ГОСТ Р 50267.0.4—99
(МЭК 60601-1-4—96)

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Изделия медицинские электрические

Часть 1

ОБЩИЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

4. Требования безопасности к программируемым медицинским электронным системам

Издание официальное

БЗ 12—99/686

ГОССТАНДАРТ РОССИИ
Москва

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Всероссийским научно-исследовательским и испытательным институтом медицинской техники (ВНИИИМТ)

ВНЕСЕН Техническим комитетом по стандартизации ТК 11 «Медицинские приборы и аппараты»

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 29 декабря 1999 г. № 855-ст

3 Настоящий стандарт, за исключением примечаний к пунктам 52.204.3.1.6 и 52.208.2, представляет собой аутентичный текст международного стандарта МЭК 60601-1-4—96 «Изделия медицинские электрические. Часть 1. Общие требования безопасности. 4. Требования безопасности к программируемым медицинским электронным системам»

4 ВВЕДЕН ВПЕРВЫЕ

© ИПК Издательство стандартов, 2000

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта России

Содержание

РАЗДЕЛ ПЕРВЫЙ. ОБЩИЕ ПОЛОЖЕНИЯ . . . 1
1 Область распространения и цель . . . 1
1.201 Область распространения . . . 1
1.202 Цель . . . 1
1.203 Связь с другими стандартами . . . 1
2 Термины и определения . . . 2
2.201 Используемые термины . . . 2
2.202 Терминология . . . 3
6 Идентификация, маркировка и документация . . . 3
6.8 ЭКСПЛУАТАЦИОННЫЕ ДОКУМЕНТЫ . . . 3
РАЗДЕЛ ДЕВЯТЫЙ. НЕНОРМАЛЬНАЯ РАБОТА И УСЛОВИЯ НАРУШЕНИЯ; ИСПЫТАНИЯ НА ВОЗДЕЙСТВИЕ ВНЕШНИХ ФАКТОРОВ . . . 3
52 Ненормальная работа и условия нарушения . . . 3
52.201 Документация . . . 3
52.202 План управления РИСКОМ . . . 4
52.203 ЦИКЛ РАЗРАБОТКИ . . . 4
52.204 Процесс управления РИСКОМ . . . 5
52.205 Квалификация персонала . . . 6
52.206 Техническое задание . . . 6
52.207 Архитектура . . . 6
52.208 Конструкция и выполнение требований . . . 7
52.209 ТЕХНИЧЕСКИЙ КОНТРОЛЬ . . . 7
52.210 СООТВЕТСТВИЕ . . . 7
52.211 Модификация . . . 7
52.212 Оценка . . . 7
Приложение AAA Алфавитный указатель терминов . . . 8
Приложение BBB Обоснование . . . 8
Приложение CCC Понятия РИСКА . . . 9
Приложение DDD Модель ЦИКЛА РАЗРАБОТКИ . . . 13
Приложение EEE Примеры структур ПМЭС/ПЭПС . . . 15
Приложение FFF Библиография . . . 16

Введение

Настоящий стандарт является прямым применением международного стандарта МЭК 60601-1-4—96 «Изделия медицинские электрические. Часть 1. Общие требования безопасности. 4. Требования безопасности к программируемым медицинским электронным системам», подготовленного Техническим комитетом МЭК 62 «Изделия медицинские электрические».

Настоящий стандарт является дополнительным стандартом по отношению к ГОСТ 30324.0/ГОСТ Р 50267.0 «Изделия медицинские электрические. Часть 1. Общие требования безопасности» (далее — общий стандарт).

Дополнительные стандарты устанавливают общие требования безопасности применительно к:

- группам изделий медицинского назначения (например, к рентгеновской аппаратуре);
- специальным характеристикам всей электромедицинской аппаратуры, не рассмотренным подробно в общем стандарте (например, электромагнитная совместимость).

Номера разделов, пунктов и подпунктов настоящего дополнительного стандарта соответствуют нумерации общего стандарта.

Номера пунктов и рисунков настоящего дополнительного стандарта, дополняющих общий стандарт, начинаются с цифры 201, дополнительные приложения обозначены буквами AAA, BBB и т.д.

Термины, используемые в настоящем стандарте, набраны прописными буквами. Методы испытаний по тексту настоящего стандарта выделены курсивом.

Все шире в МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ ИЗДЕЛИЯХ используются компьютеры, часто в критических, с точки зрения БЕЗОПАСНОСТИ, условиях. Использование компьютерных технологий в МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ ИЗДЕЛИЯХ обусловливает высокий уровень сложности этих изделий, уступающий лишь уровню сложности биологической системы организма ПАЦИЕНТА, для диагностики и/или лечения которого предназначено то или иное ИЗДЕЛИЕ. Подобная сложность означает, что при испытаниях некоторые систематические отказы могут остаться невыявленными. В соответствии с этим настоящий стандарт выходит за рамки традиционных методов испытания и оценок готовых к выпуску ИЗДЕЛИЙ и включает требования к процессу их разработки. Испытание готового изделия само по себе не является достаточным условием определения БЕЗОПАСНОСТИ сложных МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ ИЗДЕЛИЙ.

Настоящий стандарт устанавливает требования к процессу разработки и его этапам с тем, чтобы их выполнение обеспечило БЕЗОПАСНОСТЬ МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ ИЗДЕЛИЙ, включающих ПРОГРАММИРУЕМЫЕ ЭЛЕКТРОННЫЕ ПОДСИСТЕМЫ (ПЭПС). Понятия «управление РИСКОМ» и «ЦИКЛ РАЗРАБОТКИ», являющиеся основными понятиями данного стандарта, могут также иметь значение и при разработке ИЗДЕЛИЯ, в состав которого не входят ПРОГРАММИРУЕМЫЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ.

В зависимости от конкретной задачи эффективное применение настоящего стандарта требует соответствующей подготовки в следующих областях:

- БЕЗОПАСНАЯ ЭКСПЛУАТАЦИЯ конкретного медицинского ИЗДЕЛИЯ;
- процесс разработки конкретного ИЗДЕЛИЯ;
- методы, обеспечивающие АБСОЛЮТНУЮ БЕЗОПАСНОСТЬ; методы АНАЛИЗА РИСКА и УПРАВЛЕНИЯ РИСКОМ.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Изделия медицинские электрические

Часть 1

ОБЩИЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

4. Требования безопасности к программируемым медицинским электронным системам

Medical electrical equipment. Part 1.
General requirements for safety. 4. Safety requirements for programmable medical electrical systems

Дата введения 2001—01—01

РАЗДЕЛ ПЕРВЫЙ. ОБЩИЕ ПОЛОЖЕНИЯ

1 Область распространения и цель

1.201 Область распространения

Настоящий дополнительный стандарт устанавливает требования БЕЗОПАСНОСТИ ИЗДЕЛИЙ МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ и МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ СИСТЕМ, включающих ПРОГРАММИРУЕМЫЕ ЭЛЕКТРОННЫЕ ПОДСИСТЕМЫ (ПЭПС) [далее — ПРОГРАММИРУЕМЫЕ МЕДИЦИНСКИЕ ЭЛЕКТРОННЫЕ СИСТЕМЫ (ПМЭС)].

Примечание — Некоторые системы с программным обеспечением, используемые в медицинских целях и не отвечающие определениям: ИЗДЕЛИЕ МЕДИЦИНСКОЕ ЭЛЕКТРИЧЕСКОЕ по 2.2.15 ГОСТ 30324.0/ГОСТ Р 50267.0 или МЕДИЦИНСКАЯ ЭЛЕКТРИЧЕСКАЯ СИСТЕМА по 2.203 ГОСТ Р МЭК 601-1-1, не входят в область применения настоящего стандарта, например многие медицинские информационные системы.

Требования настоящего стандарта являются обязательными.

1.202 Цель

Настоящий стандарт устанавливает требования к процессу разработки программируемых электронных медицинских систем (ПМЭС) и служит основой для разработки частных стандартов, включая руководство по требованиям БЕЗОПАСНОСТИ для снижения РИСКА и с целью управления РИСКОМ. Настоящий стандарт предназначен для:

a) сертификационных центров,
b) ИЗГОТОВИТЕЛЕЙ;
c) разработчиков частных стандартов;

настоящий стандарт устанавливает требования к:

d) техническим заданиям,
e) архитектуре,
f) детальному проекту и его реализации, включая разработку программного обеспечения,
g) модификации,
h) ТЕХНИЧЕСКОМУ КОНТРОЛЮ и проверке СООТВЕТСТВИЯ,
j) маркировке и ЭКСПЛУАТАЦИОННЫМ ДОКУМЕНТАМ;

настоящий стандарт не распространяется на:

k) производство аппаратного обеспечения,
l) копирование программного обеспечения,
m) установку и сдачу в эксплуатацию;
n) функционирование и техническое обслуживание ПМЭС,
o) снятие ПМЭС с эксплуатации.

1.203 Связь с другими стандартами

1.203.1 ГОСТ 30324.0/ГОСТ Р 50267.0

Издание официальное

В части МЕДИЦИНСКИХ ЭЛЕКТРИЧЕСКИХ ИЗДЕЛИЙ настоящий стандарт является дополнением к ГОСТ 30324.0/ГОСТ Р 50267.0 и его изменениям. Здесь и далее при ссылках на ГОСТ 30324.0/ГОСТ Р 50267.0 или настоящий дополнительный стандарт принята следующая терминология:

- «общий стандарт» — только для обозначения ГОСТ 30324.0/ГОСТ Р 50267.0;
- «настоящий дополнительный стандарт» — только для обозначения данного стандарта (ГОСТ Р 50267.0.4);
- «настоящий стандарт» — для обозначения комбинации общего стандарта и настоящего дополнительного стандарта.

1.203.2 Частные стандарты

Требования частного стандарта имеют приоритет над соответствующими требованиями настоящего дополнительного стандарта.

1.203.3 Нормативные ссылки

В настоящем дополнительном стандарте использованы ссылки на следующие стандарты:

ГОСТ 30324.0—95 (МЭК 601-1—88)/ГОСТ Р 50267.0—92 (МЭК 601-1—88) Изделия медицинские электрические. Часть 1. Общие требования безопасности

ГОСТ Р МЭК 601-1-1—96 Изделия медицинские электрические. Часть 1. Общие требования безопасности. Требования безопасности к медицинским электрическим системам

ГОСТ Р ИСО 9001—96 Системы качества. Модель обеспечения качества при проектировании, разработке, производстве, монтаже и обслуживании

ИСО 9000-3—91* Общее руководство качеством и стандарты по обеспечению качества. Часть 3. Руководящие указания по применению ИСО 9001 при разработке, поставке и обслуживании программного обеспечения

МЭК 60788—84* Медицинская радиационная техника. Термины и определения

2 Термины и определения

2.201 Используемые термины

В настоящем дополнительном стандарте применяются термины с соответствующими определениями по ГОСТ 30324.0/ГОСТ Р 50267.0, ГОСТ Р МЭК 601-1-1, МЭК 60788, а также дополнительные термины по 2.201.1—2.201.15. Алфавитный указатель терминов приведен в приложении ААА.

2.201.1 **ЦИКЛ РАЗРАБОТКИ**

Необходимые действия, предпринимаемые начиная с начальной (концептуальной) стадии разработки проекта до окончания приемки ПМЭС (проверки СООТВЕТСТВИЯ).

2.201.2 **АНАЛИЗ ОПАСНОСТЕЙ**

Определение ОПАСНОСТЕЙ и вызывающих их причин.

Примечание — Количественная оценка ОПАСНОСТИ не входит в АНАЛИЗ ОПАСНОСТИ.

2.201.3 **МАКСИМАЛЬНО ДОПУСТИМЫЙ РИСК**

Величина РИСКА, которая определена в качестве максимально допустимой.

Примечание — Эта величина может быть определена для всей ПМЭС или для конкретной ОПАСНОСТИ.

2.201.4 **ПРОГРАММИРУЕМАЯ МЕДИЦИНСКАЯ ЭЛЕКТРОННАЯ СИСТЕМА (ПМЭС)**

ИЗДЕЛИЕ МЕДИЦИНСКОЕ ЭЛЕКТРИЧЕСКОЕ или МЕДИЦИНСКАЯ ЭЛЕКТРИЧЕСКАЯ СИСТЕМА, включающая ПРОГРАММИРУЕМУЮ ЭЛЕКТРОННУЮ ПОДСИСТЕМУ (ПЭПС).

2.201.5 **ПРОГРАММИРУЕМАЯ ЭЛЕКТРОННАЯ ПОДСИСТЕМА (ПЭПС)**

Система на основе одного или нескольких центральных процессоров, включающая программное обеспечение и интерфейс.

2.201.6 **ОСТАТОЧНЫЙ РИСК**

РИСК, выявленный во время проведения АНАЛИЗА ОПАСНОСТЕЙ и сохраняющийся после завершения операций по управлению РИСКОМ.

2.201.7 **РИСК**

Величина вероятности возникновения ОПАСНОСТИ, причиняющей вред и степень ТЯЖЕСТИ вредного воздействия.

2.201.8 **ДОКУМЕНТАЦИЯ ПО УПРАВЛЕНИЮ РИСКОМ**

Совокупность данных по качеству, которая предусмотрена настоящим стандартом.

2.201.9 **СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ**

Документ, позволяющий выявить каждую ОПАСНОСТЬ и ее причину для проведения анализа РИСКА и ТЕХНИЧЕСКОГО КОНТРОЛЯ каждой ОПАСНОСТИ.

---

* Международный стандарт — во ВНИИКИ Госстандарта России.

Примечание — Этот документ может быть изложен на бумаге или представлен в электронном виде.

2.201.10 **БЕЗОПАСНОСТЬ**

Отсутствие недопустимого РИСКА.

2.201.11 **ОПАСНОСТЬ**

Вредное воздействие на ПАЦИЕНТА, другие лица, животных или окружающую среду, причиной которого является МЕДИЦИНСКОЕ ЭЛЕКТРИЧЕСКОЕ ИЗДЕЛИЕ.

2.201.12 **АБСОЛЮТНАЯ БЕЗОПАСНОСТЬ**

Высокая вероятность того, что рассматриваемая система удовлетворяет требованиям БЕЗОПАСНОСТИ при функционировании в заданных условиях в течение установленного периода времени.

2.201.13 **ТЯЖЕСТЬ**

Качественный критерий возможных последствий ОПАСНОСТИ.

2.201.14 **СООТВЕТСТВИЕ**

Оценка ПМЭС (или ее составляющих) на соответствие требованиям технического задания во время или по окончании процесса разработки.

2.201.15 **ТЕХНИЧЕСКИЙ КОНТРОЛЬ**

Оценка результатов определенного этапа разработки ПМЭС (или ее составляющих) на соответствие требованиям, установленным на начальной стадии этого этапа.

2.202 Терминология

В настоящем дополнительном стандарте использована следующая терминология:

«должен» — соответствие требованиям стандарта обязательно;

«рекомендуется» — соответствие требованиям стандарта рекомендуемое, но не обязательное;

«может» — используют для описания допустимых путей достижения соответствия требованиям стандарта;

«установленный» — используется в качестве ссылки на информацию, приведенную в настоящем дополнительном стандарте или ссылочных стандартах и касающуюся, как правило, конкретных рабочих условий, методик испытаний или значений, связанных с формулировкой соответствия;

«нормированный» — используется в качестве ссылки на информацию, указанную ИЗГОТОВИТЕЛЕМ в СОПРОВОДИТЕЛЬНЫХ (далее — ЭКСПЛУАТАЦИОННЫХ) ДОКУМЕНТАХ или иной документации, относящейся к рассматриваемой ПМЭС и, как правило, касающейся назначения системы, параметров или условий ее эксплуатации, или испытаний для определения соответствия техническим требованиям.

6 Идентификация, маркировка и документация

6.8 ЭКСПЛУАТАЦИОННЫЕ ДОКУМЕНТЫ

6.8.201 Вся необходимая информация по ОСТАТОЧНОМУ РИСКУ должна быть представлена как в ИНСТРУКЦИЯХ ПО ЭКСПЛУАТАЦИИ, так и в ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

Наличие необходимой информации проверяют путем просмотра ИНСТРУКЦИИ ПО ЭКСПЛУАТАЦИИ и ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

РАЗДЕЛ ДЕВЯТЫЙ. НЕНОРМАЛЬНАЯ РАБОТА И УСЛОВИЯ НАРУШЕНИЯ; ИСПЫТАНИЯ НА ВОЗДЕЙСТВИЕ ВНЕШНИХ ФАКТОРОВ

52 Ненормальная работа и условия нарушения

52.201 Документация

52.201.1 Документы, разработанные в соответствии с настоящим стандартом, должны сохраняться и составлять неотъемлемую часть документации по качеству в соответствии с 6.3 ИСО 9000-3 и рисунком 201.

52.201.2 Документы, называемые далее ДОКУМЕНТАЦИЕЙ ПО УПРАВЛЕНИЮ РИСКОМ, должны утверждаться, публиковаться и изменяться в соответствии с правилами системы управления документацией, что соответствует требованиям 6.2 ИСО 9000-3.

52.201.3 СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ должна формироваться на протяжении всего ЦИКЛА РАЗРАБОТКИ как часть ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ. Она должна содержать информацию по:

a) идентификации ОПАСНОСТЕЙ и причин, вызывающих их;

b) оценке РИСКА;

c) мерам БЕЗОПАСНОСТИ, применяемым для устранения РИСКА или для его контроля, включая требуемую АБСОЛЮТНУЮ БЕЗОПАСНОСТЬ;

d) оценке эффективности управления РИСКОМ;

e) ТЕХНИЧЕСКОМУ КОНТРОЛЮ.

Соответствие проверяют путем просмотра ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.202 План управления РИСКОМ

52.202.1 ИЗГОТОВИТЕЛЬ должен разработать план управления РИСКОМ.

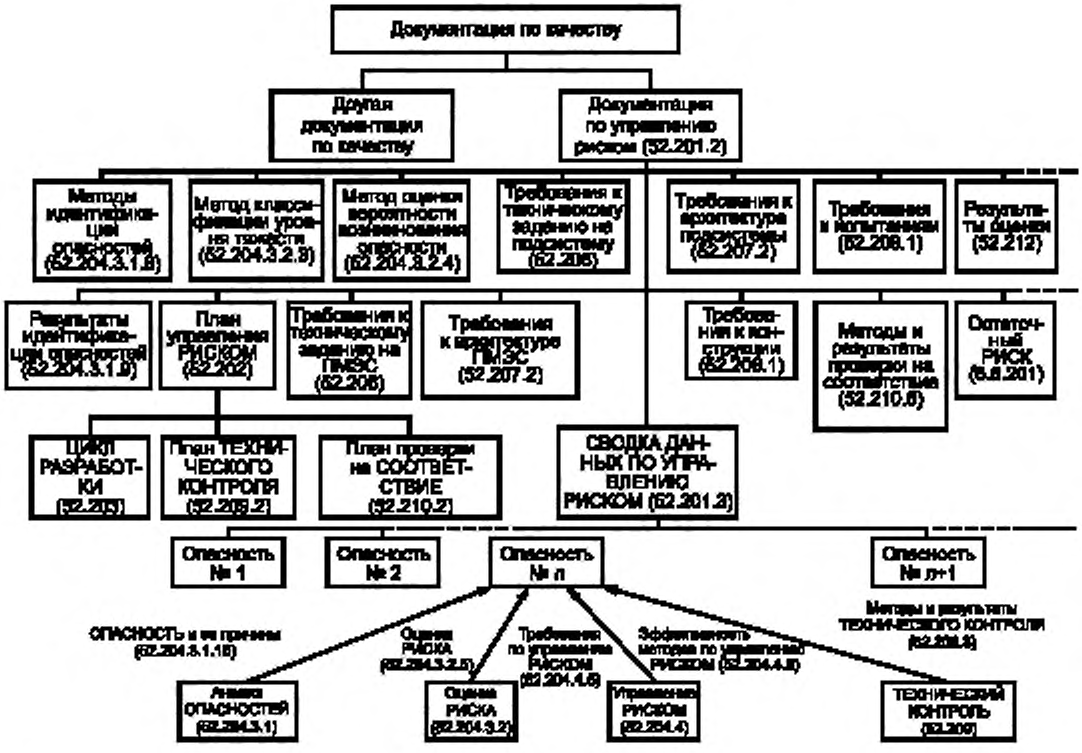


Рисунок 201 — Содержание ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ и СВОДКИ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ

52.202.2 Этот план должен включать:

a) область распространения плана, определяющую проект или изделие и фазы ЦИКЛА РАЗРАБОТКИ, к которым применим этот план;

b) ЦИКЛ РАЗРАБОТКИ (52.203), включая план ТЕХНИЧЕСКОГО КОНТРОЛЯ и план проверки на СООТВЕТСТВИЕ;

c) ответственность по управлению РИСКОМ в соответствии с 4.1 ГОСТ Р ИСО 9001;

d) процесс управления РИСКОМ;

e) требования по периодическому пересмотру.

52.202.3 В процессе разработки все изменения в плане управления РИСКОМ должны регистрироваться.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.203 ЦИКЛ РАЗРАБОТКИ

52.203.1 При проектировании и разработке ПМЭС необходимо определить ЦИКЛ РАЗРАБОТКИ.

52.203.2 ЦИКЛ РАЗРАБОТКИ необходимо разбить на отдельные этапы и задания с точно определенными входными и выходными данными и последовательностью действий по каждому этапу работы.

52.203.3 ЦИКЛ РАЗРАБОТКИ должен включать общие способы управления РИСКОМ.

52.203.4 ЦИКЛ РАЗРАБОТКИ должен включать требования к документации.

52.203.5 Мероприятия по управлению РИСКОМ должны проводиться на протяжении всего ЦИКЛА РАЗРАБОТКИ, где это необходимо (52.204).

Примечание — Пример ЦИКЛА РАЗРАБОТКИ дан в приложении DDD.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.204 Процесс управления РИСКОМ

52.204.1 Процесс управления РИСКОМ должен включать:

- анализ РИСКА,
- управление РИСКОМ.

52.204.2 Этот процесс должен применяться на протяжении всего ЦИКЛА РАЗРАБОТКИ.

52.204.3 Анализ РИСКА

52.204.3.1 АНАЛИЗ ОПАСНОСТЕЙ

52.204.3.1.1 Идентификацию ОПАСНОСТЕЙ выполняют в соответствии с планом по управлению РИСКОМ (52.202).

52.204.3.1.2 ОПАСНОСТИ должны быть идентифицированы для всех практически возможных ситуаций, включая:

- НОРМАЛЬНУЮ ЭКСПЛУАТАЦИЮ;
- неправильное использование.

52.204.3.1.3 Должны быть рассмотрены следующие ОПАСНОСТИ, если существует вероятность их возникновения:

- ОПАСНОСТИ для ПАЦИЕНТА;
- ОПАСНОСТИ для ОПЕРАТОРОВ;
- ОПАСНОСТИ для обслуживающего персонала;
- ОПАСНОСТИ для окружающих;
- ОПАСНОСТИ для окружающей среды.

52.204.3.1.4 Должна быть рассмотрена последовательность событий, способных привести к возникновению ОПАСНОСТИ.

52.204.3.1.5 Рассматриваемые причины возникновения ОПАСНОСТЕЙ должны учитывать, если уместно, следующие моменты:

- человеческие факторы;
- повреждение механической части;
- нарушения в программном обеспечении;
- ошибки в системе;
- воздействие внешних факторов.

52.204.3.1.6 При необходимости АНАЛИЗ РИСКА должен включать следующие вопросы:

- совместимость компонентов системы, включая механическую часть и программное обеспечение;
- интерфейс пользователя, включая язык команд, предупреждения и сообщения об ошибках;
- точность перевода текста, используемого в интерфейсе пользователя и в ИНСТРУКЦИЯХ ПО ЭКСПЛУАТАЦИИ;
- защиту данных от преднамеренных и случайных ошибок человека;
- критерий соотношения РИСК/польза;
- специфические особенности программного обеспечения.

Примечание — Необходимо также учитывать возможные влияния:

- совместимости различных блоков программ;
- совместимости программ обработки с поступающими данными в цифровой форме.

52.204.3.1.7 Необходимо использовать методы идентификации ОПАСНОСТЕЙ, соответствующие определенному этапу ЦИКЛА РАЗРАБОТКИ.

52.204.3.1.8 В ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ должны быть отражены используемые методы (например, анализ дерева неисправностей, возможные отказы и их последствия).

52.204.3.1.9 Результаты применения этих методов необходимо регистрировать в ДОКУМЕНТАЦИИ ПО ОБЕСПЕЧЕНИЮ УРОВНЯ РИСКА.

52.204.3.1.10 Каждая из выявленных ОПАСНОСТЕЙ и ее причины должны регистрироваться в СВОДКЕ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ.

Соответствие проверяют просмотром СВОДКИ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ.

52.204.3.2 Оценка РИСКА

52.204.3.2.1 Для каждой из выявленных ОПАСНОСТЕЙ должна быть проведена оценка РИСКА.

52.204.3.2.2 Оценка РИСКА должна проводиться на основе оценки вероятности возникновения каждой ОПАСНОСТИ и(или) степени ТЯЖЕСТИ последствий каждой ОПАСНОСТИ.

52.204.3.2.3 Метод классификации уровня ТЯЖЕСТИ должен регистрироваться в ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.204.3.2.4 Используемый метод оценки вероятности возникновения ОПАСНОСТИ должен быть либо количественным, либо качественным и должен регистрироваться в ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.204.3.2.5 В СВОДКЕ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ против каждой из ОПАСНОСТЕЙ должна быть указана оценка РИСКА.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.204.4 Управление РИСКОМ

52.204.4.1 Управление РИСКОМ должно осуществляться таким образом, чтобы обеспечивался приемлемый уровень оценки РИСКА для каждой из идентифицированных ОПАСНОСТЕЙ.

52.204.4.2 РИСК считается приемлемым, если он меньше или равен МАКСИМАЛЬНО ДОПУСТИМОМУ РИСКУ и снижен до наименьшего практически достижимого значения.

52.204.4.3 Методы по управлению РИСКОМ должны уменьшать вероятность возникновения ОПАСНОСТИ и(или) степень ее ТЯЖЕСТИ.

52.204.4.4 Методы по управлению РИСКОМ должны быть направлены на выявление причины ОПАСНОСТИ (например, на снижение вероятности ее возникновения) и (или) на установку защитных средств, которые должны срабатывать при наличии ОПАСНОСТИ, или на то и другое вместе с учетом следующих приоритетов:

- безопасность, предусмотренную конструкцией;
- защитные средства, включая сигналы тревоги;
- достаточную информацию по ОСТАТОЧНОМУ РИСКУ, предназначенную для ПОЛЬЗОВАТЕЛЯ.

52.204.4.5 Требование(я) по управлению РИСКОМ должно(ы) быть внесено(ы) в СВОДКУ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ (либо непосредственно, либо путем перекрестных ссылок).

52.204.4.6 Оценка эффективности методов по управлению РИСКОМ должна быть отражена в СВОДКЕ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.205 Квалификация персонала

Проектирование и модификация ПМЭС должны выполняться персоналом, квалификация которого соответствует требованиям 4.18 ГОСТ Р ИСО 9001.

Соответствие проверяют просмотром соответствующей картотеки персонала.

52.206 Техническое задание

52.206.1 На ПМЭС и на каждую из ее подсистем (например, ПЭПС) должно составляться техническое задание (ТЗ).

Примечание — Пример структуры ПМЭС дан в приложении EEE.

52.206.2 В техническом задании должно быть дано детальное описание функций ПМЭС, связанных с РИСКОМ. К таким функциям относятся функции, которые управляют РИСКОМ, возникающим от:

a) причин, вызванных воздействием окружающих внешних условий;

b) причин, вызванных воздействием где-нибудь в ПМЭС;

c) возможных сбоев.

52.206.3 Для каждой из этих функций в техническом задании должен быть указан уровень АБСОЛЮТНОЙ БЕЗОПАСНОСТИ, необходимый для управления РИСКОМ.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.207 Архитектура

52.207.1 Архитектура ПМЭС должна удовлетворять требованиям технического задания.

52.207.2 Архитектура ПМЭС и каждой из ее подсистем должна быть подробно определена.

52.207.3 Там, где это уместно, техническое задание должно содержать следующие требования:

a) расположение средств по управлению РИСКОМ по отношению к подсистемам и компонентам ПМЭС.

Примечание — Подсистемы и компоненты включают датчики, приводы, ПЭПС и интерфейсы;

b) резервирование;

c) разнесенность;

d) процент и типы отказов компонентов;

e) наличие элементов диагностики или уровень диагностики;

f) отказы, обусловленные общей причиной;

g) систематические отказы;
h) периодичность и продолжительность испытаний;
j) ремонтопригодность;
k) защиту от преднамеренных или случайных ошибок человека.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.208 Конструкция и выполнение требований

52.208.1 При необходимости общая конструкция ПМЭС должна быть разбита на подсистемы с собственной конструкцией и техническими требованиями к испытаниям.

52.208.2 При необходимости должны быть нормированы следующие требования к:
a) методам разработки программного обеспечения;
b) электронному аппаратному обеспечению;
c) используемым в компьютере инструментам для разработки и контроля программного обеспечения;
d) датчикам;
e) приводам;
f) интерфейсу ПМЭС-пользователь;
g) источникам питания;
h) условиям окружающей среды;
j) инструментальным средствам для программирования;
k) специфическим особенностям программного обеспечения.

Примечание — При необходимости должны быть учтены специфические особенности построения вычислительной сети.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.209 ТЕХНИЧЕСКИЙ КОНТРОЛЬ

52.209.1 Должен быть проведен ТЕХНИЧЕСКИЙ КОНТРОЛЬ выполнения требований БЕЗОПАСНОСТИ.

52.209.2 Для демонстрации способов проверки выполнения требований БЕЗОПАСНОСТИ на каждом этапе ЦИКЛА РАЗРАБОТКИ должен быть разработан план ТЕХНИЧЕСКОГО КОНТРОЛЯ.

52.209.3 В СВОДКУ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ должны быть включены ссылки на методы и результаты ТЕХНИЧЕСКОГО КОНТРОЛЯ.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.210 СООТВЕТСТВИЕ

52.210.1 Должно обеспечиваться СООТВЕТСТВИЕ требованиям БЕЗОПАСНОСТИ.

52.210.2 Должен быть разработан план проверки на СООТВЕТСТВИЕ, выполнение которого должно подтвердить правильность примененных требований БЕЗОПАСНОСТИ.

52.210.3 Руководитель группы, выполняющей проверку на СООТВЕТСТВИЕ, должен быть лицом, не зависимым от группы, выполняющей разработку проекта.

52.210.4 Любые профессиональные взаимоотношения между членами группы, выполняющей проверку на СООТВЕТСТВИЕ, и членами группы, выполняющей разработку, должны быть отражены в ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.210.5 Ни один член группы, выполняющей разработку, не может выполнять проверку на СООТВЕТСТВИЕ своего проекта.

52.210.6 В ДОКУМЕНТАЦИЮ ПО УПРАВЛЕНИЮ РИСКОМ должны быть включены ссылки на методы проверки на СООТВЕТСТВИЕ и их результаты.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.211 Модификация

52.211.1 Если вся конструкция или какие-либо ее части являются результатом модификации ранее разработанной конструкции, то настоящий стандарт применяется полностью к разработанной впервые конструкции, либо в процессе модификации документация ранее разработанного проекта должна быть проверена на соответствие.

52.211.2 Вся документация, относящаяся к ЦИКЛУ РАЗРАБОТКИ, должна быть пересмотрена, изменена и одобрена в соответствии с правилами контроля документации согласно 4.5.2 ГОСТ Р ИСО 9001 либо в соответствии с требованиями эквивалентного нормативного документа.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

52.212 Оценка

52.212.1 Для проверки соответствия ПМЭС требованиям настоящего стандарта должна быть проведена оценка, результаты которой вносят в ДОКУМЕНТАЦИЮ ПО УПРАВЛЕНИЮ РИСКОМ. Оценка может выполняться внутренней службой нормоконтроля.

Соответствие проверяют просмотром ДОКУМЕНТАЦИИ ПО УПРАВЛЕНИЮ РИСКОМ.

ПРИЛОЖЕНИЕ ААА
(обязательное)

Алфавитный указатель терминов

В настоящем указателе для каждого термина указан соответствующий номер подпункта настоящего дополнительного стандарта (2.201), общего стандарта (ОС-2), а также приведено обозначение термина по МЭК 60788 (МР-..-..) и ГОСТ Р МЭК 601-1-1 (А-).

АБСОЛЮТНАЯ БЕЗОПАСНОСТЬ	2.201.12
АНАЛИЗ ОПАСНОСТИ	2.201.2
БЕЗОПАСНОСТЬ	2.201.10
ДОКУМЕНТАЦИЯ ПО УПРАВЛЕНИЮ РИСКОМ	2.201.8
ИЗГОТОВИТЕЛЬ	МР-85-03
ИЗДЕЛИЕ МЕДИЦИНСКОЕ ЭЛЕКТРИЧЕСКОЕ	ОС-2.2.15
ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ	МР-82-02
МАКСИМАЛЬНО ДОПУСТИМЫЙ РИСК	2.201.3
МЕДИЦИНСКАЯ ЭЛЕКТРИЧЕСКАЯ СИСТЕМА	А-2.203
НОРМАЛЬНАЯ ЭКСПЛУАТАЦИЯ	ОС-2.10.8
ОПАСНОСТЬ	2.201.11
ОПЕРАТОР	МР-85-02
ОСТАТОЧНЫЙ РИСК	2.201.6
ПАЦИЕНТ	МР-602-03
ПОЛЬЗОВАТЕЛЬ	МР-85-01
ПРОГРАММИРУЕМАЯ МЕДИЦИНСКАЯ ЭЛЕКТРОННАЯ СИСТЕМА (ПМЭС)	2.201.4
ПРОГРАММИРУЕМАЯ ЭЛЕКТРОННАЯ ПОДСИСТЕМА (ПЭПС)	2.201.5
РИСК	2.201.7
СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ	2.201.9
СООТВЕТСТВИЕ	2.201.14
СОПРОВОДИТЕЛЬНЫЕ (ЭКСПЛУАТАЦИОННЫЕ) ДОКУМЕНТЫ	МР-82-01
ТЕХНИЧЕСКИЙ КОНТРОЛЬ	2.201.15
ТЯЖЕСТЬ	2.201.13
УСЛОВИЕ ЕДИНИЧНОГО НАРУШЕНИЯ	ОС-2.10.11
ЦИКЛ РАЗРАБОТКИ	2.201.1

ПРИЛОЖЕНИЕ ВВВ
(справочное)

Обоснование

Общие положения

Настоящий стандарт требует, чтобы процесс разработки ПМЭС как процесс, включающий определенные элементы, был определен и тщательно соблюдался, поскольку рассматриваемый тип изделий невозможно оценивать по принципу годен/ не годен путем испытания готовой продукции. Предлагаемый подход устанавливает, что требуется для обеспечения БЕЗОПАСНОСТИ, при этом ПОЛЬЗОВАТЕЛЮ данного стандарта предоставляется право решать, каким образом этого достичь. Такой подход аналогичен подходу, принятому в стандартах серии ИСО 9000. Так как предполагается, что ПОЛЬЗОВАТЕЛЬ должен иметь соответствующую квалификацию, подробности и уточнения при изложении стандарта были сведены к минимуму. Возможно повторение отдельных частей такого процесса, но такие требования не приводились, так как необходимость повторения процедур является индивидуальной для каждого конкретного проекта. Необходимость таких повторений возникает также при более полном понимании сущности проекта, которое возникает в ходе процесса его разработки.

Частью процесса является документация, необходимая для управления процессом разработки. Кроме того, просмотр документации позволяет контролировать соответствие применяемого процесса разработки процессу, изложенному в настоящем стандарте. СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ является частью

документации и обеспечивает ясное понимание вопросов, связанных с БЕЗОПАСНОСТЬЮ и мерами, принимаемыми для ее обеспечения в течение и по окончании процесса разработки.

Подчеркивается, что процесс по управлению РИСКОМ хотя и не может быть единым для ПМЭС, необходим вследствие исключительной сложности рассматриваемых технологий и гарантирует выявление ОПАСНОСТЕЙ на ранних стадиях разработки. Выявление ОПАСНОСТЕЙ на ранних стадиях разработки необходимо для того, чтобы впоследствии жесткость требований в отношении БЕЗОПАСНОСТИ дала соответствующий результат.

Настоящий стандарт должен применяться лицами, имеющими соответствующую квалификацию. Это условие направлено на обеспечение непрерывного соответствия требований стандарта уровню развития и объему знаний в областях обеспечения качества программ и методик оценки ОПАСНОСТЕЙ. ПОЛЬЗОВАТЕЛЮ настоящего стандарта в конкретных обстоятельствах, возникающих в процессе разработки ПМЭС, так или иначе придется применять сведения, публикуемые в специальной литературе. На ранних стадиях разработки чаще используют методику анализа «сверху вниз», такую как анализ с использованием дерева ошибок. Когда проект более детализирован, то начинает шире использоваться методика анализа «снизу вверх», такая как виды отказов и анализ режимов нарушения и их последствий.

Термины и определения

Термины и определения приводятся для удобства чтения стандарта и с целью уменьшения общего объема текста. Было сделано все возможное, чтобы сделать требования максимально ясными и исключить ошибочное использование определений в качестве требований.

Документация

СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ необходима для того, чтобы обеспечивать управление РИСКОМ при выявлении ОПАСНОСТЕЙ. Заполнение СВОДКИ ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ прекращается после завершения ЦИКЛА РАЗРАБОТКИ.

ЦИКЛ РАЗРАБОТКИ

ЦИКЛ РАЗРАБОТКИ необходим для обеспечения систематического контроля БЕЗОПАСНОСТИ и, в частности, для раннего выявления ОПАСНОСТЕЙ в сложных системах.

Процесс по управлению РИСКОМ

Требования к процессу по управлению РИСКОМ определяют основную схему, в рамках которой на основании опыта, интуиции и суждений успешно осуществляется управление РИСКОМ. Уровень детализации выбран в соответствии с настоящим дополнительным стандартом. При рассмотрении конкретного медицинского применения в частном стандарте могут быть представлены специальные методики по управлению РИСКОМ, включая требования типа годен/не годен.

Такой процесс применяется на протяжении всего ЦИКЛА РАЗРАБОТКИ для определения адекватных методов по управлению РИСКОМ при выявлении причин ОПАСНОСТЕЙ.

Оценка РИСКА

Программные и другие систематические ошибки не укладываются в концепцию вероятности как собственно события. Тем не менее, основной целью настоящего стандарта является уменьшение вероятности присутствующих систематических ошибок. Другой проблемой, связанной с предыдущей, является вероятность ошибки, приводящей к ОПАСНОСТИ, возникающей в процессе эксплуатации. Эти компоненты РИСКА, связанные с систематическими ошибками, которые редко поддаются количественной оценке, тщательно рассматриваются в каждом надежном процессе проектирования. Оценка РИСКА является необходимым шагом как при определении фокуса концентрации усилий при работе над проектом, так и при обсуждении результатов. Вопрос, как количественно или качественно оценивать вероятность возникновения систематических программных ошибок, находится в стадии рассмотрения.

ПРИЛОЖЕНИЕ CCC
(справочное)

Понятия РИСКА

РИСК

Понятие ВОЗМОЖНОГО РИСКА включает два элемента:

- вероятность возникновения опасного события;
- степень ТЯЖЕСТИ последствий опасного события.

При определении категорий РИСКА можно выделить три области:

- область недопускаемых значений;
- область целесообразно допускаемых значений (ЦДЗ);
- область допускаемых значений.

Область недопускаемых значений

РИСК некоторых ОПАСНОСТЕЙ настолько велик, что система, в которой они существуют, не может быть признана удовлетворительной. В этой области РИСК должен быть уменьшен путем снижения ТЯЖЕСТИ и/или вероятности возникновения таких ОПАСНОСТЕЙ.

Область целесообразно допускаемых значений (ЦДЗ)

Область между областями недопускаемых и допускаемых значений называется областью ЦДЗ. В области ЦДЗ РИСК снижают до минимального практически достижимого уровня, принимая во внимание разумность допустимого РИСКА и затраты на его дальнейшее уменьшение. Любой РИСК рекомендуется снижать до уровня «целесообразно допускаемого значения» (ЦДЗ). Рядом с границей области недопускаемых значений РИСК следует уменьшить даже ценой значительных затрат.

Область допускаемых значений

В некоторых случаях ТЯЖЕСТЬ ОПАСНОСТИ и/или ее вероятность настолько низки, что в сравнении с РИСКОМ от других допускаемых ОПАСНОСТЕЙ такой РИСК оказывается пренебрежимо малым. В этом случае нет необходимости в процедуре снижения РИСКА. Графически три области РИСКА изображены на рисунке ССС.1.

Уровни ТЯЖЕСТИ

ТЯЖЕСТЬ является одной из составляющих РИСКА. Приведенные ниже четыре уровня ТЯЖЕСТИ являются средством качественной оценки возможных последствий ОПАСНОСТИ и предлагаются для использования при работе с ПМЭС:

- катастрофический: возможность нескольких смертельных случаев или серьезных поражений;
- критический: возможность смертельного случая или серьезного поражения;
- серьезный: возможность поражения;
- незначительный: пренебрежимо малая вероятность поражения или его невозможность.

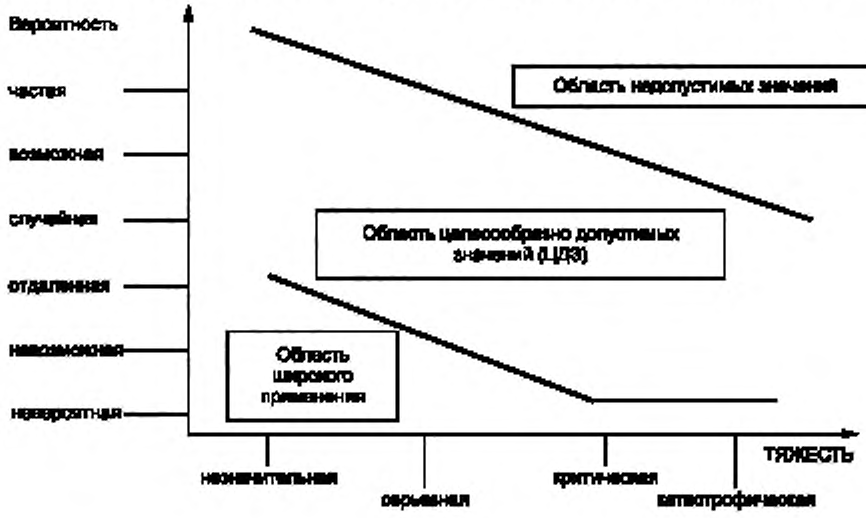


Рисунок ССС.1 — График областей РИСКА

Решение по выбору приемлемости РИСКА

Настоящий стандарт не определяет уровень приемлемости РИСКА. Предполагается, что руководство по определению приемлемости РИСКА будет содержаться в частных стандартах. Часто приемлемый РИСК будет определяться по принципу «от случая к случаю». При использовании понятия УСЛОВИЕ ЕДИНИЧНОГО НАРУШЕНИЯ, описанного в пункте 3 общего стандарта, и (или) исходя из эксплуатационных качеств аналогичного МЕДИЦИНСКОГО ЭЛЕКТРИЧЕСКОГО ИЗДЕЛИЯ, уже используемого в медицинской практике, могут быть выработаны некоторые правила.

Возможна ситуация, когда любой РИСК, связанный с ПМЭС, представляется приемлемым при улучшении прогноза заболевания ПАЦИЕНТА. Это не может служить основанием допущения неоправданного РИСКА. Всегда рекомендуется использовать принцип целесообразно допустимых значений (ЦДЗ).

Управление РИСКОМ

В настоящем стандарте требуется применение процесса управления РИСКОМ в течение всего ЦИКЛА РАЗРАБОТКИ. Цель такого процесса — обеспечить управление РИСКОМ таким образом, чтобы он был меньше МАКСИМАЛЬНО ДОПУСТИМОГО РИСКА, а также настолько мал, насколько это практически приемлемо. На рисунке ССС.2 изображена типичная схема процесса управления РИСКОМ.

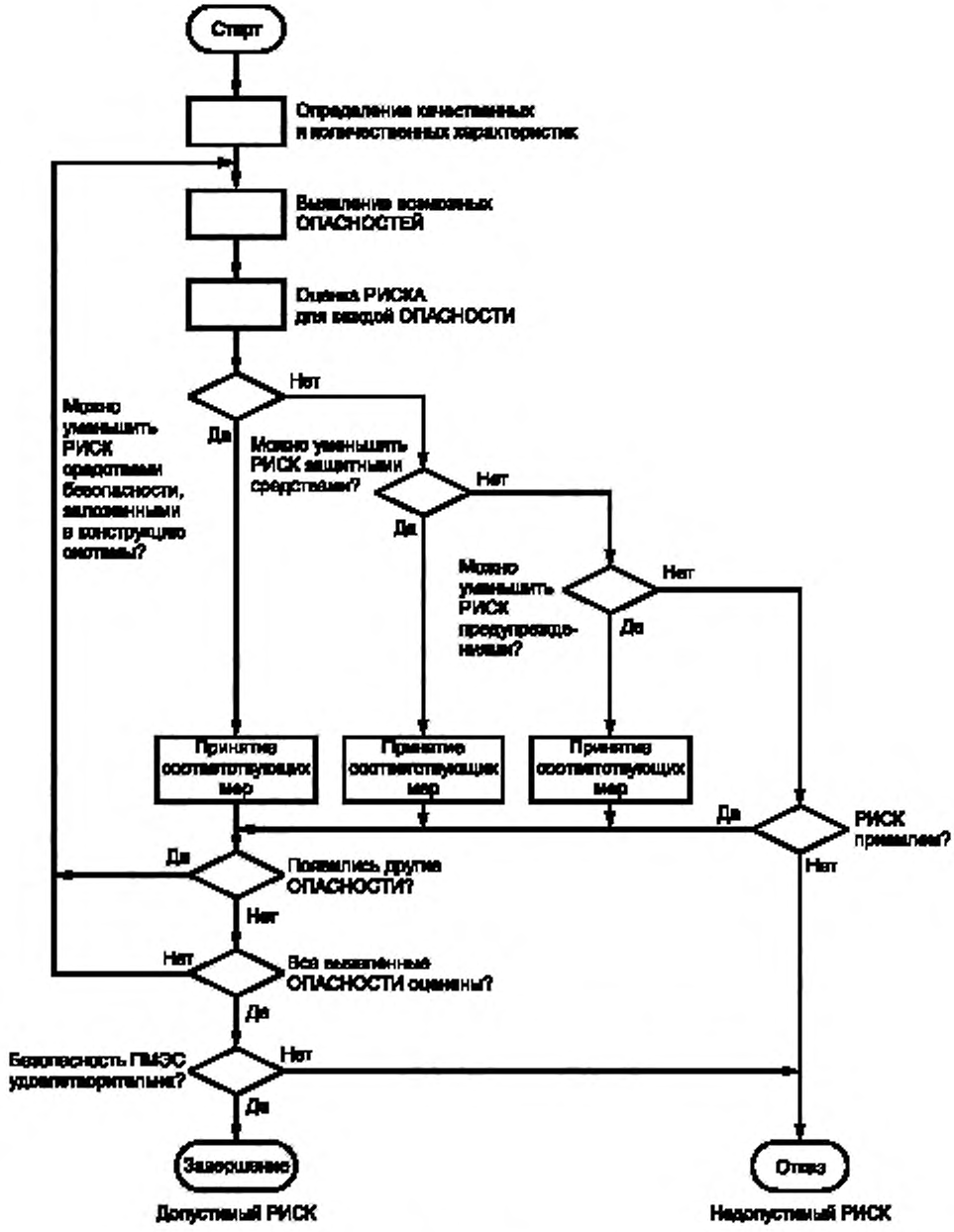


Рисунок ССС.2 — Процесс управления РИСКОМ

Причины нарушений

Опасное событие может произойти из-за нарушений в системе. Существуют два возможных вида нарушений:

- случайные нарушения;
- систематические нарушения.

Случайное нарушение

Для многих событий может быть определена статистическая вероятность их возникновения. Например, вероятность нарушения в электронной схеме часто оценивают по вероятностям отказов компонентов этой схемы. В этом случае вероятность нарушения может быть выражена числовым значением. При этом существенным является предположение о случайной природе такого нарушения. Предполагается, что нарушение в аппаратной части может быть либо случайным, либо систематическим. Нарушение в программном обеспечении может быть случайным, но его причина всегда является систематической.

Систематическое нарушение

Систематические нарушения возникают из-за ошибок (включая ошибки и упущения при проектировании) в процессе любого ЦИКЛА РАЗРАБОТКИ, которые при некоторой комбинации входных данных или при определенных внешних условиях приведут к нарушению.

Систематические нарушения возможны как в аппаратной части, так и в программном обеспечении и могут возникать на любом этапе ЦИКЛА РАЗРАБОТКИ изделия. Примером систематической ошибки является неправильная установка порогового значения в базе данных, приводящая к опасному состоянию. Неправильные данные могут появиться при их неверном определении, неправильном копировании в процессе подготовки данных или ошибочном изменении в процессе эксплуатации. Вероятность возникновения подобных случаев труднопредсказуема, хотя существует зависимость между качеством методов, используемых в течение ЦИКЛА РАЗРАБОТКИ, и вероятностью внесения такого нарушения или его необнаружения.

Оценка РИСКА

Используют различные методы оценки. В настоящем стандарте приведен пример качественной оценки РИСКА. Не требуя использования какого-либо конкретного метода оценки, в настоящем дополнительном стандарте требуется, чтобы такая оценка проводилась (52.204.3.2). При наличии подходящих данных возможна также количественная оценка РИСКА. Методы количественной оценки могут включать адаптированный метод качественной оценки, либо может подойти какой-то альтернативный подход. Метод, используемый для оценки РИСКА, является частью процесса управления РИСКОМ и должен быть определен в плане управления РИСКОМ [52.202.2, перечисление *d*)].

Для определения уровней РИСКА может применяться график РИСКА, показанный на рисунке ССС.1.

Уровни РИСКА могут быть классифицированы по одной из областей РИСКА: недопускаемая, ЦДЗ и допускаемая.

На рисунке ССС.1 дан пример графика РИСКА. Он включен в настоящий дополнительный стандарт, чтобы продемонстрировать метод оценки, но не предназначен для общего применения к ПМЭС. Если для оценки РИСКА используется подход, обозначенный на этом графике, то в этом случае следует продумать конкретный график оценки РИСКА и его интерпретацию.

АБСОЛЮТНАЯ БЕЗОПАСНОСТЬ

В тех случаях, когда оценка РИСКА показывает его неприемлемость, определяют функции управления РИСКОМ (52.206.2).

Существуют два принципиальных вопроса:

- обеспечивает ли система все необходимые функции управления РИСКОМ?
- будет ли система в рабочем состоянии после активизации таких функций?

АБСОЛЮТНАЯ БЕЗОПАСНОСТЬ относится к эксплуатационным параметрам рассматриваемой системы при выполнении ею функций, связанных с РИСКОМ.

Имеются два элемента АБСОЛЮТНОЙ БЕЗОПАСНОСТИ:

- целостность аппаратного обеспечения (в отношении случайных нарушений);
- систематическая целостность (включая аппаратное и программное обеспечения).

Целостность аппаратного обеспечения

Если вероятность отказа системы можно рассчитать или продемонстрировать (например расчет, основанный на допущении случайного отказа в аппаратном обеспечении), то это значение может быть использовано для определения ее целостности.

Систематическая целостность

Часто, если нарушения носят систематический характер, как, например, в случае программного обеспечения, практически невозможно продемонстрировать или рассчитать вероятность нарушения. В этом случае используют качественный метод определения АБСОЛЮТНОЙ БЕЗОПАСНОСТИ. Такой метод доказывает, что функция АБСОЛЮТНОЙ БЕЗОПАСНОСТИ зависит от факторов, связанных с ЦИКЛОМ РАЗРАБОТКИ, а именно:

- технологии и методов разработки;

- архитектуры;
- гарантии качества;
- управления проектированием;
- граничных значений используемых медицинских показателей.

Для каждого фактора должны выбираться соответствующие методы, которые позволят системе удовлетворительно выполнять заданную функцию во всех указанных условиях в пределах установленного периода времени.

Методы определения соотношения между различными факторами и полученной АБСОЛЮТНОЙ БЕЗОПАСНОСТЬЮ можно найти в МЭК 1508 и ИСО/МЭК 15026 (см. приложение FFF).

ПРИЛОЖЕНИЕ DDD
(справочное)

Модель ЦИКЛА РАЗРАБОТКИ

По настоящему стандарту необходимо четко определять, специфицировать этапы ЦИКЛА РАЗРАБОТКИ и затем выполнять их. Это не значит, что требуется использовать какой-то стандартный ЦИКЛ РАЗРАБОТКИ, однако ЦИКЛ РАЗРАБОТКИ должен отвечать определенным требованиям, которые изложены в 52.203 настоящего дополнительного стандарта.

На рисунке DDD.1 приведена модель ЦИКЛА РАЗРАБОТКИ. В этой модели после процесса разбивки следует интеграционный процесс. Поскольку проект, исходя из требований, разбивается на составные части, то это осуществляется на основе функциональных структурных элементов, архитектуры и технологии изготовления. Процесс разбивки заканчивают тогда, когда проектные данные дают возможность создавать компоненты ПМЭС (примерами таких данных служат схемы и коды программного обеспечения). После окончания процесса разбивки осуществляют интеграцию всех элементов в систему. По окончании объединения компонентов в одно целое проводят ТЕХНИЧЕСКИЙ КОНТРОЛЬ для того, чтобы определить, удовлетворяет ли полученная система установленным требованиям. На заключительном этапе процесса интеграции проводят проверку на СООТВЕТСТВИЕ с тем, чтобы убедиться, что ПМЭС работает в соответствии с ее назначением.

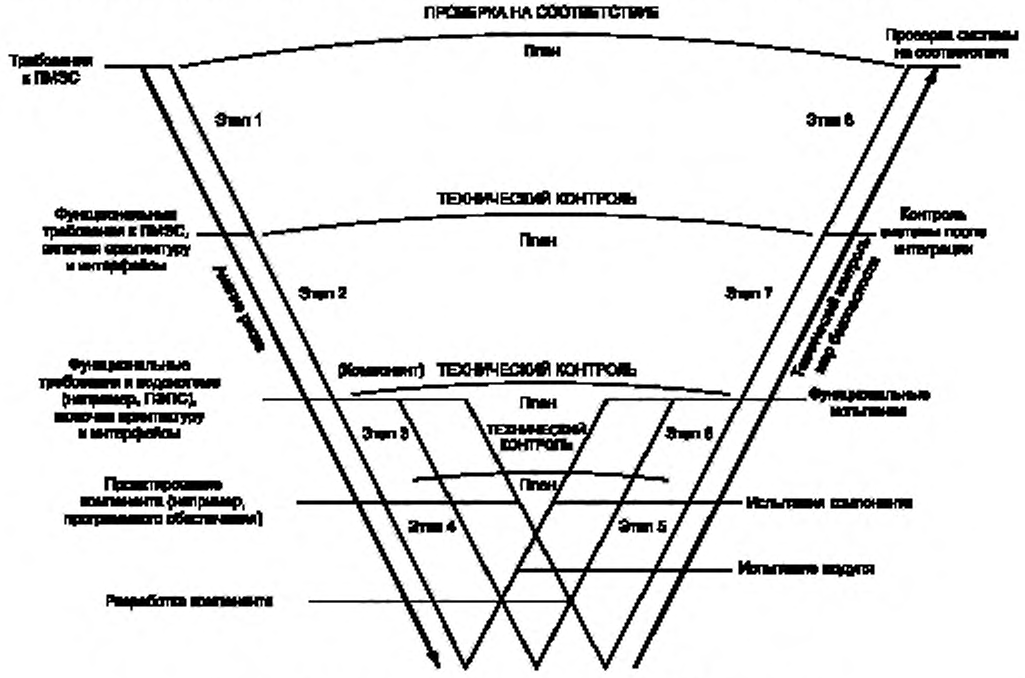


Рисунок DDD.1 — Модель ЦИКЛА РАЗРАБОТКИ для ПМЭС

Настоящий дополнительный стандарт требует, чтобы содержание ЦИКЛА РАЗРАБОТКИ было представлено в виде документов. Это требование не означает, что устанавливается жесткая связь между типами документов и ЦИКЛОМ РАЗРАБОТКИ. В таблице DDD.1 представлен возможный порядок реализации требований документов на этапах ЦИКЛА РАЗРАБОТКИ.

Одним из необходимых документов является СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ. Она содержит приведенные ниже статьи по всем этапам соответственно:

Номер пункта по настоящему дополнительному стандарту

- выявленные ОПАСНОСТИ и вызвавшие их причины 52.204.3.1.10;
- оценка РИСКА. 52.204.3.2.5;
- требования к управлению РИСКОМ 52.204.4.5;
- ссылка на методы ТЕХНИЧЕСКОГО КОНТРОЛЯ и его результаты . . . 52.209.3;
- оценка по эффективности управления РИСКОМ. . . . . 52.204.4.6.

Таблица DDD.1 — Возможный порядок реализации требований документов на этапах ЦИКЛА РАЗРАБОТКИ

Реализуемое требование	Этап							
	1	2	3	4	5	6	7	8
Выявленные ОПАСНОСТИ и вызвавшие их причины 52.204.3.1.10	*	*	*					
Оценка РИСКА 52.204.3.2.5	*	*	*					
Требования к управлению РИСКОМ 52.204.4.5	*	*	*					
План управления РИСКОМ. 52.202	*							
ЦИКЛ РАЗРАБОТКИ 52.203	*							
Техническое задание на ПМЭС 52.206	*							
План ТЕХНИЧЕСКОГО КОНТРОЛЯ. 52.209.2	*							
План проверки на СООТВЕТСТВИЕ 52.210.2	*	*						
Требования к техническому заданию на подсистему (например, ПЭПС) 52.206		*						
Техническое задание на архитектуру ПМЭС 52.207.2		*						
Техническое задание на архитектуру ПЭПС 52.207.2			*					
Техническое задание на конструкцию подсистемы 52.208.1			*					
Техническое задание на испытания подсистемы 52.208.1			*	*				
Методы и результаты ТЕХНИЧЕСКОГО КОНТРОЛЯ. 52.209.3				*	*	*	*	
Методы и результаты проверки на СООТВЕТСТВИЕ. 52.210.6								*
Оценка эффективности методов управления РИСКОМ 52.204.4.6								*
ОСТАТОЧНЫЙ РИСК 6.8.201								*
Результаты оценки 52.212								*
СВОДКА ДАННЫХ ПО УПРАВЛЕНИЮ РИСКОМ 52.201.3	*	*	*	*	*	*	*	*

*) Предлагаемый для данного этапа документ по указанному пункту настоящего дополнительного стандарта.

ПРИЛОЖЕНИЕ EEE
(справочное)

Примеры структур ПМЭС/ПЭПС

ПМЭС может быть очень простым МЕДИЦИНСКИМ ЭЛЕКТРИЧЕСКИМ ИЗДЕЛИЕМ или сложной МЕДИЦИНСКОЙ ЭЛЕКТРИЧЕСКОЙ СИСТЕМОЙ. Кроме того, ПМЭС может быть чем-то средним между двумя упомянутыми типами.

На рисунке EEE.1 показаны некоторые возможные примеры ПМЭС.

На рисунке EEE.1 *а*) изображена комплексная система. ПМЭС разбита на ряд основных подсистем, которые в свою очередь состоят из подсистем, включающих ПЭПС.

На рисунке EEE.1 *б*) показана более простая схема. В этом случае уровень промежуточных основных подсистем опущен, а ПЭПС является подсистемой ПМЭС.

На рисунке EEE.1 *с*) изображена самая простая схема ПМЭС.

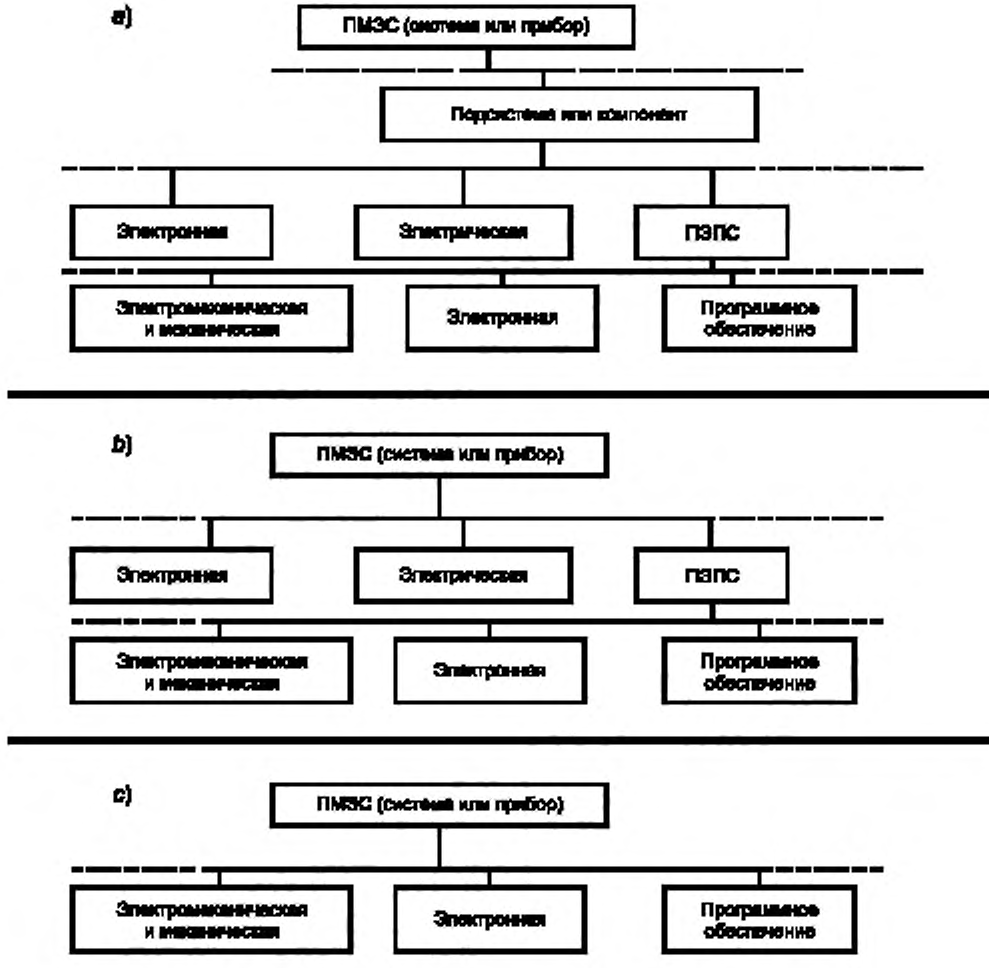


Рисунок EEE.1 — Примеры структуры ПМЭС/ПЭПС

ПРИЛОЖЕНИЕ FFF
(справочное)

Библиография

В настоящем приложении приведен список документов, которые служат руководством для методов по управлению РИСКОМ.

МЭК 513—94* Основные аспекты, нормированные в стандартах по безопасности ИМЭ

МЭК 812—85* Методика анализа надежности систем. Методика режимов нарушения и анализ воздействий (FMEA)

МЭК 880—86* Программное обеспечение компьютеров в системах безопасности атомных электростанций

МЭК 1025—90* Анализ дерева неисправностей (FTA)

МЭК 1508 (в стадии разработки) Функциональная безопасность. Системы, связанные с безопасностью

ИСО/МЭК 12119—94* Информационные технологии. Пакеты программного обеспечения. Требования к качеству и испытания

ИСО/МЭК 15026 (в стадии разработки) Системы и уровень целостности программного обеспечения

Проект ЕН 1441* (в стадии разработки) Медицинские устройства/Анализ риска

* Международные стандарты — во ВНИИКИ Госстандарта России.

УДК 615.84:006.354 ОКС 11.040.01 35.240.80 13.260 Р07 ОКП 50 8000

Ключевые слова: изделия медицинские электрические, безопасность, программируемые медицинские электронные системы, риск, цикл разработки, анализ риска, управление риском

Редактор *Т.С. Шеко*
Технический редактор *О.Н. Власова*
Корректор *В.С. Черная*
Компьютерная верстка *А.Н. Золотаревой*

Изд. лиц. № 02354 от 14.07.2000. Сдано в набор 12.09.2000. Подписано в печать 16.11.2000. Усл.печ.л. 2,32. Уч.-изд.л. 2,15. Тираж 204 экз. С 6226. Зак. 1029.

ИПК Издательство стандартов, 107076, Москва, Колодезный пер., 14.
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. "Московский печатник", 103062, Москва, Лялин пер., 6.
Плр № 080102

gost.e-ecolog.ru