ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 16085— 2007

Менеджмент риска

ПРИМЕНЕНИЕ В ПРОЦЕССАХ ЖИЗНЕННОГО ЦИКЛА СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ISO/IEC 16085:2006
Systems and software engineering — Life cycle processes — Risk management
(IDT)

Издание официальное

БЗ 2—2008/536

Москва
Стандартинформ
2008

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Открытым акционерным обществом «Научно-исследовательский центр контроля и диагностики технических систем» (ОАО «НИЦ КД») на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2007 г. № 568-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 16085:2006 «Разработка систем и программного обеспечения. Процессы жизненного цикла. Менеджмент риска» (ISO/IEC 16085:2006 «Systems and software engineering — Life cycle processes — Risk management»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (подраздел 3.5).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

ПРИМЕНЕНИЕ В ПРОЦЕССАХ ЖИЗНЕННОГО ЦИКЛА СИСТЕМ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Risk management.
Application for system and software life cycle processes

Дата введения — 2008—09—01

1 Краткий обзор

Настоящий стандарт устанавливает непрерывный процесс менеджмента риска программного обеспечения. Раздел 1 содержит краткое описание процесса, а также определение цели, области применения и критериев соответствия процесса менеджмента риска требованиям настоящего стандарта. В разделе 2 приведены ссылочные стандарты; дополнительные нормативные и справочные документы представлены в структурном элементе «Библиография». Раздел 3 содержит основные термины и определения. Раздел 4 конкретизирует применение менеджмента риска на стадиях жизненного цикла программного обеспечения. В разделе 5 установлены требования к процессу менеджмента риска.

В настоящем стандарте представлено четыре приложения. В приложениях А, В и С приведены примеры трех документов: плана менеджмента риска, информации о действиях с риском и плана обработки риска. Приложение D содержит обзор ссылок на менеджмент риска в стандартах серии ИСО/МЭК 12207 по стадиям жизненного цикла программного обеспечения. Эквивалентное приложение не включено в стандарт ИСО/МЭК 15288, относящийся к процессам жизненного цикла системы.

Приложение Е настоящего стандарта, содержит краткое описание ссылочных и взаимосвязанных с ним стандартов и других нормативных документов.

1.1 Область применения

Настоящий стандарт устанавливает процесс менеджмента риска при заказе, поставке, разработке, эксплуатации и сопровождении программного обеспечения.

1.2 Цель

Целью настоящего стандарта является установление единых требований к процессу менеджмента риска программного обеспечения для поставщиков, заказчиков, разработчиков и менеджеров. Настоящий стандарт не содержит подробного описания методов менеджмента риска, а сосредоточивает внимание пользователей на определении общего процесса менеджмента риска, в котором могут быть применены любые методы менеджмента риска.

1.3 Основные положения

Настоящий стандарт устанавливает процесс менеджмента риска на различных стадиях жизненного цикла программного обеспечения. Стандарт может быть применен во всех проектах организации. Его применение может быть полезно для установления процесса менеджмента риска при разработке систем и/или программного обеспечения.

Настоящий стандарт совместим со стандартами серии ИСО/МЭК 12207, ИСО/МЭК 15288, но может быть применен самостоятельно.

1.3.1 Связь с ИСО/МЭК 12207

ИСО/МЭК 12207 описывает процессы заказа, поставки, разработки, эксплуатации и сопровождения программного обеспечения. Согласно этому стандарту менеджмент риска является одним из основных факторов, обеспечивающих успех организации при проектировании программного обеспечения. В ИСО/МЭК 12207 применены термины «риск» и «менеджмент риска», но процесс менеджмента риска

Издание официальное

не описан (см. приложение D). В настоящем стандарте описан процесс менеджмента риска в соответствии с его определением в поправках к ИСО/МЭК 12207 (ИСО/МЭК 12207:1995/Поправка 1, ИСО/МЭК 12207:1995/Поправка 2). Настоящий стандарт может быть использован руководством, персоналом и другими причастными сторонами для управления риском в организации или при разработке проекта в любой области и на любой стадии жизненного цикла.

В соответствии со структурой процесса жизненного цикла, установленной ИСО/МЭК 12207, менеджмент риска относится к процессам менеджмента жизненного цикла. Ответственность за работы и задачи процесса менеджмента несет организация, выполняющая процесс.

Использование настоящего стандарта совместно с ИСО/МЭК 12207 основано на предположении о том, что обработка риска должна быть выполнена в других процессах менеджмента и технических процессах в соответствии с ИСО/МЭК 12207. В настоящем стандарте рассмотрена также его взаимосвязь с ИСО/МЭК 12207.

1.3.2 Связь с ИСО/МЭК 15288

ИСО/МЭК 15288 устанавливает процесс менеджмента риска и использует термины «риск» и «менеджмент риска» в нескольких местах. Настоящий стандарт может быть использован для менеджмента риска организации или проекта в любой области и на любой стадии жизненного цикла продукции и может быть полезен при планировании перспективного развития руководству, персоналу и другим причастным сторонам.

Настоящий стандарт совместим с процессом менеджмента риска, установленным ИСО/МЭК 15288, и содержит дополнительную информацию о планировании и реализации процесса менеджмента риска.

Использование настоящего стандарта совместно с ИСО/МЭК 15288 основано на предположении о том, что обработка риска должна быть выполнена в других процессах менеджмента и технических процессах в соответствии с ИСО/МЭК 15288. Цели, область применения и требования, приведенные в разделе 1 настоящего стандарта, могут быть интерпретированы для применения к жизненному циклу системы. Термины и определения (раздел 3), информация о процессе (раздел 5), а также основные положения плана менеджмента риска (приложение А), информация о действиях с риском (приложение В) и план обработки риска (приложение С) могут быть непосредственно применены к жизненному циклу системы.

1.3.3 Самостоятельное применение стандарта

Настоящий стандарт может быть использован независимо от других стандартов, относящихся к процессам жизненного цикла программного обеспечения. В этом случае для применения настоящего стандарта должны быть установлены дополнительные требования по обработке риска.

1.4 Соответствие

Соответствие организации или проекта требованиям настоящего стандарта может быть достигнуто путем разработки и внедрения соответствующих планов и выполнения всех необходимых требований (обязательность которых подчеркнута словом «должен»), установленных в разделе 5.

Для случаев применения настоящего стандарта независимо от ИСО/МЭК 12207 или ИСО/МЭК 15288 дополнительные требования по обработке риска приведены в 5.1.4.2.2.

1.5 Ограничения

Настоящий стандарт устанавливает минимальные требования для процесса, действий и задач менеджмента риска программного обеспечения. Выполнение этих требований, подготовка планов менеджмента риска программного обеспечения или информации о действиях с риском программного обеспечения в соответствии с настоящим стандартом не гарантирует отсутствие другого риска. Соответствие настоящему стандарту не освобождает организацию или другие заинтересованные стороны от любых социальных, моральных, финансовых и/или юридических обязательств.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ИСО/МЭК Руководство 51:1999 Аспекты безопасности. Руководящие указания по включению их в стандарты

ИСО/МЭК Руководство 73:2002 Управление риском. Словарь. Руководящие указания по использованию в стандартах

ИСО 3534-1:2006 Статистика. Словарь и условные обозначения. Часть 1. Общие статистические термины и термины, используемые в вероятностных задачах

ИСО 10006:2003 Системы менеджмента качества. Руководство по менеджменту качества при проектировании

ИСО/МЭК 12207:1995 Информационная технология. Процессы жизненного цикла программного обеспечения

ИСО/МЭК 12207:1995/Поправка 1:2002 Информационные технологии. Процессы жизненного цикла программного обеспечения. Поправка 1

ИСО/МЭК 12207:1995/Поправка 2:2004 Информационные технологии. Процессы жизненного цикла программного обеспечения. Поправка 2

ИСО 14971:2007 Устройства медицинские. Применение управления рисками к медицинским устройствам

ИСО/МЭК 15026:1998 Информационная технология. Уровни целостности систем и программных средств

ИСО/МЭК 15288:2002 Информационная технология. Процессы жизненного цикла системы

ИСО/МЭК 15939:2007 Технология программного обеспечения. Процесс измерения

ИСО/МЭК ТО 19760:2003 Системотехника. Руководство по применению ИСО/МЭК 15288 (Процессы жизненного цикла системы)

МЭК 60300-1:2003 Менеджмент надежности. Часть 1. Системы менеджмента надежности

МЭК 60300-2:2004 Менеджмент надежности. Часть 2. Руководство по менеджменту надежности

МЭК 60300-3-9:1995 Управление общей надежностью. Часть 3. Руководство по применению. Раздел 9. Анализ риска технологических систем

МЭК 60812:2006 Методы анализа надежности систем. Метод анализа видов и последствий отказов (FMEA)

МЭК 61025:2006 Анализ дерева неисправностей (FTA)

МЭК 61508-1:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

МЭК 61508-2:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам

МЭК 61508-3:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

МЭК 61508-4:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Определения и сокращения

МЭК 61508-5:1998 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Примеры методов определения уровней полноты безопасности

МЭК 61508-6:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению МЭК 61508-2:2000 и МЭК 61508-3:1998

МЭК 61508-7:2000 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Анализ методов и средств

МЭК 61713:2000 Функциональная надежность программного обеспечения в процессе жизненного цикла программного обеспечения. Руководство по применению

МЭК 62198:2001 Менеджмент риска при проектировании. Руководство по применению

Примечания

1 Если настоящий стандарт применяют самостоятельно, нет необходимости в применении ИСО/МЭК 12207.

2 Вместо IEEE/EIA 12207.0 [1] может быть использован ИСО/МЭК 12207.

3 Если настоящий стандарт применяют самостоятельно, нет необходимости в применении ИСО/МЭК 15288.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

Примечание — Для терминов, не установленных в настоящем разделе, должна быть приведена ссылка на словарь терминов IEEE 100 [2] и IEEE 610.12 [3].

3.1 **последствие** (consequence): Результат события.

Примечания

1 Результатом события может быть одно или более последствие.

2 Последствия могут быть ранжированы от позитивных до негативных. Однако применительно к безопасности последствия всегда негативные.

3 Последствия могут быть выражены количественно и качественно.
[ИСО/МЭК Руководство 73:2002, пункт 3.1.2]

3.2 **событие** (event): Возникновение специфического набора обстоятельств, при которых происходит явление.

Примечания
1 Событие может быть определенным или неопределенным.
2 Событие может быть единичным или многократным.
3 Вероятность, связанная с событием, может быть оценена для данного интервала времени.
[ИСО/МЭК Руководство 73:2002, пункт 3.1.4]

3.3 **вероятность** (probability): Мера того, что событие может произойти.

Примечания
1 ИСО 3534-1 дает математическое определение вероятности: «действительное число в интервале от 0 до 1, относящееся к случайному событию». Число может отражать относительную частоту в серии наблюдений или степень уверенности в том, что некоторое событие произойдет. Для высокой степени уверенности вероятность близка к единице.
2 При описании риска вместо вероятности может быть использована частота.
3 Степени уверенности относительно вероятности могут быть выбраны как классы или ранги такого типа, как:
- редкий/маловероятный/умеренный/вероятный/почти уверенный, или
- невероятный / маловероятный /незначительный/ случайный / вероятный / частый.
[ИСО/МЭК Руководство 73:2002, пункт 3.1.3]

3.4 **профиль риска проекта** (project risk profile): Текущие и хронологические данные о риске, присущем проекту, в виде резюме или общего описания всех соответствующих индивидуальных рисков.

Примечание — Информация, относящаяся к профилю риска проекта, наряду с хронологическими записями о риске включает в себя профили индивидуальных рисков, приоритеты измерений, связанных с риском, статус обработки риска, план действий в случае непредвиденных обстоятельств и информацию о действиях с риском. Профиль риска представляет собой совокупность профилей риска всех индивидуальных рисков, которые в свою очередь включают в себя текущие и исторические данные о риске (см. 3.14 и 3.15).

3.5 **риск** (risk): Сочетание вероятности события и его последствий.

Примечания
1 Термин «риск » обычно применяют только тогда, когда существует возможность негативных последствий.
2 В некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата.
3 Применительно к безопасности см. ИСО Руководство 51.
[ИСО/МЭК Руководство 73:2002, пункт 3.1.1]

3.6 **принятие риска** (risk acceptance): Решение принять риск.

Примечания
1 Термин «принятие риска» выбран для того, чтобы отразить требование минимальной приемлемости риска.
2 Принятие риска зависит от критериев риска.
[ИСО/МЭК Руководство 73:2002, пункт 3.4.10]

3.7 **информация о действиях с риском** (risk action request): Рекомендуемые альтернативные методы обработки риска (одного или более) и соответствующая необходимая информация при превышении допустимого значения риска.

3.8 **категория риска** (risk category): Класс или тип риска (например, технический, юридический, организационный, экономический риск, а также риск, связанный с безопасностью, затратами, невыполнением графика).

Примечание — Категория риска — это характеристика источников риска.

3.9 **критерии риска** (risk criteria): Правила, по которым оценивают значимость риска.

Примечание — Критерии риска могут включать в себя соответствующие ущерб и выгоды, законодательные и обязательные требования, социально-экономические и экологические факторы, озабоченность и приоритеты причастных сторон, и другие данные для оценки риска.
[ИСО/МЭК Руководство 73:2002, пункт 3.1.6]

3.10 **экспозиция риска** (risk exposure): Потенциальные потери, относящиеся к конкретному человеку, проекту или организации в виде функции вероятности появления опасного события и величины последствий его возникновения.

Примечание — Экспозицию риска обычно определяют как произведение вероятности опасного события на величину его последствий, т. е. на математическое ожидание этой величины, что дает математическое ожидание экспозиции риска. Настоящий стандарт по менеджменту риска устанавливает более широкое представление о воздействии риска, включая его качественное выражение.

3.11 **план менеджмента риска** (risk management plan): Описание того, как элементы и ресурсы процесса менеджмента риска будут применены в организации или для проекта.

3.12 **процесс менеджмента риска** (risk management process): Непрерывный процесс, направленный на систематическую идентификацию, анализ, обработку и мониторинг риска на всех стадиях жизненного цикла продукции или услуг.

3.13 **система менеджмента риска** (risk management system): Набор элементов системы менеджмента организации в отношении риска.

Примечания

1 Элементы системы менеджмента риска могут включать в себя стратегическое планирование, принятие решений и другие процессы, затрагивающие риск.

2 На системе управления риском обычно отражается культура организации.

[ИСО/МЭК Руководство 73:2002, пункт 3.1.8]

3.14 **профиль риска** (risk profile): Записи текущей и хронологической информации о состоянии риска.

3.15 **состояние риска** (risk state): Текущая информация о риске проекта, относящаяся к индивидуальным рискам.

Примечание — Информация об индивидуальном риске может включать в себя описание текущего состояния, причины, вероятность, последствия, оценочную шкалу, достоверность оценок, обработку, допустимый риск и оценку достижения риском своего порога.

3.16 **допустимый риск** (risk threshold): Условие, на основе которого причастные стороны предпринимают действия, связанные с риском.

Примечание — Для каждого вида риска могут быть определены свой допустимый риск, категория риска и комбинация опасных событий.

3.17 **обработка риска** (risk treatment): Процесс выбора и выполнения мер по изменению (снижению) риска.

Примечания

1 Термин «обработка риска» иногда используют для обозначения самих мер.

2 Меры по обработке риска могут включать в себя предотвращение, оптимизацию, перенос или сохранение риска.

[ИСО/МЭК Руководство 73:2002, пункт 3.4.1]

3.18 **источник** (source): Объект или деятельность с потенциальными последствиями.

Примечание — Применительно к безопасности источник представляет собой опасность (см. ИСО/МЭК Руководство 51).

[ИСО/МЭК Руководство 73:2002, пункт 3.1.5]

3.19 **причастная сторона** (stakeholder): Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечания

1 Лицо, принимающее решение, также является причастной стороной.

2 Причастная сторона включает в себя заинтересованную сторону, но имеет более широкое значение, чем заинтересованная сторона

[ИСО/МЭК Руководство 73:2002, пункт 3.2.1]

4 Применение настоящего стандарта

Для удобства применения настоящего стандарта совместно с ИСО/МЭК 12207 и ИСО/МЭК 15288 при описании процесса менеджмента риска использованы основные положения этих стандартов. Процесс менеджмента риска разделен на ряд действий, а требования к каждому действию установлены в наборе задач. Подразделы второго уровня (х.1) обозначают процессы, пункты третьего уровня (х.х.1) обозначают действия, а подпункты четвертого уровня (х.х.х.1) обозначают задачи.

Настоящий стандарт, относящийся к менеджменту риска программного обеспечения, предназначен для поддержки процессов заказа, поставки, разработки, эксплуатации и сопровождения программного обеспечения товаров и услуг. Применение стандарта не требует от организации разработки специальной модели процесса жизненного цикла программного обеспечения.

Процесс менеджмента риска программного обеспечения функционирует более эффективно, если его используют совместно с другими процессами менеджмента риска организации. Организация должна объединить процессы, действия и задачи менеджмента риска, установленные настоящим стандартом, с другими методами и системами менеджмента риска организации. Если в организации не установлены процессы менеджмента риска, настоящий стандарт может быть полезным в качестве руководства по их созданию.

Несмотря на то, что применение стандарта ориентировано на риски, связанные с программным обеспечением, процесс должен быть интегрирован и скоординирован с другими проблемами и подходами менеджмента организации, например при внедрении плана действий в случае непредвиденных обстоятельств. К управлению обработкой риска в организации должны быть предъявлены те же требования, что и к управлению проектом.

Менеджмент риска становится наиболее эффективным при его интеграции с процессами измерений. ИСО/МЭК 15939 определяет процесс измерений, применимый к техническим и управленческим вопросам. Процесс измерений, определенный в ИСО/МЭК 15939, совместно с действиями и задачами менеджмента риска, определенными в настоящем стандарте, позволяет охарактеризовать и получить количественную оценку риска.

5 Менеджмент риска жизненного цикла программного обеспечения

Основная цель менеджмента риска состоит в постоянной идентификации, анализе, обработке и мониторинге риска. Результатом успешного внедрения процесса менеджмента риска являются:

a) определение области применения менеджмента риска;

b) определение и внедрение соответствующих стратегий менеджмента риска;

c) идентификация риска на всех стадиях реализации проекта;

d) проведение анализа риска и определение приоритетных областей вложения ресурсов, необходимых для мониторинга риска;

e) определение, применение и оценка риска для определения изменения статуса риска и его мониторинга;

f) проведение соответствующей обработки риска, необходимой для корректировки и предотвращения воздействия риска и основанной на определении приоритетов, вероятности и последствий.

5.1 Процесс менеджмента риска

Процесс менеджмента риска представляет собой непрерывные систематические действия с риском на всех стадиях жизненного цикла продукции или услуги.

Процесс менеджмента риска состоит из следующих действий:

a) планирования и внедрения менеджмента риска;

b) управления профилем риска проекта;

c) анализа риска;

d) мониторинга риска;

e) обработки риска;

f) оценки процесса менеджмента риска.

Процесс менеджмента риска представлен на рисунке 1. Обработка риска является общей составляющей технических процессов и процессов менеджмента. Цифры в кружочках в приведенном ниже тексте соответствуют аналогичным цифрам на рисунке 1.

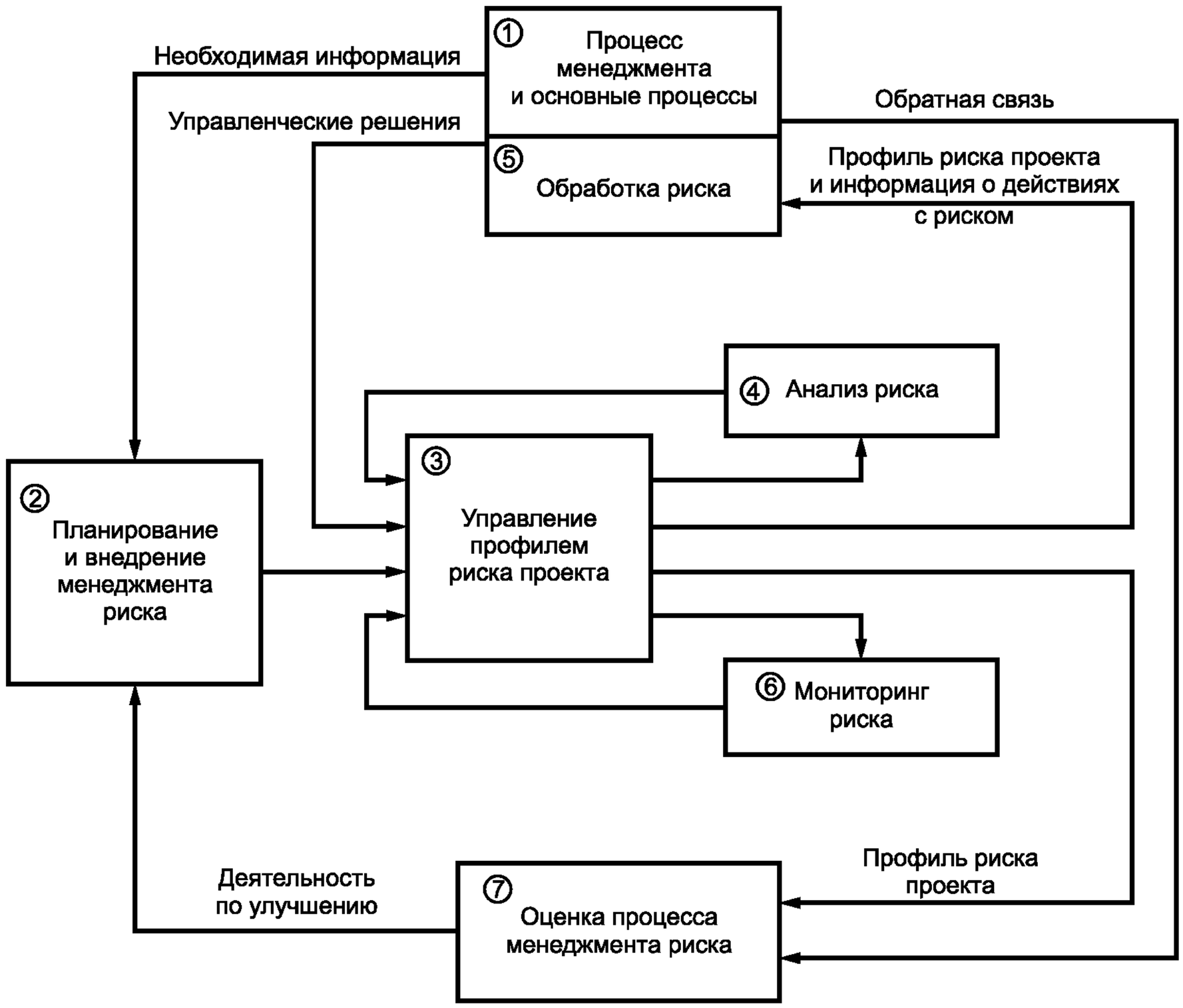

Рисунок 1 — Модель процесса менеджмента риска

На основе процессов менеджмента и технических процессов ① причастные стороны определяют информацию, необходимую для поддержки процессов менеджмента риска (данные, используемые причастными сторонами для принятия обоснованных решений, связанных с риском). Эту информацию используют при планировании и внедрении менеджмента риска проекта и управлении профилем риска проекта. На этапе планирования и внедрения менеджмента риска ② организация должна установить политику в области менеджмента риска, а также применяемые процедуры и методы менеджмента риска.

На этапе управления профилем риска проекта ③ организация должна проанализировать информацию о прошлом и текущем состояниях менеджмента риска. Профиль риска проекта включает в себя все профили индивидуальных рисков (т. е. текущие и исторические данные об индивидуальных рисках), которые, в свою очередь, включают в себя все состояния риска.

Организация должна постоянно актуализировать информацию о профиле риска проекта путем выполнения анализа риска ④. В процессе анализа риска организация должна идентифицировать риски, определить соответствующие вероятности появления опасного события, его последствия и экспозицию риска, а также подготовить информацию о действиях с риском, на основании которой разрабатывают рекомендации по обработке рисков, превысивших допустимый риск.

Рекомендации по обработке риска, наряду со статусом других рисков и их обработкой, должны быть подвергнуты анализу со стороны руководства ⑤. Руководство организации должно принять решение о том, какая обработка риска будет проведена для риска, признанного недопустимым. Для риска, требующего обработки, организация должна разработать планы обработки риска. Эти планы должны быть скоординированы с другими планами и действиями организации.

Организация должна проводить постоянный мониторинг риска ⑥ всех видов, например отступлений на отклонение, пока существует такая необходимость. Кроме того, организация должна выявлять новые риски.

Для обеспечения результативности процесса менеджмента риска организация должна через запланированные интервалы времени проводить его оценку. На этапе оценки процесса менеджмента риска ⑦ должен быть проведен сбор информации, полученной от пользователей по обратной связи, необходимой для улучшения процесса менеджмента риска и/или возможностей менеджмента риска организации или проекта. Данные, полученные в результате оценки процесса менеджмента риска, должны быть использованы на этапе планирования и внедрения менеджмента риска ②.

Организация должна применять процесс менеджмента риска непрерывно на всех стадиях жизненного цикла продукции. Однако действия и задачи процесса менеджмента риска итеративно воздействуют на индивидуальные риски только с момента начала процесса менеджмента риска. Например, при выполнении действий по анализу риска ④ риск может быть повторно оценен несколько раз из-за увеличения данных о риске, полученных во время выполнения задачи оценки риска. Процесс менеджмента риска не является каскадным процессом.

5.1.1 Планирование и внедрение менеджмента риска

Основной целью деятельности по планированию и внедрению менеджмента риска является установление процесса менеджмента риска. Если в организации установлен процесс менеджмента риска, процесс менеджмента риска программного обеспечения должен быть совместим с ним. В результате этих действий организация должна установить персонал, ответственный за менеджмент риска, определить самостоятельный процесс менеджмента риска, выделить ресурсы, необходимые для выполнения указанного процесса, определить способ обмена информацией о риске для причастных сторон и скоординировать их действия.

Действия по планированию и внедрению менеджмента риска должны быть предприняты в начале разработки проекта и повторены при получении информации о необходимости изменений. Информация, полученная в результате этих действий, должна быть зарегистрирована в плане менеджмента риска. Пример плана менеджмента риска представлен в приложении А.

Примечание — IEEE 1058 [4] содержит требования к документированию плана менеджмента риска в плане менеджмента проекта программного обеспечения. AS/NZS 4360 [5] содержит общую структуру для установления и внедрения системы менеджмента риска организации.

Эта деятельность состоит из задач, перечисленных в 5.1.1.1—5.1.1.5.

5.1.1.1 Установление политики в области менеджмента риска

Организация должна разработать политику в области менеджмента риска, устанавливающую руководящие принципы, в соответствии с которыми должен функционировать процесс менеджмента риска. Политика в области менеджмента риска должна помогать в сборе информации о риске, требуемой причастными сторонами, и предусматривать обеспечение:

a) внедрения, управления и поддержки в рабочем состоянии менеджмента риска со стороны руководства и остального персонала организации;

b) распределения обязанностей по менеджменту риска между причастными сторонами;

c) скоординированной деятельности по процессу менеджмента риска между причастными сторонами;

d) обучения персонала по процессу менеджмента риска и наличия требований к квалификации персонала в области риска;

e) необходимой информации о риске, например, каким образом и как часто профиль риска проекта должен быть направлен причастным сторонам для рассмотрения;

f) ресурсами, необходимыми для обработки риска.

Политика в области менеджмента риска должна учитывать, по возможности, существующую политику менеджмента риска организации. Если вышеперечисленные положения уже установлены в документально оформленной политике организации в области менеджмента риска, то на них может быть дана ссылка, а задокументированы только отдельные положения, вытекающие из особенностей проекта.

5.1.1.2 Установление процесса менеджмента риска

Описание внедряемого процесса менеджмента риска должно быть документально оформлено и доведено до сведения всех заинтересованных сторон. Описание процедур, необходимых для внедрения и функционирования процесса менеджмента риска, должно включать в себя следующее:

a) частоту повторного анализа и мониторинга риска;

b) тип анализа риска (количественный и/или качественный);

c) шкалу оценки вероятности опасного события и его последствий, неопределенность измерений и описание последствий;

d) типы используемых допустимых рисков;

e) типы средств измерений, используемых для прослеживания и мониторинга состояния риска;

f) приоритетность обработки риска;

g) определение причастных сторон процесса менеджмента риска;

h) категории риска.

В решение этой задачи входит определение процедур и методов процесса менеджмента риска в соответствии с требованиями проекта.

Примечание — МЭК 60300-3-9 содержит руководство по выбору и реализации методов анализа риска. МЭК 61508-7 содержит полезные материалы по измерениям и методам, связанным с безопасностью.

Процесс менеджмента риска должен учитывать, по возможности, существующие процессы менеджмента риска организации. При документировании процесса менеджмента риска организация должна определить и оформить в установленном порядке необходимую для работы документацию и/или особые требования к процессу менеджмента риска.

5.1.1.3 Распределение ответственности

Стороны, ответственные за внедрение менеджмента риска, их обязанности и полномочия должны быть установлены. Организация должна определить ответственных за функционирование процесса менеджмента риска в организации.

5.1.1.4 Обеспечение ресурсами

Ответственные за функционирование процесса менеджмента риска должны быть обеспечены необходимыми ресурсами.

5.1.1.5 Оценка процесса менеджмента риска

Организация должна описать процессы оценки и улучшения процесса менеджмента риска, а также способы изучения полученного опыта. Этот опыт должен быть учтен при внедрении процесса.

5.1.2 Управление профилем риска проекта

Целью деятельности по управлению профилем риска должно быть формирование текущих и хронологических данных о видах риска и способах их обработки, иметь которые необходимо причастным сторонам. Эти данные включают в себя текущее состояние и хронологию риска организации.

Управление профилем риска проекта должно быть проведено на всех этапах жизненного цикла программного обеспечения. Эта деятельность состоит из задач, перечисленных в 5.1.2.1—5.1.2.4.

5.1.2.1 Определение особенностей менеджмента риска

Организация должна определить и задокументировать особенности процесса менеджмента риска.

Определение особенностей менеджмента риска предусматривает следующее: описание одной или более причастной стороны, которая ведет сопровождение информации о действиях с риском; определение одной или более управляемой категории риска. Отдельно могут быть определены другие категории риска, такие как риски, связанные с защитой и безопасностью, имеющие особое значение для организации.

Примечание — Настоящий стандарт может быть использован совместно со стандартами IEEE 1228 [6], ИСО 14971, серий МЭК 60300 и МЭК 61508 для управления риском, связанным с безопасностью организации.

При определении особенностей менеджмента риска организация должна описать (или дать ссылку) технические и управленческие:

a) цели (например, ключевые технические, политические или экономические критерии выполнения требований проекта);

b) предположения (например, соображения, выходящие за пределы управления проектом);

c) ограничения (например, установленные границы проекта).

Организация должна описать любую другую необходимую информацию, которая может повлиять на анализ или обработку риска (например, возможно или нет в рамках проекта открытое предоставление информации, связанной с риском).

5.1.2.2 Установление допустимого риска

Организация должна определить и зарегистрировать допустимый риск, определяющий условия приемлемости риска.

Допустимый риск — наихудший риск, который считают приемлемым в соответствии с установленным критерием без дополнительного анализа и согласования с причастными сторонами. Допустимый риск должен быть определен для индивидуального риска или комбинации рисков. Организация должна установить допустимый риск для проекта в целом. Допустимый риск для систем и программного обеспечения должен быть определен исходя из уровней целостности системы в соответствии с ИСО/МЭК 15026. Допустимый риск может быть определен для таких характеристик, как стоимость, пла-

новые сроки выполнения работ, и других технических характеристик, подверженных влиянию опасного события.

Организация должна определить и зарегистрировать в статусе риска соответствующие меры, которые должны быть предприняты, если возникнет возможность превышения риском своего допустимого значения.

Примечание — Стандарт IEEE Std 1012 [7] содержит описание уровней целостности при планировании деятельности по валидации и верификации. ИСО/МЭК 15026 содержит описание уровней целостности систем и программного обеспечения. В МЭК 61508-5 приведены примеры методов определения безопасных уровней целостности. ИСО/МЭК 15939 описывает процесс измерений, позволяющий охарактеризовать и количественно определить риск.

5.1.2.3 Установление и поддержка профиля риска проекта

Организация должна установить и поддерживать в рабочем состоянии профиль риска проекта. Профиль риска проекта должен содержать информацию о совокупном риске проекта, профилях всех индивидуальных рисков, которые, в свою очередь, включают в себя текущее состояние и хронологию риска. Профиль риска проекта должен включать в себя (при необходимости список может быть дополнен):

a) особенности менеджмента риска;

b) хронологические записи о статусе каждого риска, в том числе вероятность появления опасного события, его последствия и допустимый риск;

c) приоритет каждого риска на основании критериев, представленных причастными сторонами;

d) информацию о действиях с риском, а также статус обработки риска.

Профиль риска должен содержать подробное описание каждого риска и причины опасного события, используемую шкалу оценок, необходимые измерения для оценки статуса риска, планы действий в случае непредвиденных обстоятельств и другую информацию, связанную с определением статуса риска.

Если произошли изменения в статусе индивидуального риска, организация должна актуализировать профиль риска проекта, например при изменениях в описании, экспозиции или обработке риска, изменениях особенностей менеджмента риска проекта или при выявлении нового риска. Для быстрого сбора данных, обмена информацией и ее оценки информация может быть представлена в электронном виде.

5.1.2.4 Обмен информацией о статусе риска

Обмен информацией о профиле риска проекта или уместном профиле риска (например, индивидуальном риске или комбинации рисков) между причастными сторонами в соответствии с их потребностями должен быть проведен через запланированные интервалы времени. Информация о статусе риска должна быть по возможности доступна всем причастным сторонам.

5.1.3 Анализ риска

Цели деятельности по анализу риска:

a) идентификация исходных событий, опасностей, угроз или ситуаций, которые могут вызвать риск;

b) оценка вероятности возникновения опасных событий и их последствий для каждого риска и среднего времени возникновения риска;

c) проверка каждого индивидуального риска или определенной комбинации рисков на соответствие допустимому риску, выбор альтернативных вариантов обработки риска в случае, когда значения риска выше допустимого риска, и представление рекомендаций для обработки риска на основе выбранных приоритетов.

Анализ риска должен проводиться непрерывно на всех стадиях жизненного цикла программного обеспечения.

Деятельность по анализу риска состоит из задач, перечисленных в 5.1.3.1—5.1.3.3.

5.1.3.1 Идентификация риска

Организация должна идентифицировать категории риска в соответствии с особенностями менеджмента риска. Должны также быть идентифицированы изменения менеджмента риска, например дополнительный риск, связанный с изменениями в используемых предположениях.

Организация должна использовать различные подходы к идентификации риска. Эти подходы могут предусматривать использование анкет по риску, систематизацию информации, мозговой штурм, анализ сценариев развития опасного события, изучение передового опыта, разработку макетов и другие. Повторный процесс идентификации может быть проведен на основе полученного опыта. По возможности, должны быть идентифицированы события, угрозы или ситуации, потенциально вызывающие

опасное событие, для помощи при обработке риска в будущем. Неидентифицированные риски неявно считают принятыми.

Организация должна использовать категории риска для эффективного обмена информацией между причастными сторонами. Связанные риски могут быть объединены для простоты анализа, мониторинга и обработки. Организация должна непрерывно анализировать ошибки системы и/или программного обеспечения, записи результатов измерений и другие показатели программного обеспечения как потенциальные источники возникновения риска.

Примечание — IEEE 1044 [8] содержит полезную информацию о классификации ошибок программного обеспечения. IEEE Std 982.1 [9] содержит полезную информацию о характеристиках надежности программного обеспечения. ИСО/МЭК 15939 описывает процесс измерений, позволяющий идентифицировать и охарактеризовать риск.

5.1.3.2 Количественная оценка риска

Организация должна оценивать вероятность возникновения и последствия каждого идентифицированного опасного события.

Оценки могут быть количественные или качественные. Причастные стороны должны выбрать методы количественной или качественной оценки каждого риска.

Организация должна последовательно использовать шкалу оценки вероятности возникновения опасного события и его последствий. В плане менеджмента риска должны быть приведены качественная и количественная характеристики неопределенности. В статусе риска должен быть указан уровень доверия оценок риска.

5.1.3.3 Проверка допустимости риска

Каждый риск должен быть проверен на соответствие его допустимому риску. Организация должна проверить индивидуальные риски, комбинации различных рисков и взаимодействие рисков с системными рисками и другими рисками предприятия. Общий риск проекта должен быть проверен на соответствие допустимому риску проекта. Это необходимо для обеспечения того, чтобы комбинация рисков, не превышающих свой допустимый уровень, не приводила к потере свойства безопасности проекта в целом. Организация может использовать различные методы для оценки риска, такие как дерево решений, разработка сценариев опасных событий, теория игр, вероятностный анализ и линейное программирование.

Риски должны быть ранжированы в соответствии с критериями, определяемыми причастными сторонами. Критериями ранжирования рисков могут быть временные характеристики риска, экспозиция риска, результаты измерений, связанных с риском, или другие критерии.

Организация должна исследовать различные альтернативные варианты обработки риска, необходимые для его снижения или устранения. Для каждого риска, превышающего свой допустимый уровень, должна быть определена и зарегистрирована в информации о действиях с риском рекомендованная стратегия обработки риска, такая как устранение риска, снижение вероятности возникновения соответствующего опасного события или серьезности его последствий, или принятие риска. Пример информации о действиях с риском приведен в приложении В. Организация должна разработать планы действий в критических обстоятельствах для всех рисков при превышении ими соответствующего допустимого риска. Организация должна определить необходимость оценки результативности альтернативных вариантов обработки риска. Причастные стороны должны быть информированы о риске, рекомендациях по его обработке и оценке результативности обработки риска для одобрения, отклонения или модификации.

Примечание — IEEE Std 982.1 [9] содержит информацию, которая может быть полезной при определении измерений, связанных с риском. МЭК 60300-3-9, МЭК 60812 и МЭК 61025 содержат методы, которые можно использовать при оценке риска. ИСО/МЭК 15939 описывает процесс измерений, который можно использовать при оценке риска.

5.1.4 Обработка риска

Целями деятельности по обработке риска являются:

a) определение допустимости риска для причастных сторон;

b) принятие необходимых мер и действий для снижения риска при превышении им допустимого уровня.

Обработка риска включает в себя выбор, планирование, мониторинг и управление действиями для снижения экспозиции риска.

Причастные стороны должны оценить необходимость обработки каждого риска, по которому произошло превышение допустимого уровня. Обработка риска, при необходимости, должна быть непрерывной.

5.1.4.1 Выбор обработки риска

Причастные стороны должны быть обеспечены данными о рекомендованных альтернативных методах обработки риска, указанных в информации о действиях с риском. Если в информации о действиях с риском рекомендован альтернативный вариант обработки риска, причастные стороны должны оценить приемлемость риска. Если причастные стороны принимают решение о выполнении действий, требуемых для достижения допустимого риска, то должен быть применен альтернативный вариант обработки риска, обеспечены необходимые ресурсы, проведен мониторинг, и эта деятельность должна быть скоординирована с другими действиями проекта.

Причастные стороны могут принять риск даже при превышении им допустимого риска, например, если стоимость обработки риска слишком высока, нарушены сроки выполнения работ или не хватает ресурсов для обработки риска. В этой ситуации риск считают более приоритетным и должен проводиться его непрерывный мониторинг для определения необходимости каких-либо действий по обработке риска в будущем.

При формировании информации о действиях с риском причастные стороны могут также запросить дополнительную информацию для принятия решения об обработке риска или могут предложить иной способ обработки риска. Если причастные стороны предложат альтернативные варианты обработки риска, которые не были отражены в информации о действиях с риском, то информация о действиях с риском должна быть возвращена на этап анализа риска для проведения анализа предложенных методов обработки. Информация о действиях с риском в этом случае должна быть снова представлена причастным сторонам для повторной оценки.

5.1.4.2 Планирование и выполнение обработки риска

Если настоящий стандарт применяют совместно с ИСО/МЭК 12207 или ИСО/МЭК 15288, то выполняют требования 5.1.4.2.1. В противном случае выполняют требования 5.1.4.2.2.

5.1.4.2.1 Обработка риска с использованием ИСО/МЭК 12207 или ИСО/МЭК 15288

Данный подпункт относится только к пользователям, которые применяют настоящий стандарт совместно с ИСО/МЭК 12207 или ИСО/МЭК 15288.

Если организация выбрала соответствующую обработку риска, деятельность со стороны руководства должна соответствовать требованиям ИСО/МЭК 12207, подпункт 7.1.3.3 или ИСО/МЭК 15288, подпункт 5.4.4.3.

5.1.4.2.2 Обработка риска без использования ИСО/МЭК 12207 или ИСО/МЭК 15288

Данный подпункт относится к пользователям, которые применяют настоящий стандарт независимо от ИСО/МЭК 12207 или ИСО/МЭК 15288.

Если принят альтернативный вариант обработки риска, причастные стороны должны определить детальный план обработки риска. Пример плана обработки риска представлен в приложении С. Организация должна установить методы внедрения обеспечения ресурсами, мониторинг исполнения и полученных результатов плана обработки риска. Организация должна назначить лиц, ответственных за выполнение каждой обработки риска.

План обработки риска должен быть внедрен и объединен с существующими планами проекта, процессами и действиями менеджмента.

Причастные стороны должны определить план действий в непредвиденных обстоятельствах в случае неудачи при обработке риска. Для некоторых рисков, которые считают приемлемыми, может быть необходим план действий в непредвиденных обстоятельствах.

5.1.5 Выполнение мониторинга риска

Цели деятельности по мониторингу риска:

a) анализ и актуализация индивидуального риска и особенностей менеджмента риска;

b) оценка результативности обработки риска;

c) поиск нового риска.

5.1.5.1 Мониторинг риска

Организация должна проводить мониторинг всех рисков, необходимый для внесения изменений в их статус с использованием соответствующих измерений, которые должны быть зарегистрированы в профиле риска проекта. Должен быть проведен мониторинг изменений особенностей менеджмента риска, которые должны быть задокументированы в профиле риска проекта. Мониторинг риска должен проводиться по приоритетам, основанным на критериях, установленных причастными сторонами (экспозиция риска, сроки выполнения работ и т. п.). Организация должна проводить частый мониторинг риска с высоким приоритетом. Если состояние риска изменилось, должна быть проведена оценка риска. Оценку следует проводить немедленно после выявления риска.

5.1.5.2 Мониторинг обработки риска

Организация должна выполнять оценку результативности обработки риска и проводить мониторинг этой оценки. Причина неэффективной обработки должна быть идентифицирована и быстро устранена. Причастные стороны должны установить критерии для определения момента времени, когда организация должна прекратить проведение мониторинга результативности обработки риска.

Примечание — ИСО/МЭК 15939 описывает процесс измерений, помогающий проводить мониторинг влияния обработки риска.

5.1.5.3 Выявление новых рисков

Организация должна проводить непрерывный мониторинг для выявления новых рисков системы на всех этапах жизненного цикла. Обмен информацией о новых рисках с причастными сторонами должен быть проведен после анализа риска.

5.1.6 Оценка процесса менеджмента риска

Целью деятельности по оценке процесса менеджмента риска является обеспечение обратной связи от причастных сторон. Эта деятельность предусматривает:

a) обеспечение качества процесса менеджмента риска;

b) определение областей улучшения процедуры, процесса или политики менеджмента риска;

c) идентификацию возможностей изменения процедуры, процесса или политики менеджмента риска на снижение или устранение системного риска.

Деятельность состоит из задач, перечисленных в 5.1.6.1—5.1.6.3.

5.1.6.1 Сбор информации о менеджменте риска

Для улучшения процесса менеджмента риска и изучения полученного опыта организация должна собирать информацию об идентифицированных рисках, их причинах, обработке и успехе выбранных способов обработки риска на всех этапах жизненного цикла программного обеспечения. Собранная информация может быть полезной для улучшения процедур, процессов или политики менеджмента риска организации. Информация может быть представлена в электронном виде для облегчения ее сбора, обмена и оценки.

5.1.6.2 Оценка и улучшение процесса менеджмента риска

Организация должна проводить анализ результативности и эффективности процесса менеджмента риска через запланированные интервалы времени. Возможности для улучшения проекта или системы менеджмента риска организации должны быть идентифицированы, включая рассмотрение того, как риски, описанные в процессе менеджмента риска, могут быть снижены или устранены. По возможности процесс необходимо улучшать, а политика, процесс, система и план менеджмента риска организации должны быть актуализированы. Причастные стороны должны определить периодичность анализа.

5.1.6.3 Изучение полученного опыта

Причастные стороны и другие заинтересованные стороны должны проводить анализ информации относительно идентифицированного риска, его обработки и результатов обработки через запланированные интервалы времени в целях идентификации системного риска проекта и организации. Организация может изучать опыт, полученный при работе по индивидуальным проектам. Результаты этой деятельности могут быть использованы при идентификации системных рисков. Причастные стороны должны определить периодичность анализа.

Приложение А
(справочное)

План менеджмента риска

А.1 Цель

Цель плана менеджмента риска состоит в определении способов внедрения и поддержки деятельности по менеджменту риска проекта. План менеджмента риска относится к основным выходным данным процесса планирования и служит механизмом внедрения менеджмента риска программного обеспечения. План менеджмента риска должен отвечать требованиям ИСО/МЭК 12207, подпункт 5.2.4.5, перечисление k); IEEE/EIA 12207.1 [10], подпункт 6.11.3, перечисление 1) и ИСО/МЭК 15288, подпункт 5.3.6.4, перечисление а), в соответствии с которыми информация о менеджменте риска должна быть включена в план менеджмента проекта или другие документы проекта. План менеджмента риска, приведенный в рамке ниже, также соответствует IEEE 1058, пункт 4.5.4 [4].

А.2 План менеджмента риска

Результатом процесса менеджмента риска является план менеджмента риска, который должен включать в себя разделы, представленные ниже. Если отсутствует информация, подходящая для раздела или параграфа, план менеджмента должен содержать следующую фразу «Параграф в настоящем плане не применяют» ниже раздела или заголовка параграфа вместе с указанием причины исключения. При необходимости может быть включена дополнительная информация. Часть плана менеджмента риска может быть приведена в других документах. В этом случае в плане должны быть приведены ссылки на эти документы.

Схема плана менеджмента риска:

1 Краткий обзор
1.1 Дата введения в действие и статус
1.2 Организация-разработчик
1.3 Подписи лиц, уполномоченных утверждать и согласовывать план
1.4 Данные об актуализации
2 Область применения
[Определение границ проекта и ограничений на риск]
3 Ссылочная документация
4 Термины и определения
5 Краткий обзор менеджмента риска
[Описание особенностей менеджмента риска для конкретного проекта или организации]
6 Политика менеджмента риска
[Описание основных принципов менеджмент риска]
7 Краткий обзор процесса менеджмента риска
8 Ответственность руководства в области менеджмента риска
[Определение сторон, ответственных за выполнение менеджмента риска]
9 Организация менеджмента риска
[Описание распределения ответственности за менеджмент риска в организации]
10 Координирование и обучение в области менеджмента риска
11 Затраты и план-график выполнения работ по менеджменту риска
12 Описание процесса менеджмента риска
[Если в организации установлен процесс менеджмента риска, используемый при разработке проекта или в конкретной ситуации, на него должна быть дана ссылка. Если процесс был соответствующим образом адаптирован, эта адаптация должна быть описана. Должны быть описаны процедуры, в соответствии с которыми осуществляется процесс менеджмента риска. Если в организации процесс менеджмента риска не установлен, должны быть описаны процесс и процедуры менеджмента риска, используемые для проекта или ситуации]
12.1 Особенности менеджмента риска
12.2 Анализ риска
12.3 Мониторинг риска
12.4 Обработка риска
[Должно быть приведено описание обработки риска. Если в организации установлен стандартный процесс менеджмента для работы с отклонениями или выявленными проблемами, необходимо использовать этот процесс и дать на него ссылки. Если в силу конкретных обстоятельств требуются специальные действия по обработке риска, следует описать эту деятельность]
13 Оценка процесса менеджмента риска
[Описание того, как в проекте или организации следует собирать и использовать информацию о мероприятиях для улучшения процесса менеджмента риска в проекте и/или организации]

13.1 Сбор информации о риске

13.2 Оценка процесса менеджмента риска

13.3 Изучение полученного опыта

14 Обмен информацией о риске

[Описание координации и обмена информацией о менеджменте риска между причастными сторонами и другими заинтересованными сторонами (например, заинтересованными в успешном выполнении проекта, но не работающими непосредственно в организации) таким путем, как, например, описание отчетов о рисках на соответствующих уровнях и в соответствующих подразделениях]

14.1 Документирование и отчетность по процессу менеджмента риска

14.2 Координирование менеджмента риска с причастными сторонами

14.3 Координирование менеджмента риска с заинтересованными сторонами

15 Хронология и процедуры изменения плана менеджмента риска

Приложение В
(справочное)

Информация о действиях с риском

В.1 Цель

Цель информации о действиях с риском состоит в обеспечении механизма сбора информации о риске и доведении ее до причастных сторон. Процесс менеджмента риска требует формирования информации о действиях с риском при превышении риском допустимого уровня.

В.2 Информация о действиях с риском

Результатом процесса менеджмента риска является информация о действиях с риском, которая должна включать в себя сведения, представленные ниже в заключенной в рамку схеме. Если отсутствует информация, подходящая для раздела или параграфа в пределах раздела, информация о действиях с риском должна содержать следующую фразу «Параграф не применяют в настоящем плане» ниже раздела или заголовка параграфа вместе с соответствующей причиной его исключения. При необходимости может быть включена дополнительная информация. Часть информации о действиях с риском может быть приведена в других документах. В этом случае в информации должны быть приведены ссылки на эти документы.

Схема информации о действиях с риском:

1 Дата формирования
2 Область применения
3 Предмет
4 Создатель информации
5 Особенности процесса менеджмента риска
[В первой информации о действиях с риском этот раздел может быть описан, а затем, если не произошли изменения, в последующих формах информации о действиях с риском достаточно привести ссылку на первую информацию]
5.1 Область применения процесса
5.2 Перспективы причастной стороны
5.3 Категории риска
5.4 Допустимые значения риска
5.5 Цели проекта
5.6 Предположения проекта
5.7 Ограничения проекта
6 Риски
[Раздел может охватывать по выбору пользователя один или несколько видов риска. Если вышеназванная информация относится к целому набору рисков, может быть достаточно разработать одну форму информации о действиях с риском. Если произошло изменение информации, каждая новая форма может включать в себя только новую или изменившуюся информацию]
6.1 Описание(я) риска(ов)
6.2 Вероятность опасного события
6.3 Последствия опасного события
6.4 Ожидаемое время возникновения опасного события
7 Альтернативные варианты обработки риска
7.1 Альтернативные описания
7.2 Рекомендованные альтернативные варианты
7.3 Обоснование
8 Управление информацией о действиях с риском
[Каждая форма информации должна содержать сведения о принятии, отклонении или изменении информации о действиях с риском и объяснение принятого решения]

Приложение С
(справочное)

План обработки риска

С.1 Цель

Основной целью плана обработки риска является определение способов обработки риска, признанного недопустимым. План обработки риска — это механизм выполнения выбранного рекомендованного метода обработки риска в информации о действиях с риском.

С.2 План обработки риска

После того как один из рекомендованных методов обработки, описанных в информации о действиях с риском, был выбран, должен быть разработан план обработки риска, включающий в себя разделы, приведенные в рамке ниже. Часть информации плана обработки риска может быть приведена в информации о действиях с риском. В этом случае информация о действиях с риском должна быть приведена в плане обработки риска. Если информация, подходящая для раздела или параграфа отсутствует, в плане обработки должна быть приведена фраза «Параграф не применяют в настоящем плане» ниже раздела или заголовка параграфа вместе с указанием причин исключения. При необходимости может быть включена дополнительная информация.

Чтобы исключить разработку индивидуальных планов обработки риска для каждого индивидуального риска, можно использовать общие планы обработки риска для рисков, имеющих схожие характеристики.

Схема плана обработки риска:

1 Краткий обзор
1.1 Дата выпуска и статус
1.2 Организация-разработчик
1.3 Подписи лиц, уполномоченных утверждать и согласовывать план
1.4 Данные об актуализации
2 Область применения
3 Ссылочные документы
4 Термины и определения
5 Запланированные действия и задачи обработки риска
[Организация должна описать особенности обработки риска, выбранной для одного риска или комбинации рисков, признанных недопустимыми. Должны быть описаны любые трудности, которые могут появиться при проведении обработки риска]
6 План обработки
7 Выделение ресурсов для обработки риска и их распределение
8 Ответственность и полномочия
[Организация должна назначить лиц, ответственных за выполнение обработки риска и описать их полномочия]
9 Контрольные измерения при обработке риска
[Организация должна определить мероприятия, необходимые для определения результативности обработки риска]
10 Стоимость обработки риска
11 Интерфейсы с заинтересованными сторонами
[Организация должна описать способы координации деятельности причастных сторон с планом владельца проекта, которая необходима для проведения обработки риска надлежащим образом]
12 Производственная среда и инфраструктура
[Организация должна описать требования к производственной среде и инфраструктуре и возможные воздействия на них, например безопасность и нарушение безопасности под воздействием опасного события]
13 Процедуры изменения плана обработки риска и хронология

Приложение D
(справочное)

Применение менеджмента риска в процессах жизненного цикла программного обеспечения

Настоящее приложение приводит ссылки на разделы, содержащие термин «риск» в ИСО/МЭК 12207 и во всех стандартах серии IEEE/EIA 12207. В подразделе D.1 дан перечень ссылок на ИСО/МЭК 12207, а в подразделе D.2 — на стандарты серии IEEE/EIA 12207.

В ИСО/МЭК 12207 и во всех стандартах серии IEEE/EIA 12207 применены понятия «риск» и «менеджмент риска». Фрагменты стандартов этой серии, имеющие отношение к «менеджменту риска», приведены ниже.

D.1 Применение менеджмента риска в стандартах серии ИСО/МЭК 12207

Во всех случаях в ИСО/МЭК 12207 применены понятия «риск» и «менеджмент риска». Фрагменты этих стандартов приведены и для удобства перефразированы.

D.1.1 Общие положения

ИСО/МЭК 12207:1995/Поправка 1 (приложения F, H) устанавливает информацию о менеджменте риска. Настоящий стандарт совместим с информацией, представленной в указанных приложениях.

[ИСО/МЭК 12207:1995/Поправка 1, приложения F, H]

D.1.2 Процесс закупки

При рассмотрении различных вариантов закупок (приобрести готовую продукцию, заказать разработку и т. д.) покупатель должен включать риск в критерии закупок.

[ИСО/МЭК 12207, подпункт 5.1.1.6]

План закупок должен содержать описание риска и методов менеджмента риска.

[ИСО/МЭК 12207, подпункт 5.1.1.8]

Целями процесса закупок являются обеспечение качества закупаемой продукции в соответствии с миссией, целями и задачами организации, а также создание основы для планирования всех видов деятельности, связанных с закупками в проекте. В качестве результата выступает успешное выполнение процесса: должны быть идентифицированы деловые риски, финансовые и технические последствия, а также последствия, связанные с ресурсами организации для различных вариантов принимаемых решений.

[ИСО/МЭК 12207:1995/Поправка 1, H.1.2, перечисление 5)]

D.1.3 Процесс поставки

Поставщик должен рассматривать варианты разработки программного продукта или предоставления услуг по программному обеспечению (разработанного, имеющегося в наличии и т. д.) в соответствии с анализом риска, связанным с каждым вариантом.

[ИСО/МЭК 12207, подпункт 5.2.4.4]

Поставщик должен разработать и задокументировать план управления проектом. Пункты плана должны включать в себя менеджмент риска, связанный с управлением областями проекта, в которых может возникнуть риск, влияющий на затраты, выполнение плана, а также на технические аспекты проекта.

[ИСО/МЭК 12207, подпункт 5.2.4.5, перечисление k)]

D.1.4 Процесс эксплуатации

В результате успешного внедрения процесса эксплуатации риски ввода в эксплуатацию и эксплуатации должны быть идентифицированы и должен быть проведен их мониторинг.

[ИСО/МЭК 12207:1995/Поправка 1, F.1.4.1 перечисление 1)]

D.1.5 Процесс верификации

Организация должна определить необходимость проведения верификации и степень независимости этой деятельности. Требования проекта должны быть проанализированы на критичность по отношению к рискам. Критичность может быть измерена в терминах зрелости и рисков проекта, связанных с используемыми методами программного обеспечения.

[ИСО/МЭК 12207, подпункт 6.4.1.1, перечисление b)]

D.1.6 Процесс объединенного анализа

Статус проекта должен быть оценен в соответствии с применяемыми планами, графиками, стандартами и руководящими принципами. Результаты анализа должны быть рассмотрены партнерами и должны быть использованы для оценки опасных событий и управления ими, которые могут влиять на успешность выполнения проекта.

[ИСО/МЭК 12207, подпункт 6.6.2.1, перечисление d)]

Менеджер должен подготовить планы выполнения процесса. Планы выполнения процесса должны содержать описание взаимосвязанных действий и задач и идентифицировать разрабатываемый программный продукт. Указанные планы должны предусматривать (но не ограничиваться) определение количественной оценки риска, связанного непосредственно с задачами или процессом.

[ИСО/МЭК 12207, подпункт 7.1.2.1, перечисление f)]

D.1.7 Процесс менеджмента

Процесс менеджмента включает в себя цели и выходы следующих подпроцессов… Менеджмент риска…

[ИСО/МЭК 12207:1995/Поправка 1, F.3.1]

Цель менеджмента риска состоит в непрерывной идентификации риска, управлении им и снижении риска на уровне проектов или организации в целом. Результатами успешного внедрения менеджмента риска являются:

1) определение области применения менеджмента риска проекта;

2) определение и внедрение стратегий менеджмента риска;

3) идентификация рисков в стратегии менеджмента риска проекта и наблюдение риска проекта на всех стадиях жизненного цикла проекта;

4) анализ риска и определение его приоритетности для выделения необходимых ресурсов для мониторинга этого риска;

5) выбор методов мониторинга риска для определения изменений в статусе риска и выполнения действий по мониторингу;

6) выполнение корректирующих и предупреждающих действий, направленных на устранение риска.

[ИСО/МЭК 12207:1995/Поправка 1, F.3.1.5]

Цель менеджмента риска состоит в непрерывном проведении идентификации, анализа, обработки и мониторинга риска. Результатами успешного внедрения менеджмента риска являются:

1) определение области применения менеджмента риска проекта;

2) определение и внедрение стратегий менеджмента риска;

3) идентификация рисков в стратегии менеджмента риска проекта и наблюдение риска проекта на всех стадиях жизненного цикла проекта;

4) анализ риска и определение его приоритетности для выделения необходимых ресурсов для мониторинга этого риска;

5) определение, применение и оценка системы показателей риска для измерения изменений в состоянии риска и продвижения в его снижении;

6) выполнение корректирующих и предупреждающих действий, направленных на устранение риска на основе приоритетности, вероятности и последствии или другом определенном допустимом риске.

[ИСО/МЭК 12207:1995/Поправка 2, F.3.1.5]

D.1.8 Процесс адаптации

Риск — фактор, который должен быть рассмотрен при адаптации стандарта.

[ИСО/МЭК 12207, приложение А]

D.1.9 Сопровождение процессов жизненного цикла

Специалист по оптимизации процессов в сотрудничестве с разработчиком должен оценить риск для причастных сторон и пользователей.

[ИСО/МЭК 12207:1995/Поправка 1, G.1.1 и 6.9.2.2, перечисление d)]

D.1.10 Потребность в финансовых ресурсах

Цель процесса определения потребностей в финансовых ресурсах состоит в установлении требований к инфраструктуре для эффективного финансового менеджмента процессом закупок. Результатом успешного выполнения процесса является установление финансового менеджмента, риска и затрат на процесс закупок.

[ИСО/МЭК 12207:1995/Поправка 1, Н.1.6, перечисление 1)]

D.1.11 Требования к проекту

Целью процесса установления требований к проекту является обеспечение закупок по проекту и связанными с этим адекватным планированием, укомплектованием персоналом, руководством, организацией и контролем над задачами и действиями проекта. В результате успешного выполнения процесса будут идентифицированы риски, связанные с жизненным циклом проекта и поставщиками.

[ИСО/МЭК 12207:1995/Поправка 1, Н.1.7, перечисление 6)]

D.1.12 Согласование контракта

Цель процесса согласования контракта состоит в обсуждении и одобрении контракта/соглашения, в котором ясно и однозначно должны быть определены ожидания и обязанности сторон, поставляемая продукция, условия поставки и обязанности поставщика(ов) и покупателя. Результатами успешного выполнения процесса являются рассмотрение и анализ механизмов мониторинга возможностей поставщика(ов) и выполнения ими работ, а также снижение идентифицированных рисков, необходимые для дальнейшего включения этих вопросов в условия контракта.

[ИСО/МЭК 12207:1995/Поправка 1, Н.1.11, перечисление 2)]

D.1.13 Взаимоотношения с поставщиками

Цель процесса взаимоотношений с поставщиками состоит в улучшении сотрудничества покупатель — поставщик в вопросах качества обслуживания и соотношения цены и качества; это необходимо для лучшего понимания потребностей обеих сторон. В результате успешного выполнения процесса будут идентифицированы потенциальные выгоды от улучшения взаимоотношений и неизменный взаимный риск.

[ИСО/МЭК 12207:1995/Поправка 1, Н.1.15, перечисление 4)]

Частью политики менеджмента взаимоотношений с поставщиками является идентификация потенциальных выгод от улучшения взаимоотношений и неизменного взаимного риска.

[ИСО/МЭК 12207:1995/Поправка 1, Н.2.1.3, 5.1.8.3, перечисление с)]

D.1.14 Взаимоотношения с пользователями

Цель процесса взаимоотношений с пользователями состоит в улучшении сотрудничества покупатель — пользователь в вопросах качества обслуживания и соотношения цены и качества; это необходимо для лучшего понимания потребностей обеих сторон. В результате успешного выполнения процесса будут идентифицированы потенциальные выгоды от улучшения взаимоотношений и неизменный взаимный риск.

[ИСО/МЭК 12207:1995/Поправка 1, Н.1.15, перечисление 3)]

Частью политики менеджмента взаимоотношений с пользователями является идентификация потенциальных выгод от улучшения взаимоотношений и неизменного взаимного риска.

[ИСО/МЭК 12207:1995/Поправка 1, Н.2.1.4, 5.1.9.2, перечисление с)]

D.2 Применение менеджмента риска в IEEE/EIA серии 12207

Во всех ссылках на риск в IEEE/EIA 12207 (см. [1], [10] и [11]) применены понятия «риск» и «менеджмент риска». Фрагменты этих стандартов приведены и перефразированы для удобства.

D.2.1 Общие положения

IEEE/EIA 12207.2 [11], приложение L устанавливает информацию о менеджменте риска. Настоящий стандарт совместим с информацией, представленной в указанном приложении.

Менеджмент данных по стадиям жизненного цикла должен учитывать требования, связанные с данными об управленческих и технических рисках.

[IEEE/EIA 12207.1 [10], пункт 4.2.4]

Любой план должен включать в себя информацию о рисках или содержать ссылку на нее.

[IEEE/EIA 12207.1 [10], пункт 5.2.2]

D.2.2 Процесс закупки

При рассмотрении различных вариантов закупок (приобрести готовую продукцию, заказать разработку и т. д.) покупатель должен включать риск в критерии закупок.

[IEEE/EIA 12207.0 [1], подпункт 5.1.1.6]

План закупок должен содержать описание риска и методов менеджмента риска.

[IEEE/EIA 12207.0 [1], подпункт 5.1.1.8]

План закупок должен устанавливать программу измерений, связанных с программным обеспечением, которое, кроме других целей, помогает организации в управлении затратами, выполнением графика работ и техническим риском.

[IEEE/EIA 12207.2 [11], подпункт 5.1.1.8]

План закупок должен включать в себя риски, рассматриваемые вместе с методами их управления.

[IEEE/EIA 12207.1 [10], пункт 6.1.3]

Исследование воздействий изменений контракта должно охватывать все возможные существующие риски.

[IEEE/EIA 12207.2 [11], подпункт 5.1.3.5]

Должны быть установлены способы взаимовыгодных отношений и сотрудничества между покупателем и поставщиком, предусматривающие обеспечение необходимой информацией, позволяющей решать возникающие проблемы и добиваться снижения риска.

[IEEE/EIA 12207.2 [11], подпункт 5.1.4.2]

D.2.3 Процесс поставки

Поставщик должен рассматривать варианты разработки программного продукта или предоставления услуг по программному обеспечению (разработанного, имеющегося в наличии и т. д.) в соответствии с анализом риска, связанным с каждым вариантом.

[IEEE/EIA 12207.0 [1], подпункт 5.2.4.4]

Поставщик должен разработать и задокументировать план управления проектом. Пункты плана должны включать в себя менеджмент риска, связанный с управлением областями проекта, в которых может возникнуть риск, влияющий на затраты, выполнение плана, а также на технические требования.

[IEEE/EIA 12207.0 [1], подпункт 5.2.4.5 перечисление k)]

IEEE/EIA 12207.2 [11], подпункт 5.2.4.5 и приложение L описывают информацию о менеджменте риска.

План управления проектом должен включать в себя менеджмент риска.

[IEEE/EIA 12207.1 [10], пункт 6.11.3]

При проведении поставщиком мониторинга на всех стадиях жизненного цикла договора рекомендуется использовать менеджмент риска.

[IEEE/EIA 12207.2 [11], подпункт 5.2.5.3, перечисление а)]

D.2.4 Процесс разработки

При планировании разработки должны быть описаны действия (методы/процедуры/ инструменты) и задачи процесса разработки, которые должны охватывать все применимые пункты разработки и идентифицировать соответствующие риски и неопределенность.

[IEEE/EIA 12207.2 [11], подпункт 5.3.1.4]

Пример процесса анализа риска для определения стратегии разработки представлен на рисунке 1.2 IEEE/EIA 12207.2 [11].

Системные технические требования должны устанавливать ограничения на компьютерные ресурсы, совместимые «со степенью идентифицированного риска».

[IEEE/EIA 12207.1 [10], подпункт 6.2.6.3]

D.2.5 Процесс эксплуатации

Цели процесса эксплуатации включают в себя идентификацию и снижение эксплуатационного риска.

[IEEE/EIA 12207.0 [1] G.11, перечисление a)]

D.2.6 Процесс верификации

Организация должна определить необходимость проведения верификации и степень независимости этой деятельности. Требования проекта должны быть проанализированы на критичность по отношению к рискам. Критичность может быть измерена в терминах зрелости и рисков проекта, связанных с используемыми методами программного обеспечения.

[IEEE/EIA 12207.0 [1], подпункт 6.4.1.1, перечисление b)]

D.2.7 Процесс объединенного анализа

Пункты о риске должны быть включены в совместный анализ.

[IEEE/EIA 12207.2 [11], подпункт 6.6.1.3]

Статус проекта должен быть оценен в соответствии с применяемыми планами, графиками, стандартами и руководящими принципами. Результаты анализа должны быть рассмотрены партнерами и использованы для оценки опасных событий, которые могут влиять на успешность выполнения проекта и управления им.

[IEEE/EIA 12207.0 [1], подпункт 6.6.2.1, перечисление d)]

В дополнение к анализу, предусмотренному контрактом (см. IEEE/EIA 12207.1 [10], подпункт 5.1.2.3 и IEEE/EIA 12207.2 [11], подпункт 5.2.4.5), поставщик, включая разработчика, обслуживающий персонал или оператора, может предложить проведение дополнительного совместного анализа вместе с анализом со стороны руководства. Поставщик и другие заинтересованные стороны должны планировать проведение такого дополнительного анализа и принимать участие в нем. Место и срок проведения анализа должны быть предложены поставщиком и одобрены покупателем. Варианты совместного анализа указаны в приложении G IEEE/EIA 12207.2 [11]. Такой анализ должны проводить лица, обладающие полномочиями для принятия решений по стоимости и графику выполнения работ. Целями анализа могут быть: разработка согласованной стратегии снижения риска в краткосрочный и долгосрочный периоды, которая не была ранее определена в совместном техническом анализе, а также идентификация и принятие решения соответствующим подразделением на соответствующем уровне по спорным вопросам и риску, не рассмотренным в совместном техническом анализе.

[IEEE/EIA 12207.2 [11], подпункт 6.6.2.1, перечисления c) и d)]

Поставщик, включая разработчика и/или обслуживающий персонал и/или оператора, должен планировать проведение совместного технического анализа, место и дату которого предложил поставщик и одобрил покупатель. Этот анализ должны проводить лица, имеющие необходимые знания для анализа программных продуктов. Данные вспомогательных процессов (например, обеспечение качества, управление конфигурацией, верификация, валидация) должны быть использованы в качестве входных данных или учтены при совместном анализе, а сами вспомогательные процессы могут быть объектами исследования в совместном анализе. Анализу должны быть подвергнуты незавершенный программный продукт, находящийся в работе, и заключительные версии программного продукта, но не материалы, подготовленные специально для анализа. Анализ может преследовать такие цели, как достижение согласованной стратегии снижения идентифицированных рисков в пределах установленных полномочий и идентификацию риска и спорных вопросов, которые должны быть рассмотрены в совместном анализе вместе с руководством.

[IEEE/EIA 12207.2 [11], подпункт 6.6.3.1, перечисления c) и d)]

D.2.8 Процесс решения проблемы

В соответствии с рисунком J.2) IEEE/EIA 12207.2 [11] характер воздействия на риск является признаком классификации отчетов об исследовании соответствующих задач.

D.2.9 Процесс менеджмента

Цели процесса менеджмента следующие:

k) определение области применения менеджмента риска проекта;

l) идентификация рисков проекта;

m) анализ риска и определение его приоритетности в целях выделения необходимых ресурсов для снижения этого риска;

n) определение, внедрение и оценка соответствующих стратегий снижения риска;

o) определение, применение и оценка системы показателей риска для измерения изменений в состоянии риска и продвижения в его снижении.

[IEEE/EIA 12207.0 [1] G.10]

Руководитель должен подготовить планы выполнения процесса. Эти планы должны содержать описание действий и задач поставляемого программного продукта. Планы должны включать в себя количественную характеристику рисков, связанных с задачами или процессом.

[IEEE/EIA 12207.0 [1], подпункт 7.1.2.1]

D.2.10 Процесс адаптации

Риск — фактор, который должен быть рассмотрен при адаптации стандарта.

[IEEE/EIA 12207.0 [1], приложение А]

D.2.11 Разное

Примерами возможных критериев оценки многократного использования программного продукта являются технические риски, риски, связанные с затратами, выполнением графика работ и наличием альтернативных вариантов использования программного продукта.

[IEEE/EIA 12207.2 [11] F.2, перечисление i)]

При определении требований, относящихся к оценке программного обеспечения, должны быть рассмотрены соответствующие задачи риска и неопределенности.

[IEEE/EIA 12207.2 [11] H.1]

Приложение Е
(справочное)

Краткое содержание ссылочных стандартов

Стандарт GEIA EIA-632 [12] содержит требования к процессу разработки систем. Он предусматривает применение процесса менеджмента риска для снижения влияния неопределенных событий, которые могут привести к изменениям в качестве, стоимости, графике производства или технических характеристиках систем.

Стандарт AS/NZS 4360 [5] устанавливает общую структуру для определения и реализации системы менеджмента риска организации и направлен на повышение безопасности и качества выполнения работ организации. Требования стандарта дополняют требования IEEE Std 1540 [13].

Британский стандарт BS 6079-3 [14] по менеджменту содержит руководство по управлению коммерческой деятельностью с учетом соответствующего риска. Стандарт применим к широкому спектру проектов, работающих в промышленных, коммерческих и общественных секторах. Стандарт описывает спонсоров и/или менеджеров проектов, ответственных обычно за один или несколько проектов различных типов и размеров. Стандарт предназначен для применения в соответствии с обстоятельствами и потребностями организации.

Канадское руководство Q850-97-CAN/CSA [15] разработано в помощь персоналу, связанному с принятием решений в области риска. Руководство поможет более эффективно управлять риском всех видов, включая вред или ущерб, нанесенный здоровью, собственности, окружающей среде. Это руководство описывает процесс получения, анализа, оценки информации и обмена ею для принятия решений. Руководство содержит описание главных компонентов процесса принятия решений в области управления риском и их взаимоотношений в пошаговом процессе.

Стандарт МЭК 60300-1 содержит информацию об обеспечении надежности, в частности обеспечении безотказности и ремонтопригодности продукции, а также устанавливает требования к выполнению технического обслуживания потребителем (и/или поставщиком).

Стандарт МЭК 60300-2 предлагает различные методы, которые могут быть полезны в понимании рисков, связанных с продукцией, и быть использованы при анализе, прогнозировании или проектировании, где необходимо обеспечение надежности.

Стандарт МЭК 60300-3-9 устанавливает руководящие указания для выбора и использования методов анализа риска, которые могут быть полезными при определении методов, применяемых для выполнения общего анализа риска.

Стандарт МЭК 60812 содержит руководство по выполнению метода анализа видов и последствий отказов (FMEA) и метода анализа видов, последствий и критичности отказов (FMECA). Этот материал важен при анализе безопасности или другом исследовании риска.

Стандарт МЭК 61025 содержит всестороннее описание метода анализа дерева неисправностей (FTA). Этот материал важен при анализе безопасности или другом исследовании риска.

Стандарт МЭК 61508-1 предлагает общий подход для всех действий жизненного цикла систем безопасности, состоящих из электрических и/или электронных и/или программируемых электронных компонентов [электрические/электронные/программируемые электронные системы (E/E/PESs)], необходимых для обеспечения функции безопасности.

Стандарт МЭК 61508-2 определяет способы усовершенствования информации, полученной в соответствии с МЭК 61508-1, за исключением устройств, использующих программное обеспечение, определенное в МЭК 61508-3.

Стандарт МЭК 61508-3 охватывает любое программное обеспечение, которое является частью системы, связанной с безопасностью, или используется для разработки системы безопасности на основе МЭК 61508-1 и МЭК 61508-2. МЭК 61508-3 содержит материал, который может быть полезен при рассмотрении риска в области программного обеспечения, связанного с продукцией.

Стандарт МЭК 61508-4 содержит определения терминов, используемых в стандартах серии МЭК 61508.

Стандарт МЭК 61508-5 содержит много полезных примеров определения уровней целостности безопасности. Перечень уровней целостности может быть использован при анализе риска, при определении приемлемости или допустимых уровней риска.

Стандарт МЭК 61508-6 содержит руководящие указания по применению МЭК 61508-2 и МЭК 61508-3.

Стандарт МЭК 61508-7 содержит краткий обзор различных методов и средств, используемых при определении функциональной безопасности систем и предпринимаемых мер, уместных при применении МЭК 61508-2 и МЭК 61508-3.

Стандарт МЭК 61713 идентифицирует виды деятельности, связанной с процессами жизненного цикла программного обеспечения, которые помогут в достижении надежности программного обеспечения (т. е. выполнении программным обеспечением установленных функций). Материал этого стандарта может быть полезным в идентификации источников риска.

МЭК 62198 устанавливает процесс менеджмента риска. Стандарт разработан в помощь персоналу, ответственному за принятие решений, включая менеджеров проектов, менеджеров риска и коммерческих директоров.

IEEE 100 [2] — авторитетный словарь терминов стандартов IEEE.

Некоторые из методов измерений надежности программного обеспечения, описанных в стандартах IEEE Std 982.1 [9] и IEEE Std 982.2 [16], могут быть применены в области менеджмента риска.

Стандарт IEEE Std 1012 [7] использует уровни целостности для определения соответствующих действий по верификации и валидации. Целесообразно определение этих уровней целостности в базовой модели риска.

Требования к риску, установленные в стандарте IEEE 1044 [8], могут быть полезными при классификации возможных отклонений.

Стандарт IEEE 1058 [4], относящийся к планированию менеджмента проекта программного обеспечения, содержит структуру IEEE/EIA 12207.1 [10]. Он устанавливает требования к разработке спецификаций к плану менеджмента риска относительно идентификации, анализа и расположения по приоритетам факторов риска проекта так же, как процедур для планирования действий в случае непредвиденных обстоятельств, мониторинга риска и изменения статуса риска.

Стандарт IEEE 1220 [17] описывает действия по управлению процессами разработки систем, а также считает необходимой интеграцию требований менеджмента риска в общую систему менеджмента.

Стандарт IEEE 1228 [6] содержит материал, полезный в менеджменте программного обеспечения, являющегося частью системы безопасности.

Цель документа IEEE 1490 [18] состоит в идентификации и описании общепринятой совокупности знаний по управлению проектами. «Общепринятый» означает, что знания и описанные методы применимы к большинству проектов и признаны ценными и исчерпывающими. Это не означает, что одни и те же знания и методы должны быть применены ко всем проектам без рассмотрения их пригодности в конкретной ситуации. Стандарт содержит специальный раздел по управлению базой знаний в менеджменте проекта.

Стандарт IEEE/EIA 12207.1 [10] содержит единицы информации для записи данных производственных процессов IEEE/EIA 12207.0 [1].

Стандарт IEEE/EIA 12207.2 [11] содержит дополнительное руководство для IEEE/EIA 12207.0 [1].

Стандарт ИСО 3534-1 определяет 204 термина в области теории вероятности и общей статистики. Стандарт устанавливает основные положения и словарь, используемые в стандартах серии ИСО 9000 на системы менеджмента качества.

ИСО 10006 содержит руководство по применению менеджмента качества в проектах. Стандарт не является «руководством по выполнению проекта», а скорее представляет собой руководство по качеству в процессе управления проектом.

ИСО 14971 содержит материалы по применению менеджмента риска для медицинских устройств с учетом требований безопасности.

ИСО/МЭК Руководство 51 предоставляет разработчикам стандартов руководящие указания для включения требований безопасности в стандарты. Стандарт применим к любым требованиям безопасности, связанным с безопасностью для людей, собственности, окружающей среды или их комбинации (например, только люди; люди и собственность; люди, собственность и окружающая среда).

Терминология, используемая в настоящем стандарте, совместима со словарем, установленным в ИСО/МЭК, Руководство 73.

ИСО/МЭК ТО 19760 содержит в таблице С.12 «Процесс менеджмента риска» руководство по выполнению процесса менеджмента риска в соответствии с ИСО/МЭК 15288. Дополнительно имеются несколько других ссылок для использования менеджмента риска в различных процессах.

ИСО/МЭК 12207 устанавливает действия и задачи для 17 процессов, вовлеченных в жизненный цикл программного продукта или услуги. Две поправки устанавливают цели и критерии результативности для большего числа процессов.

ИСО/МЭК 15026 устанавливает основные положения, связанные с уровнями целостности, в том числе определяет уровни целостности объекта, необходимые для технического обслуживания системы, обеспечивающей риск в рамках допустимых пределов. Стандарт устанавливает требования к процессам определения уровней целостности, а также целостности программного обеспечения. Положения стандарта могут быть полезны при определении приемлемости или допустимости риска.

Требования ИСО/МЭК 15288 в области менеджмента риска направлены на снижение влияния неопределенных событий, которые могут привести к изменениям в качестве, стоимости, графике производства или технических характеристиках продукции.

ИСО/МЭК 15939 определяет возможность применения процесса измерений в различных областях менеджмента. Процесс измерений, определенный в ИСО/МЭК 15939, совместно с действиями и задачами менеджмента риска, определенными в настоящем стандарте, позволяет охарактеризовать риск и определить его количественную оценку.

Японский промышленный стандарт JIS Q 2001 [19] устанавливает основные принципы и элементы системы менеджмента риска, применимые для любых типов организаций и любых видов риска. Этот стандарт не предназначен для использования при оценке соответствия.

Приложение F
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица F.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК Руководство 51:1999	ГОСТ Р 51898—2002 Аспекты безопасности. Правила включения в стандарты
ИСО/МЭК Руководство 73:2002	ГОСТ Р 51897—2002 Менеджмент риска. Термины и определения
ИСО 3534-1:2006	ГОСТ Р 50779.10—2000 (ИСО 3534-1—93) Статистические методы. Вероятность и основы статистики. Термины и определения
ИСО 10006:2003	ГОСТ Р ИСО 10006—2005 Системы менеджмента качества. Руководство по менеджменту качества при проектировании
ИСО/МЭК 12207:1995	ГОСТ Р ИСО/МЭК 12207—99 Информационная технология. Процессы жизненного цикла программных средств
ИСО/МЭК 12207:1995/ Поправка 1:2002	*
ИСО/МЭК 12207:1995/ Поправка 2:2004	*
ИСО 14971:2007	ГОСТ Р ИСО 14971—2006 Изделия медицинские. Применение менеджмента риска к медицинским изделиям
ИСО/МЭК 15026:1998	ГОСТ Р ИСО/МЭК 15026—2002 Информационная технология. Уровни целостности систем и программных средств
ИСО/МЭК 15288:2002	ГОСТ Р ИСО/МЭК 15288—2005 Информационная технология. Системная инженерия. Процессы жизненного цикла систем
ИСО/МЭК 15939:2007	*
ИСО/МЭК ТО 19760:2003	*
МЭК 60300-1:2003	ГОСТ Р 51901.2—2005 (МЭК 60300-1:2003) Менеджмент риска. Системы менеджмента надежности
МЭК 60300-2:2004	ГОСТ Р 51901.3—2007 (МЭК 60300-2:2004) Менеджмент риска. Руководство по менеджменту надежности
МЭК 60300-3-9:1995	ГОСТ Р 51901.1—2002 Менеджмент риска. Анализ риска технологических систем
МЭК 60812:2006	ГОСТ Р 51901.12—2007 (МЭК 60812:2006) Менеджмент риска. Метод анализа видов и последствий отказов
МЭК 61025:2006	ГОСТ Р 51901.13—2005 (МЭК 61025:1990) Менеджмент риска. Анализ дерева неисправностей
МЭК 61508-1:1998	ГОСТ Р МЭК 61508-1—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

Окончание таблицы F.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
МЭК 61508-2:2000	ГОСТ Р МЭК 61508-2—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам
МЭК 61508-3:1998	ГОСТ Р МЭК 61508-3—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению
МЭК 61508-4:1998	ГОСТ Р МЭК 61508-4—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения
МЭК 61508-5:1998	ГОСТ Р МЭК 61508-5—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности
МЭК 61508-6:2000	ГОСТ Р МЭК 61508-6—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2—2007 и ГОСТ Р МЭК 61508-3—2007
МЭК 61508-7:2000	ГОСТ Р МЭК 61508-7—2007 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства
МЭК 61713:2000	*
МЭК 62198:2001	ГОСТ Р 51901.4—2005 (МЭК 62198:2001) Менеджмент риска. Руководство по применению при проектировании
* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.	

Библиография

[1] IEEE[1)]/EIA 12207.0—1996 Стандарт IEEE/EIA. Промышленное применение международного стандарта ИСО/МЭК 12207:1995 «Информационные технологии. Процессы жизненного цикла программного обеспечения»
(IEEE/EIA Standard Industry Implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207) Standard for Information Technology Software Life Cycle Processes)

[2] IEEE 100—2000 Авторитетный словарь терминов стандартов IEEE
(The Authoritative Dictionary of IEEE Standards Terms)

[3] IEEE 610.12—1990 Глоссарий стандартов IEEE. Термины и определения по программному обеспечению
(IEEE standard glossary of software engineering terminology)

[4] IEEE 1058—1998 Стандарт IEEE по планам менеджмента проекта программного обеспечения. Содержит структуру IEEE/EIA 12207.1
(IEEE standard for software project management plans)

[5] AS/NZS 4360:2004 Risk management

[6] IEEE 1228—1994 Стандарт IEEE по планам безопасности программного обеспечения.
(IEEE standard for software safety plans)

[7] IEEE Std 1012—2004 Стандарт IEEE по планам верификации и валидации программного обеспечения
(IEEE Standard for Software Verification and Validation)
IEEE 1012—1998 использует уровни целостности для определения соответствующих действий по верификации и валидации. Целесообразно определение этих уровней целостности в базовой модели риска

[8] IEEE 1044—1993 Классификация ошибок программного обеспечения для стандартов серии IEEE
(IEEE standard classification for software anomalies)
Аспекты риска могут быть полезными при классификации ошибок

[9] IEEE Std 982.1—2005 Словарь стандарта IEEE по измерениям надежности программного обеспечения
(IEEE Standard Dictionary of Measures of the Software Aspects of Dependability)

[10] IEEE/EIA 12207.1—1997 Стандарт IEEE/EIA. Промышленное внедрение международного стандарта ИСО/МЭК 12207:1995 «Информационные технологии. Процессы жизненного цикла. Данные жизненного цикла»
(IEEE/EIA Standard Industry implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207) Standard for information technology — Software life cycle processes — Life cycle data)

[11] IEEE/EIA 12207.2—1997 Стандарт IEEE/EIA. Промышленное внедрение международного стандарта ИСО/МЭК 12207:1995 «Информационные технологии. Процессы жизненного цикла. Аспекты внедрения»
(IEEE/EIA Standard Industry implementation of International Standard ISO/IEC 12207:1995 (ISO/IEC 12207 Standard for information technology — Software lifecycle processes — Implementation considerations)

[12] GEIA EIA-632 1999 Processes for Engineering a System

[13] IEEE Std 1540—2001 IEEE Standard for Software Life Cycle Processes—Risk Management-Description

[14] BS 6079-3:2000 Управление предприятием. Часть 3. Руководство по управлению коммерческой деятельностью с точки зрения риска
BS 6079-3:2000 (Project management. Guide to the management of business related project risk)

[15] Q850-97-CAN/CSA Risk Management: Guideline for Decision-Makers

[16] IEEE Std 982.2—1988 Руководство IEEE по применению словаря стандарта IEEE по измерениям надежности программного обеспечения
(IEEE guide for the use of IEEE standard dictionary of measures to produce reliable software)

[17] IEEE 1220—2005 IEEE Standard for Application and Management of the Systems Engineering Process

[18] IEEE 1490—2003 IEEE Guide Adoption of PMI Standard — A Guide to the Project Management Body of Knowledge

[19] JIS Q 2001—2001 Рекомендации по разработке и внедрению системы менеджмента рисков
(Guidelines for development and implementation of risk management system)

[1)] Публикации IEEE разработаны Американским институтом инженеров по электротехнике и электронике.

УДК 658:562.014:006.354 ОКС 35.180 Т59

Ключевые слова: приемлемость, целостность, риск, анализ степени риска, менеджмент риска, обработка риска, менеджмент риска программного обеспечения

Редактор *Л.В. Афанасенко*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 25.09.2008. Подписано в печать 28.10.2008. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 3,72. Уч.-изд. л. 3,20. Тираж 303 экз. Зак. 1243.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.