гарантийного случая. «Требования» включают в себя требования к свойствам, которые должны быть доказаны, в конечном счете на основе требований, направленных на ограничение, уменьшение или управление связанными со свойством затратами и убытками. «Стандарты, методические материалы» могут быть как техническими, определяющими технологию для использования в системе или программном обеспечении, так и нетехническими, определяющими аспекты процесса, которые далее очерчены «процедурами», обеспечивающими возможность удовлетворения требований к системе.

Управление действиями жизненного цикла включает в себя обработку как действий, непосредственно связанных с относящейся к гарантии качества информацией, так и того влияния, которое относящаяся к гарантии качества информация оказывает на другие действия. Успешное управление лучше всего осуществляется в случае, если требования верхнего уровня рассматриваются с самого начала разработки концепции, когда они влияют на все последующие действия и системы и становятся неотъемлемой частью полного процесса разработки (см.[140] и [22, приложение В]). Все это возможно лишь тогда, когда одновременно разрабатывается система и информационный блок, показывающий удовлетворение требований.

Параллельная природа обоснования и аргументации разработки является всего лишь одним из преимуществ одновременной разработки системы и ее гарантийного случая. Процесс разработки и система могут быть нацелены не только на удовлетворение требований, но и на то, чтобы посредством гарантийного случая можно было доказать соответствие. Гарантийный случай влияет на систему, побуждая выбирать такое направление разработки, которое обеспечивает практичное построение аргументации. Зачастую это приводит к более простой системе (по крайней мере, внутренне), элементы которой могут использоваться изолированно, для того чтобы показать определенные подтребования, и к такому расположению элементов системы, при котором обоснование композиции отвечает современным техническим требованиям и требованиям практики. Параллельные процессы могут включать в себя требования, покрывающие больше условий и событий, а также соответствующий уровень восстанавливаемости, методы, используемые для уменьшения числа дефектов, валидацию или верификацию, направленные на конкретное требование и доказательство его соответствия.

10 Заключение

Цель настоящего стандарта — обеспечить пользователей всех частей ИСО/МЭК 15026 объяснением соответствующих понятий и терминов, используемых в ИСО/МЭК 15026, которые ранее не были общепринятыми в разных сообществах. Объяснения того, что изложено в каждой из частей ИСО/МЭК 15026, должно обеспечить возможность для выбора и использования этих частей, а также обоснование выбора других стандартов, не принадлежащих к серии ИСО/МЭК 15026.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 15026-4:2012	IDT	ГОСТ Р ИСО/МЭК 15026-4—2016 «Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 4. Гарантии жизненного цикла»

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

- IDT — идентичный стандарт.

Библиография

[1] Abran A., & Moore J.W. (Executive editors), Pierre Bourque, Robert Dupuis, Leonard Tripp (Editors). Guide to the Software Engineering Body of Knowledge. 2004 Edition. Los Alamitos, California: IEEE Computer Society, Feb. 16, 2004. Available at http://www.swebok.org

[2] Adamski A., & Westrum R. Requisite imagination: The fine art of anticipating what might go wrong. In: [55], pp. 193—220, 2003

[3] Adelard. The Adelard Safety Case Development Manual. Available at http://www.adelard.com/web/hnav/resources/ascad

[4] Alexander I *Systems Engineering Isn't Just Software*. 2001. Available at http://easyweb.easynet.co.uk/~iany/consultancy/systems_engineering/se_isnt_just_sw.htm.

[5] Allen J.H., Barum S., Ellison R.J., Mcgraw G., Mead N.R. *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley, 2008

[6] Altman W., Ankrum T., Brach W. *Improving Quality and the Assurance of Quality in the Design and Construction of Nuclear Power Plants: A Report to Congress*. U.S. Nuclear Regulatory Commission. Office of Inspection and Enforcement, 1987

[7] Anderson J.P. *Computer Security Technology Planning Study Volume I*, ESDTR-73-51, Vol. I, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01730, Oct. 1972.

[8] Anderson R.J. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley and Sons, Second Edition, 2008

[9] Ankrum T.S., & Kromholz A.H. Structured Assurance Cases: "Three Common Standards," Ninth IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), pp. 99—108, 2005

[10] Armstrong J.M., & Paynter S.P. *The Deconstruction of Safety Arguments through Adversarial Counter-argument*. School of Computing Science, Newcastle University CS-TR-832, 2004

[11] Atchison B., Lindsay P., Tombs D. *A Case Study in Software Safety Assurance Using Formal Methods*. Technical Report No. 99—31. Sept. 1999

[12] ATSIN Number 17 Issued 9. Lapses and Mistakes. Air Traffic Services Information Notice, Safety Regulation Group, ATS Standards Department. UK Civil Aviation Authority, August 2002

[13] Bahill A.T., & Gissing B. Re-evaluating Systems Engineering Concepts Using Systems Thinking. *IEEE Trans. Syst. Man Cybern. C*. 1998 November, 28 (4) pp. 516—527

[14] Berg C.J. *High-Assurance Design: Architecting Secure and Reliable Enterprise Applications*. Addison Wesley, 2006

[15] Bernstein Lawrence, & Yuhas C. M. Trustworthy Systems through Quantitative Software Engineering. Wiley-IEEE Computer Society Press, 2005. About reliability not security

[16] Bishop M., & Engle S. *The Software Assurance CBK and University Curricula*. Proceedings of the 10th Colloquium for Information Systems Security Education, 2006

[17] Bishop M. *Computer Security: Art and Practice*. Addison-Wesley, 2003

[18] Bishop P., & Bloomfield R. *A Methodology for Safety Case Development*. Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium, Birmingham. 1998

[19] Bishop P., & Bloomfield R. *The SHIP Safety Case Approach*. SafeComp95, Belgirate, Italy. Oct 1995

[20] Buehner M.J., & Cheng P.W. Causal Learning. In: *The Cambridge Handbook of Thinking and Reasoning*, (Morrison R., & Holyoak K.J. eds.). Cambridge University Press, 2005, pp. 143—68.

[21] Cannon J.C. *Privacy*. Addison Wesley, 2005

[22] CAP 670 Air Traffic Services Safety Requirements. UK Civil Aviation Authority Safety Regulation Group, 2012

[23] CAP 730 Safety Management Systems for Air Traffic Management. A Guide to Implementation. UK Civil Aviation Authority Safety Regulation Group, 12 September 2002

[24] CAP 760 Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases For Aerodrome Operators and Air Traffic Service Providers, 10 December 2010

[25] Chung L. et al. *Non-Functional Requirements in Software Engineering*. Kluwer, 1999

[26] Clark D.D., & Wilson D.R. *A Comparison of Commercial and Military Computer Security Policies*, Proc. of the 1987 IEEE Symposium on Security and Privacy, IEEE, pp. 184—196, 1987

[27] CNSS. National Information Assurance Glossary. CNSS Instruction No. 4009, 26 April 2010. Available at http://www.cnss.gov/full-index.html

[28] Committee on Information Systems Trustworthiness. *Trust in Cyberspace, Computer Science and Telecommunications Board*. National Research Council, 1999

[29] Committee on National Security Systems (CNSS) Instruction 4009: National Information Assurance (IA) Glossary. Revised May 2003. Available at http://www.cnss.gov/Assets/ pdf/cnssi_4009.pdf

[30] Common Criteria Recognition Arrangement (CCRA). Common Criteria v 3.1 Revision 2. NIAP September 2007. Available at http://www.commoncriteriaportal.org

[31] Common Weaknesses Enumeration. MITRE, 2012. Available at http://cwe. mitre.org

[32] Cooke N.J., Gorman J.C., Winner J.L. Team Cognition. In:[43], pp. 239—268

[33] Courtois P.-J. *Justifying the Dependability of Computer-based Systems: With Applications in Nuclear Engineering*. Springer, 2008

[34] Cranor L., & Garfinkel S. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, 2005

[35] Dayton-Johnson. Jeff. Natural disasters and adaptive capacity. OECD Development Centre Research programme on: Market Access, Capacity Building and Competitiveness. Working Paper No. 237 DEV/DOC(2004)06, August 2004

[36] Department of Defense Directive 8500.1 (6 February 2003). Information Assurance (IA), Washington, DC. US Department of Defense, ASD(NII)/DoD CIO, April 23, 2007. Available at http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.

[37] Department of Defense Strategic Defense Initiative Organization. Trusted Software Development Methodology, SDI-S-SD-91-000007, vol. 1, 17 June 1992

[38] Department of Homeland Security National Cyber Security Division's "Build Security In" (BSI) web site, 2012, http://buildsecurityin.us-cert.gov

[39] Dependability Research Group. *Safety Cases*. University of Virginia, Available at: http:// dependability.cs.virginia.edu/info/Safety_Cases

[40] Despotou G., & Kelly T. *Extending the Safety Case Concept to Address Dependability*, Proceedings of the 22nd International System Safety Conference, 2004

[41] Dowd M., McDonald J., Schuh J. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Addison-Wesley, 2006

[42] Dunbar K., & Fugelsang J. Scientific Thinking and Reasoning. In: [59], pp.705—727

[43] Durso F.T., Nickerson R.S., Dumais S.T., Lewandowsky S., Perfect T.J. eds. *Handbook of Applied Cognition* 2nd edition. Wiley, 2007

[44] Ellsworth P.C. Legal Reasoning. In: [59], p. 685—704

[45] Ericsson K.A., Charness N., Feltovich P.J., Hoffman R.R. eds. *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, 2006

[46] Fenton N., Littlewood B., Neil M., Strigini L., Sutcliffe A., Wright D. Assessing dependability of safety critical systems using diverse evidence. *IEE Proc. Softw.* 1998 145 (1) pp. 35—39

[47] Gasser M. Building a Secure Computer System. Van Nostrand Reinhold, 1988. Available at http:// deke.ruc.edu.cn/wshi/readings/cs02.pdf

[48] Gray J.W. *Probabilistic Interference*. Proceedings of the IEEE Symposium on Research in Security and Privacy. IEEE, pp.170—179, 1990

[49] Greenwell W., Strunk E., Knight J. *Failure Analysis and the Safety-Case Lifecycle*. IFIP Working Conference on Human Error, Safety and System Development (HESSD) Toulouse, France. Aug 2004

[50] Greenwell W.S., Knight J.C., Pease J.J. *A Taxonomy of Fallacies in System Safety Arguments*. 24th International System Safety Conference, Albuquerque, NM, August 2006

[51] Hall A., & Chapman R. Correctness by Construction: Developing a Commercial Secure System. *IEEE Softw.*2002 Jan/Feb, 19 (1) pp. 18—25

[52] Herrmann D.S. *Software Safety and Reliability*. IEEE Computer Society Press, 1999

[53] Hoglund G., & McGraw G. *Exploiting Software: How to break code*. Addison-Wesley, 2004

[54] Hollnagel E., Woods D.D., Leveson N. eds. *Resilience Engineering: Concepts and Precepts*. Ashgate Pub Co, 2006

[55] Hollnagel E. ed. *Handbook of cognitive task design*. Lawrence Erlbaum Associates, 2003

[56] Hollnagel E. Human Error: Trick or Treat? In: [43], pp.219—238

[57] Hollnagel E. *Barriers and Accident Prevention*. Ashgate, 2004

[58] Hollnagel E. Human Factors: From Liability to Asset. Presentation, 2007. Available at www.vtt. fi/liitetiedostot/muut/Hollnagel.pdf

[59] Holyoak K.J., & Morrison R.G. eds. *The Cambridge Handbook of Thinking and Reasoning*. Cambridge University Press, 2005

[60] Howard M., & LeBlanc D.C. *Writing Secure Code*. Microsoft Press, Second Edition, 2002

[61] Howard M., & Lipner S. *The Security Development Lifecycle*. Microsoft Press, 2006

[62] Howell C. Assurance Cases for Security Workshop (follow-on workshop of the 2004 Symposium on Dependable Systems and Networks), June, 2005

[63] IEC 60050-191, *International Electrotechnical Vocabulary, Chapter 191: Dependability and Quality of Service*

[64] IEC 60300 *Dependability management [several parts]*

[65] IEC 60300-3-15 ed 1.0 (2009-06) Dependability management — Part 3-15 — Application guide — Engineering of system dependability

[66] IEC 60300-3-2 ed 2.0(2004-11), *Dependability management — Part 3-2: Application guide — Collection of dependability data from the field*

[67] IEC 60812 ed 2.0 (2006-01), *Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)*

[68] IEC 61025 ed 2.0 (2006-12), *Fault tree analysis (FTA)*

[69] IEC 61078 ed 2.0 (2006-01), *Analysis techniques for dependability — Reliability block diagram and Boolean methods*

[70] IEC 61508 ed 2.0, *Functional safety of electrical/electronic/programmable electronic safety-related systems* [several parts]

[71] IEC 61508-7 ed 2.0 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 7: Overview of techniques and measures*

[72] IEC 61511 ed 1.0, *Functional safety — Safety instrumented systems for the process industry sector* [several parts]

[73] [IEC] 61882 ed 1.0 (2001-05), *Hazard and operability studies (HAZOP studies) — Application guide*

[74] IEC CD 62741 ed 1.0, *Reliability of systems, equipment, and components. Guide to the demonstration of dependability requirements. The dependability case*

[75] Std IEEE 1228-1994, *IEEE Standard for Software Safety Plans*

[76] International Council on Systems Engineering INCOSE. Guide to Systems Engineering Body of Knowledge (G2SEBoK). Available at http:/ g2sebok.incose.org/

[77] ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

[78] ISO 13849, *Safety of machinery — Safety-related parts of control systems* [three parts]

[79] ISO 14620, *Space systems — Safety requirements* [three parts]

[80] ISO 14625:2007, *Space systems — Ground support equipment for use at launch, landing or retrieval sites — General requirements*

[81] ISO 19706:2011, *Guidelines for assessing the fire threat to people*

[82] ISO 20282, *Ease of operation of everyday products* [four parts]

[83] ISO 2394:1998, *General principles on reliability for structures*

[84] ISO 28003:2007, *Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems*

[85] ISO 9241-400:2007, *Ergonomics of human — system interaction — Part 400: Principles and requirements for physical input devices*

[86] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

[87] ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

[88] ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security* [three parts]

[89] ISO/IEC TR 15443, *Information technology — Security techniques — Security assurance framework* [two parts]

[90] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*

[91] ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk Management*

[92] ISO/IEC/IEEE 16326:2009, *Systems and software engineering — Life cycle management — Project management*

[93] ISO/IEC 18014, *Information technology — Security techniques — Time-stamping services* [three parts]

[94] ISO/IEC 18028, *Information technology — Security techniques — IT network security* [many parts]

[95] ISO/IEC 19770, *Information technology — Software Asset Management* [two parts]

[96] ISO/IEC 21827:2008, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*

[97] ISO/IEC 2382-14:1997, *Information technology — Vocabulary — Part 14: Reliability, maintainability and availability*

[98] ISO/IEC 25000:2005, *Software Engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE*

[99] ISO/IEC 25010:2011, *Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

[100] ISO/IEC 25012:2008, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data quality model*

[101] ISO/IEC 25020:2007, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE)— Measurement reference model and guide*

[102] ISO/IEC 25030:2007, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality requirements*

[103] ISO/IEC 25040:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*

[104] ISO/IEC 25051:2006, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing*

[105] ISO/IEC 26702:2007, *Systems engineering — Application and management of the systems engineering process*

[106] ISO/IEC 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[107] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[108] ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

[109] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[110] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[111] ISO/IEC 27006:2011, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[112] ISO/IEC 27011:2008, *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[113] ISO/IEC/IEEE 42010:2011, *Systems and software engineering — Architecture Description*

[114] ISO/IEC 90003:2004, *Software engineering Guidelines for the application of ISO 9001:2000 to computer software*

[115] ISO/IEC TR 15446:2009, *Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets*

[116] ISO/IEC TR 19791:2010, *Information technology — Security techniques — Security assessment of operational systems*

[117] ISO/IEC TR 24748-1:2010, *Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management*

[118] ISO/TR 16982:2002, *Ergonomics of human-system interaction — Usability methods supporting human-centred design*

[119] ISO/TR 18529:2000, *Ergonomics — Ergonomics of human-system interaction — Human-centred lifecycle process descriptions*

[120] ISO/TR 27809:2007, *Health informatics — Measures for ensuring patient safety of health software*

[121] ISO/TS 25238:2007, *Health informatics — Classification of safety risks from health software*

[122] Kazman R., Asundi J., Klein M. *Making Architecture Design Decisions: An Economic Approach, SEI-2002-TR-035*. Software Engineering Institute, Carnegie Mellon University, 2002

[123] Kazman R., Klein M., Clements P. ATAM: Method for Architecture Evaluating the Quality Attributes of a Software Architecture. Technical Report CMU/SEI-200-TR004. Software Engineering Institute, Carnegie Mellon University, 2000

[124] Kelly T. *Arguing Safety — A Systematic Approach to Managing Safety Cases*. Doctorial Thesis — University of York. Department of Computer Science. Sept 1998

[125] Kelly T. *Reviewing Assurance Arguments — A Step-by-Step Approach*. Workshop on Assurance Cases for Security: The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[126] Kelly T., & Weaver R. *The Goal Structuring Notation — A Safety Argument Notation*. Workshop on Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities, Florence, Italy. July 2004

[127] Ladkin P. *The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed*. 29 Aug 2002. Available at http://www.rvs.uni-bielefeld.de/publications/Reports/SCflawed-paper.html

[128] Landwehr C. Computer Security. *IJIS*. 2001, 1 pp. 3—13

[129] Lautien S., Cooper D., Jackson D. *SafSec: Commonalities Between Safety and Security Assurance*. Proceedings of the Thirteenth Safety Critical Systems Symposium — Southampton, 2005

[130] LeBoeuf R.A., & Shafir E.B. Decision Making. In: [59], pp.243—266

[131] Leveson N. A Systems-Theoretic Approach to Safety in Software-Intensive Systems, *IEEE Trans. Dependable Sec. Comput*. 2004, 1 (1) pp. 66—86

[132] Lipner S., & Howard M. *The Trustworthy Computing Security Development Lifecycle*, Microsoft, 2005. Available at http://msdn.microsoft.com/en-us/library/ms995349.aspx

[133] Maguire R. *Safety Cases abd Safety Reports: Meaning, Motivation and Management*. Ashgate, 2006

[134] McDermid J. *Software Safety: Where's the Evidence?* 6th Australian Workshop on Industrial Experience with Safety Critical Systems and Software (SCS'01), Brisbane. 2001

[135] McGraw G. *Software Security: Building Security In*. Addison Wesley, 2006

[136] McLean J. Security Models. In: *Encyclopedia of Software Engineering*, (Marciniak J. ed.). Wiley, 1994

[137] Meier J.D., Mackman A., Vasireddy S., Dunner M., Escamilla R., Murukan A. *Improving Web Application Security: Threats and Countermeasures*, Microsoft, 2004. Available at: http://download.microsoft.com/download/d/8/c/d8c02f31-64af-438ca9f4-e31acb8e3333/Threats_Countermeasures.pdf

[138] Merkow M.S., & Breithaupt J. *Computer Security Assurance Using the Common Criteria*. Thompson Delamr Learning, 2005

[139] Ministry of Defence. Defence Standard 00-42 Issue 2, Reliability and Maintainability (R&M) Assurance Guidance. Part 3, R&M Case, 6 June 2003

[140] Ministry Of Defence. Defence Standard 00-55 (PART 1)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 1: Requirements, 21 August 1997

[141] Ministry of Defence. Defence Standard 00-55 (PART 2)/Issue 2, Requirements for Safety Related Software in Defence Equipment Part 2: Guidance, 21 August 1997

[142] Ministry of Defence. Interim Defence Standard 00-56, Safety Management Requirements for Defence Systems Part 1: Requirements, 17 December 2004

[143] Ministry of Defence. Interim Defence Standard 00-56, Safety Management Requirements for Defence Systems Part 2: Guidance on Establishing a Means of Complying with Part 1, 17 December 2004

[144] Moore A., Klinker E., Mihelcic D. How to Construct Formal Arguments that Persuade Certifiers. In: *Industrial Strength Formal Methods in Practice*. Academic Press. 1999

[145] National Aeronautics and Space Administration (NASA) Software Assurance Guidebook. September 1989 (NASA-GB-A201). Available at http.//www.hq.nasa. gov/office/codeq/doctree/ nasa_gb_a201.pdf

[146] National Offshore Petroleum Safety Authority. Safety case. [Online Documents [cited on: 20 Jun 2012] Available at http://www.nopsema.gov.au/safety/safety-case/

[147] National Research Council (NRC) Computer Science and Telecommunications Board. (CSTB). Cybersecurity Today and Tomorrow: Pay Now or Pay Later. National Academies Press, 2002. Available at http://www.nap.edu/topics.php? topic=320&start=10

[148] National Security Agency, The Information Systems Security Engineering Process (IATF) v3.1. 2002

[149] Naval Research Laboratory. *Handbook for the Computer Security Certification of Trusted Systems*. US Naval Research Laboratory, 1995

[150] NDIA System Assurance Committee. *Engineering for System Assurance*. National Defense Industrial Association, USA, 2008

[151] NIST. Federal Information Processing Standards Publication (FIPS PUB) 200: Minimum Security Requirements for Federal Information and Information Systems. March 2006. Available at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

[152] NIST. NIST Special Publication 800-27, Rev A: Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Revision A, June 2004. Available at http://csrc.nist. gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[153] NIST. NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security, December 2001. Available at http://csrc.nist.gov/publications/ nistpubs/800-33/sp800-33.pdf

[154] Process Framework O.P.E.N. Safety Cases. [Online Document cited on: 20 Jun 2012] Available at: http://www.opfro.org/index.html? Components/WorkProducts/SafetySet/SafetySet. html~Contents

[155] OPSI. The Offshore Installations (Safety Case) Regulations 2005. [Online Document cited on: 20 June 2012]. Available at http://www.opsi.gov.uk/si/si2005/20053117.htm

[156] Park J., Montrose B., Froscher J. *Tools for Information Security Assurance Arguments. DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01*. Proceedings, 2001

[157] Petroski H. *Design Paradigms*. Cambridge University Press, 1994

[158] Prasad D. *Dependable Systems Integration using Measurement Theory and Decision Analysis*, PhD Thesis, Department of Computer Science, University of York, UK, 1998

[159] PSM Safety & Security TWG. *Security Measurement*. Nov. 2004

[160] Pullum L.L. *Software Fault Tolerance*. Artech House, 2001

[161] Randell B., & Koutny M. Failures: Their Definition, Modelling and Analysis. School of Computing Science, Newcastle University CS-TR NO 994, Dec. 2006 Randell B. & Rushby J.M. Distributed Secure Systems. Then and Now. CS-TR No 1052 School of Computing Science, Newcastle University, Oct. 2007

[162] Rechtin E. *Systems Architecting of Organizations: Why Eagles Can't Swim*. CRC Press, Boca Raton, FL, 2000

[163] Redwine S.T. Jr. ed. *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software Version 1.1*. US Department of Homeland Security, September 2006

[164] Redwine S.T. Jr. *The Quality of Assurance Cases*. Workshop on Assurance Cases for Security: The Metrics Challenge, International Conference on Dependable Systems and Networks, 2007

[165] Redwine S.T. Jr., & Davis N. eds. Processes for Producing Secure Software: Towards Secure Software. Vols. I and II. Washington, D.C.: National Cyber Security Partnership, 2004. Available at http://www.cigital.com/papers/download/secure_software_process.pdf

[166] Ross K.G., Shafer J.L., Klein G. Professional Judgements and 'Naturalistic Decision Making'. In: [45], pp. 403—420

[167] Ross R. et al. Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, Aug 2009. Available at http://csrc.nist.gov/publications/nistpubs/80053-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[168] SAE JA1000, *Reliability Program Standard, SAE International, June 1998. Available at* http://www. sae.org

[169] Saltzer J.H., & Schroeder M.D. The protection of information in computer systems. *Proc. IEEE*. 1975, 63 (9), pp. 1278—1308. Available at: http://cap-lore.com/CapTheory/ProtInf/

[170] Seminal Papers — History of Computer Security Project, University of California Davis Computer Security Laboratory. Available at: http://seclab.cs. ucdavis.edu/projects/history/seminal.html

[171] Serene. "Safety argument", [Online Document] [cited on. 13 Feb 2007] Available at: http://www2. dcs.qmul.ac.uk/~norman/SERENE_Help/sereneSafety_argument.htm

[172] Severson K. *Yucca Mountain Safety Case Focus of NWTRB September Meeting*. United States Nuclear Waste Technical Review Board. Aug. 2006

[173] Sieck W.R., & Klein G. Decision making. In: [43], pp. 195—218

[174] Software and Systems Engineering Vocabulary (sevocab). Available at www.computer.org/sevocab

[175] Sommerville I. *Software Engineering*. Pearson Education, Eighth Edition, 2006

[176] Stoneburner G., Hayden C., Feringa A. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Revision A, NIST Special Publication 800-27 Rev A, June 2004

[177] Storey N. *Safety-Critical Computer Systems*. Addison Wesley, 1996

[178] Strunk E., & Knight J. *The Essential Synthesis of Problem Frames and Assurance Cases*. IWAAPF'06, Shanghai, China. May 2006

[179] Swiderski F., & Snyder W. *Threat Modeling*. Microsoft Press, 2004

[180] U.S. NRC. "Quality Assurance Case Studies at Construction Projects"

[181] Vanfleet W.M. et al. MILS: "Architecture for High Assurance Embedded Computing," Crosstalk, August, 2005

[182] Viega J., & McGraw G. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison Wesley, Reading, MA, 2001

[183] Walker V.R. Risk Regulation and the 'Faces' of Uncertainty, *Risk: Health, Safety and Environment*. pp. 27—38, Winter 1998

[184] Ware W.H. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security, The RAND Corporation, Santa Monica, CA (Feb. 1970)

[185] Weaver R. *The Safety of Software — Constructing and Assuring Arguments*. Doctorial Thesis — University of York: Department of Computer Science. 2003

[186] Weaver R., Fenn J., Kelly T. *A Pragmatic Approach to Reasoning about the Assurance of Safety Arguments*. 8th Australian Workshop on Safety Critical Systems and Software (SCS'03), Canberra. 2003

[187] Whittaker J.A., & Thompson H.H. *How to Break Software Security: Effective Techniques for Security Testing*. Pearson Education, 2004

[188] Williams J., & Schaefer M. Pretty Good Assurance. Proceedings of the New Security Paradigms Workshop. IEEE Computer Society Press. 1995

[189] Williams J.R., & Jelen G.F. A Framework for Reasoning about Assurance, Document Number ATR 97043, Arca Systems, Inc., 23 April 1998

[190] Yates J.F., & Tschirhart M.D. Decision-Making Expertise. In: [45], pp. 421—438

[191] Yee K.-P. User interaction design for secure systems. Proceedings of the 4th International Conference on Information and Communications Security, Springer-Verlag, LNCS 2513, 2002

УДК 006.34:004.05:004.052:006.354 ОКС 35.080

Ключевые слова: информационные технологии, программное обеспечение, гарантия, гарантирование, требование, гарантийный случай, надежность, процесс, продукт, система, элемент системы, уровень целостности, последствие, риск, дефект, ошибка, атака, нарушение, отказ, организация, ответственный за систему, ответственный проектировщик, ответственный за обеспечение целостности

Редактор *П.М. Смирнов*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 05.05.2016. Подписано в печать 13.05.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,80. Тираж 33 экз. Зак. 1281.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru