ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56849— 2015/ ISO/TR 17791:2013

Информатизация здоровья

РУКОВОДСТВО ПО СТАНДАРТАМ БЕЗОПАСНОСТИ МЕДИЦИНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(ISO/TR 17791:2013, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного перевода русский язык англоязычной версии международного документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 468 «Информатизация здоровья» при ЦНИИОИЗ Минздрава — постоянным представителем ИСО ТК 215

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 декабря № 2241-ст

4 Настоящий стандарт идентичен международному документу ISO/TR 17791:2013 «Информатизация здоровья. Руководство по стандартам безопасности медицинского программного обеспечения» (ISO/TR 17791:2013 «Health informatics — Guidance on standards for enabling safety in health software», IDT)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Январь 2019 г.

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

© ISO, 2013 — Все права сохраняются
© Стандартинформ, оформление, 2016, 2019

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Термины и определения 2
3 Сокращения 4
4 Безопасность медицинского программного обеспечения 5
4.1 Инциденты, связанные с безопасностью медицинского программного обеспечения 5
4.2 Определения медицинского программного обеспечения 6
4.3 К более безопасному медицинскому программному обеспечению 7
4.4 Жизненный цикл медицинского программного обеспечения 7
4.5 Метод выбора стандартов для оценки 10
4.6 Стандарты, оценка которых выполнена в настоящем стандарте 11
4.7 Менеджмент рисков 13
4.8 Человеческий фактор 15
4.9 Уровень детализации 16
5 Оценка стандартов и руководящие указания 16
5.1 Оценка стандартов 16
5.2 Распределение стандартов по их применению для стадий жизненного цикла и уровню детализации, рассматриваемого в них программного обеспечения 28
5.3 Анализ неохваченных и повторно рассмотренных вопросов при оценке стандартов 31
5.4 Стандарты по обеспечению безопасности медицинского программного обеспечения. Руководство по реализации и использованию 34
Приложение А (справочное) Повышение безопасности пациентов благодаря инвестициям в разработку медицинских программ 37
Приложение В (справочное) Анализ стандартов с позиции жизненного цикла программного обеспечения 38
Приложение С (справочное) Информация об области применения стандартов СТК 1, касающихся безопасности 42
Библиография 44

Введение

Повышение безопасности пациентов

Безопасность пациентов является одной из основных общемировых проблем в здравоохранении. Как отмечается в публикации ИСО/ТК 215 «Сводный отчет экспертной группы по качеству обслуживания и безопасности пациента» (ISO/TC215 Summary Report from the Task Force on Patient Safety and Quality) 2010 г., прошло более десяти лет с момента выпуска фундаментальной публикации в 1999 г. «Человеку свойственно ошибаться: создание более надежной системы здравоохранения» Института медицины (ИМ) [1], [2].

С 1999 г. безопасность пациентов являлась объектом пристального внимания во время обсуждения и принятия решения на национальном и международном уровнях. Появились передовые практические решения в области обеспечения безопасности пациентов, связанные с созданием документов, описывающих первопричины риска, а также методы его анализа, предотвращения и ослабления. Эти решения повлияли на национальные и общемировые подходы к повышению безопасности пациентов. Образовательные программы, национальные кампании, первостепенные задачи местных больниц, неблагоприятные события и инструменты создания отчетов об аварийных событиях, обучение менеджменту рисков и программы аттестации практикующих врачей по безопасности являются примерами постоянной работы по формированию культуры повышения безопасности пациентов и улучшению качества.

Такое внимание к безопасности пациентов стимулировало инвестирование в интероперабельные системы электронного медицинского архива (ЭМА) и средства поддержки принятия решений, такие как автоматизированная система назначения лечения (АСНЛ) (компьютеризированный ввод заказа врача). Эти инвестиции в конечном счете позволят избежать, если не снизить, частоту возникновения инцидентов, угрожающих безопасности пациентов, вызванных такими факторами, как взаимодействие препаратов.

Информатизация здоровья может как снизить существующие, так и добавить новые риски обеспечения безопасности пациентов

Информатизация здоровья и связанные с ней электронные медицинские системы имеют значительные возможности для устранения, снижения или ослабления установленных угроз безопасности пациента и качеству обслуживания (см. приложение А) и являются на данный момент объектами для крупных инвестиций в здравоохранение.

Любое крупное преобразующее технологическое изменение, внедренное в промышленность, особенно в такую сложную и изменяющую жизнь область, как здравоохранение, будет иметь как предсказуемые, так и непредвиденные последствия. Непредвиденные последствия могут быть как положительными (например, способствовать развитию новых возможностей для совместной работы клинических врачей в качестве пользователей, работающих с новой технологией, и тем самым улучшению клинического процесса), так и отрицательными (например, появление новых рисков, возникающих при разработке, реализации или использовании технологии в сложных клинических условиях).

Хотя польза информатизации здоровья для обеспечения безопасности пациентов получает все большее признание, существуют риски случайных и неблагоприятных событий, вызванных реализациями медицинского программного обеспечения, и эти риски становятся все более очевидными. Так как разворачиваются все более сложные реализации медицинского программного обеспечения, которые обеспечивают более высокий уровень поддержки принятия решений и интегрируют данные пациентов различных систем в различных организациях и различных предоставленных медицинских услуг, то безопасность пациента повышается наряду с возникновением рисков неблагоприятных событий, вызванных программным обеспечением.

В ИТ-программе Национальной службы здравоохранения Англии (НСЗ) «Connecting for Health» создан упреждающий процесс управления инцидентами, связанными с безопасностью, для решения вопросов, связанных с безопасностью программного обеспечения [3]. За пятилетний период с 2006 г. по 2010 г. зарегистрировано и изучено 708 сообщений об инцидентах. Установлено, что примерно 80 % этих инцидентов представляли некоторую угрозу безопасности пациентов (4.1).

Стандарты, направленные на обеспечение безопасности медицинского программного обеспечения. Текущие разработки

Вопрос безопасности медицинского программного обеспечения впервые затронут в ИСО/ТК 215 в 2006 г., когда началась работа над следующими стандартами:

- ISO/TS 25238:2007 Health informatics — Classification of safety risks from health software (Информатизация здоровья. Классификация угроз для безопасности, вызванных медицинским программным обеспечением), и

- ISO/TR 27809:2007 Health informatics — Measures for ensuring patient safety of health software (Информатизация здоровья. Меры обеспечения безопасности пациента при использовании медицинского программного обеспечения).

ISO/TS 25238 направлен на определение концепции и требований для стадий жизненного цикла программного обеспечения, где необходимо понять в общих чертах, каким будет класс риска предложенной системы. Несмотря на то что ISO/TS 25238 включает примеры категорий степени тяжести и вероятности риска, а также демонстрационную матрицу риска, которые могут иметь более широкое использование, его применение при проектировании медицинского программного обеспечения или снижение любых выявленных рисков до приемлемого уровня не является задачей этого стандарта.

В ISO/TR 27809 дан обзор классификаций продуктов медицинского программного обеспечения, обсуждаются варианты мер управления, связанные с таким программным обеспечением, схема классификации риска, описанная в ISO/TS 25238, а также идентификация национальных и международных стандартов по менеджменту рисков.

В течение многих лет сообщество, образовавшееся вокруг медицинского оборудования, поддерживало разработку стандартов на программное обеспечение в МЭК/ТК 62 ПК А [Общие аспекты электрооборудования, используемого в медицинской деятельности (Common aspects of electrical equipment used in medical practice)], в ИСО/ТК 215 [Информатизация здоровья (Health informatics)] и в ИСО/ТК 210 [Менеджмент качества и соответствующие общие аспекты медицинских приборов (Quality management and corresponding general aspects for medical devices)]. Несколько других технических комитетов ИСО и МЭК, таких как ИСО/МЭК СТК 1 подкомитет 7 [Разработка систем и программного обеспечения (Software and systems engineering)], создавали стандарты по разработке систем и программного обеспечения начиная с конца 1980-х гг.

Действующие в настоящее время стандарты по медицинскому оборудованию сосредоточены на функциональности и испытании установленного медицинского оборудования и включают в себя стандарты на «программное обеспечение как медицинский прибор» [в МЭК 62304 Медицинское программное обеспечение устройства. Процессы жизненного цикла программного обеспечения (IEC 62304:2006, Medical device software — Software life cycle processes). «Программное обеспечение как медицинский прибор» определяется как «система программного обеспечения, которая разработана с целью включения в разрабатываемый медицинский прибор или предназначена для самостоятельного использования в качестве медицинского прибора»]. Основные стандарты, разработанные или приведенные в качестве справочного материала, используемые для обеспечения безопасности медицинских приборов и программного обеспечения для медицинских приборов, включают:

- ISO 13485:2003, Medical devices — Quality management systems — Requirements for regulatory purposes (Медицинские приборы. Системы менеджмента качества. Требования для целей регулирования);

- ISO/TR 14969:2004, Medical devices — Quality management systems — Guidance on the application of ISO 13485:2003 (Медицинские приборы. Системы менеджмента качества. Руководство по применению ИСО 13485:2003);

- IEC 62304:2006, Medical device software — Software life cycle processes (Программное обеспечение медицинских приборов. Процессы жизненного цикла программного обеспечения);

- ISO 14971:2007, Medical devices — Application of risk management to medical devices (Медицинские приборы. Применение менеджмента риска к медицинским приборам);

- IEC 80001-1:2010, Application of risk management for IT networks incorporating medical devices, Part 1: Roles, responsibilities and activities (Применение менеджмента рисков для ИТ-сетей с медицинскими приборами. Часть 1. Роли, ответственности и деятельность).

В центре внимания данных стандартов отражена заинтересованность медицинского приборостроения в предпродажных (т. е. проектирование и разработка) стадиях жизненного цикла приборов с программным обеспечением, включая программное обеспечение и медицинские приборы, работающие самостоятельно. Недавнее дополнение IEC/TR 80001-1 является признаком растущего внимания к подключению приборов к физической сети.

Поскольку понимание того, какое программное обеспечение считается самостоятельным медицинским изделием, существенно различается в разных странах, настоящий стандарт дает представление о передовых практических методах обеспечения безопасной разработки, внедрения и эксплуатации медицинского программного обеспечения независимо от того, работает ли оно как медицинское изделие.

Настоящий стандарт рассматривает стандарты, которые могут предоставить полезное руководство для покупателей, специалистов по внедрению и пользователей, а также для разработчиков и производителей вплоть до конфигурирования, реализации и текущего использования при любых настройках и условиях работы. Анализ и рекомендации, представленные в настоящем стандарте, указывают, что медицинское программное обеспечение все чаще внедряется и эксплуатируется в сложной среде «экосистемы» или «социально-технологической системы», где программное обеспечение тесно связано с другими системами, технологиями, инфраструктурами и предметными областями (людьми, организациями и внешними условиями) и где оно также должно быть сконфигурировано, чтобы поддерживать локальные клинические и бизнес-процессы.

Следовательно, повышение безопасности пациента и риски, связанные с реализацией отдельных программных компонентов, должны оцениваться и управляться в рамках контекста реализуемой информационной структуры организации, используя стандарты и проверенные процессы, которые направляют и вовлекают как специалистов по информатизации здоровья, так и врачей на всех стадиях, а также используя семейство стандартов, которые обеспечивают безопасность медицинского программного обеспечения.

Раздел 4 рассматривает вопросы, связанные с обеспечением условий безопасности, и предоставляет концептуальный подход для оценки стандартов вместе с кратким описанием соответствующих стандартов.

Раздел 5 построен на этом основополагающем подходе, предоставляя аналитические оценки того, какие стандарты являются наиболее подходящими для различных стадий жизненного цикла программного обеспечения. В данном разделе также идентифицируются существующие проблемы и содержится практическое руководство по стандартам, представляющим передовые практические методы. Важно отметить, что, несмотря на то что нормативные документы, рассмотренные в настоящем стандарте, могут быть полезны для обеспечения безопасности медицинского программного обеспечения, во многих случаях они не были подготовлены специально для этой цели.

Кому следует ознакомиться с настоящим стандартом?

Общий вопрос красной нитью проходит через все обсуждения безопасности медицинского программного обеспечения: «Какие стандарты должны использоваться для того, чтобы обеспечить безопасность медицинского программного обеспечения?» Настоящий стандарт предназначен для национальных комитетов-членов и пользователей, которые ищут ответ на этот вопрос.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

РУКОВОДСТВО ПО СТАНДАРТАМ БЕЗОПАСНОСТИ МЕДИЦИНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Health informatics. Guidance on standards for enabling safety in health software

Дата введения — 2016—11—01

1 Область применения

Настоящий стандарт предоставляет руководящие указания для национальных комитетов-членов (НКЧ) и пользователей путем выявления связанного набора международных стандартов, имеющих отношение к разработке, реализации и использованию безопасного медицинского программного обеспечения. Подход, представленный в настоящем стандарте, вместе с отображением стандартов в этом подходе иллюстрирует соответствующие стандарты и их оптимальное применение. Такое отображение ясно демонстрирует, где существуют пробелы и совпадения в стандарте. В частности, настоящий стандарт:

- определяет связанный набор международных стандартов, которые поддерживают безопасную для пациента (или более безопасную) разработку, внедрение и использование медицинского программного обеспечения;
- дает представление о применимости этих стандартов для достижения оптимальной безопасности медицинского программного обеспечения в рамках методов всеобщего менеджмента риска и менеджмента качества, а также в рамках стадий жизненного цикла и процессов разработки медицинского программного обеспечения;
- решает вопросы безопасности медицинского программного обеспечения, которые остаются нерассмотренными или дублируются в рассматриваемых стандартах;
- рассматривает, как эти пробелы и дублирование можно устранить (за короткий или длительный срок) путем пересмотра действующих стандартов или разработки новых.

Вред, наносимый операторам медицинским программным обеспечением, если такой риск существует, выходит за рамки настоящего стандарта.

Несмотря на ссылки, касающиеся норм и правил для медицинского программного обеспечения, имеющиеся в настоящем стандарте, установление, обеспечение исполнения и подтверждение норм и правил не является ни целью, ни намерением настоящего стандарта. Это в первую очередь является зоной национальной ответственности или ответственности юрисдикции и не входит в область применения настоящего стандарта. Тем не менее настоящий стандарт не стремится создать такую структуру международных стандартов, которая будет всемирно признана и принята, а также дать указания, с помощью которых органы юрисдикции в составе НКЧ смогут решить, есть ли необходимость реализации данного подхода на нормативной основе. Поэтому, несмотря на то что поддержка НКЧ в их стремлении к гармонизации среды норм и правил могла бы быть эффективной, она не является целью или намерением настоящего стандарта.

Кроме того, если некоторый стандарт рекомендован для использования в настоящем стандарте, то это не означает, что требуется полное соблюдение всех требований такого рекомендованного стандарта. Поэтому соответствие требованиям также не входит в задачу настоящего стандарта.

Издание официальное

2 Термины и определения

В соответствии с целями и задачами настоящего стандарта применены следующие термины с соответствующими определениями:

2.1 **общий подход** (framework): Неотъемлемая поддерживающая или лежащая в основе структура.

[ИСО 9001:2008]

2.2 **степень структурированности** (granularity): Уровень сложности или то, до какой степени система поделена на более мелкие части.

Примечание — Несмотря на то что определение для термина «степень структурированности» можно найти в ИСО 17115 Информатизация здоровья. Словарь терминологических систем, оно не касается области применения и контекста настоящего стандарта.

2.3 **вред** (harm): Смерть, телесное повреждение и/или ущерб, причиненный здоровью или состоянию пациента.

[Руководство ИСО/МЭК 51:1999 измененное]

2.4 **опасность** (hazard): Потенциальный источник вреда.

[Руководство ИСО/МЭК 51:1999]

2.5 **информатизация здоровья** (health informatics): Пересечение клинических практик, практик ИМ/ИТ (информационный менеджмент, информационные технологии) и методик управления для достижения наилучшего качества здравоохранения.

Примечание — Информатизация здоровья включает в себя применение информационных технологий для облегчения создания и использования данных, информации и знаний, связанных со здравоохранением. Информатизация здоровья обеспечивает условия и поддерживает все аспекты медицинского обслуживания. [ИСО/ТК 215 Отчет рабочей группы организации (Organization Task Force Report) (план) — по материалам

gost.e-ecolog.ru

2.6 **медицинское программное обеспечение** (health software): Программное обеспечение, используемое в здравоохранении, способное оказывать влияние на здоровье и предоставление медицинских услуг субъекту оказания медицинской помощи.

Примечание — Включает следующее:

- программное обеспечение в исходной форме, которое включает в себя системы, элементы и модули (см. МЭК 62304);
- связанные системы кодирования, механизмы логического вывода, архетипы и онтологии;
- сопроводительная документация, необходимая для внедрения, использования и обслуживания программного обеспечения;
- программное обеспечение, которое используется эффективно или применяется в любой части сектора здравоохранения, в том числе во всех государственных и частных организациях или предприятиях, а также у конечных потребителей;
- программное обеспечение, которое приобретается на коммерческих и некоммерческих условиях.

2.7 **жизненный цикл** (lifecycle): Развитие системы, изделия, услуги, проекта или других изготовленных человеком объектов, начиная со стадии разработки концепции и заканчивая выводом из эксплуатации.

Примечание — В ИСО/МЭК 12207 (предыдущая редакция) модель жизненного цикла программного обеспечения определена как «концептуальная основа, используемая для организации и управления развитием, работой, техническим обслуживанием и действиями по выводу из эксплуатации программного обеспечения». В ИСО/МЭК 12207 также отмечается, что «модели жизненного цикла используются для управления развитием программного обеспечения от начала их создания и до прекращения их службы».

[ИСО/МЭК 12207:2008]

2.8 **медицинский прибор** (medical device): Любой прибор, устройство, приспособление, машина, аппарат, имплантат, лабораторный реагент или калибратор, программное обеспечение, материал или другие подобные или связанные с ними изделия:

а) предполагаемые производителем для применения к человеку, отдельно или в сочетании друг с другом для одной или более заданных целей, таких как:

- диагностика, профилактика, контроль, лечение или облегчение течения заболеваний,
- диагностика, контроль, лечение, облегчение травмы или компенсация последствий травмы,
- исследование, замещение, изменение или поддержка анатомического строения или физиологических процессов,

- поддержание и сохранение жизни,
- предупреждение беременности,
- дезинфекция медицинских приборов,
- предоставление информации для медицинских или диагностических целей посредством лабораторных исследований проб, полученных из тела человека; и

b) не реализующие свое основное предназначение в или на теле человека с помощью фармакологических, иммунологических или метаболических средств, но такие средства могут помочь в реализации намеченной для человека функции.

Примечания

1 Определение прибора для лабораторных исследований включает, например, реагенты, калибраторы, приборы забора и хранения образцов, контрольные материалы и связанные с этим инструменты и приспособления. Данные, полученные с помощью такого лабораторного диагностического прибора, могут использоваться в целях диагностики, контроля или совместимости. В некоторых юрисдикциях отдельные приборы лабораторной диагностики, включая реагенты и подобные им, могут подчиняться отдельным правилам и положениям.

2 Изделия, которые в некоторых юрисдикциях могут рассматриваться как медицинские приборы, но для которых еще не существует согласованного подхода в этом вопросе, — это:

- средства помощи инвалидам и людям с ограниченными возможностями;
- приборы для лечения/диагностики болезней и травм животных;
- аксессуары для медицинских приборов (см. примечание 3);
- дезинфицирующие вещества;
- приборы, использующие ткани животных и людей, которые могут соответствовать описанным выше определениям, но находятся в ведении других органов управления.

3 Аксессуары, специально предназначенные производителями для использования совместно с медицинским прибором, для которого они разработаны, реализующие цели медицинского прибора, должны подчиняться тем же процедурам GHT (Целевая группа глобальной гармонизации), которые применяются к самому медицинскому прибору. Например, аксессуар классифицируется так, как будто он является медицинским прибором. Это может привести к другой классификации аксессуара, отличной от его «исходной» классификации.

4 Компоненты медицинских приборов в общем случае контролируются через систему менеджмента качества производителя и процедуры оценки соответствия прибора. В некоторых юрисдикциях компоненты включаются в определение «медицинский прибор».

[Специальная группа по глобальной гармонизации (GHTF) Исследовательская группа 1: 2005]

2.9 **риск** (risk): Сочетание вероятности причинения вреда и его последствий.

[ИСО 14971:2007]

2.10 **применимость риска** (risk applicability): Отношение, обоснованность и уместность риска в определенном контексте.

2.11 **менеджмент риска** (risk management): Систематическое применение менеджмента политик, процедур и методик при выполнении задач по анализу, оцениванию и управлению рисков.

[ИСО 14971:2007]

2.12 **распределение риска** (risk sharing): Форма обработки риска путем соглашения о распределении риска с другими вовлеченными сторонами.

Примечания

1 Законодательные или нормативные требования могут ограничивать, запрещать или делать обязательным распределение риска.

2 Распределение риска может проводиться с помощью договора страхования или других видов договоров.

3 Степень распределения риска может зависеть от надежности и четкости договоренностей о распределении.

4 Передача риска является формой распределения риска.

[Руководство ИСО 73:2009]

2.13 **обработка риска** (risk treatment): Процесс преобразования риска.

Примечания

1 Обработка риска может включать:

- предотвращение риска путем принятия решения не начинать или не продолжать деятельность, которая приводит к риску,
- принятие или повышение риска с целью реализации возможностей,
- удаление источника риска,
- изменение вероятности возникновения,
- изменение последствий,
- распределение риска с другим лицом или лицами (включая договоры и финансирование риска) и
- сохранение за собой риска путем принятия обоснованного решения.

2 Обработку риска, который касается негативных последствий, иногда называют «смягчение последствий рисков», «устранение рисков», «предотвращение рисков» и «снижение рисков».

3 Обработка риска может привести к возникновению новых рисков или изменению существующих.

[Руководство ИСО 73:2009]

2.14 **безопасность** (safety): Отсутствие неприемлемых рисков.

Примечание — Роль медицинского программного обеспечения в способствовании возникновению ятрогенного вреда пациентам может быть прямой (т. е. проект не отвечает требованиям заданного применения) или косвенной (т. е. выполняется соответствие проекта требованиям заданного применения, однако система не настроена должным образом). Для безопасности пациентов это означает снижение риска причинения вреда, связанного с медицинским программным обеспечением до приемлемого минимума. Данный контекст, используемый в определении, находится на стадии активного рассмотрения Всемирной организацией здравоохранения.

[Руководство ИСО/МЭК 51:1999]

2.15 **стандарт** (standard): Документ, созданный по общему согласию и утвержденный признанным органом, который обеспечивает правила, инструкции или характеристики различных видов деятельности или их результатов, направленные на достижение оптимальной степени порядка в заданном контексте, для общего и многократного использования.

Примечания

1 Международные стандарты ИСО являются соглашениями. Стандарты ИСО относятся к соглашениям, поскольку члены этой организации должны договориться о содержании и давать формальное одобрение, перед их публикацией. Международные стандарты ИСО разрабатываются техническими комитетами. Члены этих комитетов — представители разных стран. Таким образом, международные стандарты ИСО, как правило, имеют очень широкую поддержку.

2 Стандарты должны основываться на консолидированных результатах науки, техники, опыта и должны быть направлены на достижение оптимальных положительных результатов для сообщества.

[Руководство ИСО/МЭК 2:2004]

2.16 **субъект оказания медицинской помощи** (subject of care): Человек, которому должны предоставить, предоставляют или уже предоставили медицинское обслуживание.

Примечание — Субъектом оказания медицинской помощи считается и здоровый человек.

[ИСО 18308:2011]

3 Сокращения

ЕКС	—	Европейская комиссия по стандартизации;
ЕКСЭЛ	—	Европейский комитет по стандартизации в области электротехники;
COCIR	—	Европейский координационный комитет по радиологической, электромедицинской и медицинской ИТ-отраслям;
АСНЛ	—	автоматизированная система назначения лечения;
DICOM	—	формирование цифровых изображений и обмен ими в медицине;
ЭМА	—	электронный медицинский архив;
ЭМК	—	электронная медицинская карта;
FDA	—	управление по контролю продуктов и лекарств;
GCM	—	модель базового компонента;
GHTF	—	специальная группа по глобальной гармонизации;
ИЗ	—	информатизация здравоохранения (медицинская информатика);
ИКТ	—	информационно-коммуникационные технологии;
СМИБ	—	система менеджмента информационной безопасности;
ITIL	—	библиотека инфраструктуры информационных технологий;
ЛИС	—	лабораторная информационная система;
НСЗ	—	национальная служба здравоохранения;

НКЧ — национальный комитет-член;
PACS — системы передачи и архивирования изображений;
СМК — система менеджмента качества;
ЦРПО — жизненный цикл разработки программного обеспечения;
ОРС — организация — разработчик стандартов;
СУЗС — средство управления знаниями стандарта;
UCD — проектирование с ориентацией на пользователя;
ВОЗ — Всемирная организация здравоохранения.

В ИТ-программе НСЗ Англии «Connecting for Health» создан упреждающий процесс управления инцидентами, связанными с безопасностью, для решения вопросов, связанных с безопасностью программного обеспечения [3]. За пятилетний период с 2006 по 2010 гг. зарегистрировано и изучено 708 сообщений об инцидентах. Установлено, что примерно 80 % этих инцидентов представляли некоторую угрозу безопасности пациентов (4.1).

4 Безопасность медицинского программного обеспечения

4.1 Инциденты, связанные с безопасностью медицинского программного обеспечения

В рамках ИТ-программы НСЗ Англии «Connecting for Health» реализован упреждающий процесс менеджмента инцидентами, связанными с безопасностью, для решения вопросов безопасности программного обеспечения в Англии. За пятилетний период с 2006 по 2010 гг. зарегистрировано и изучено 708 сообщений об инцидентах. Обнаружено, что примерно 80 % этих инцидентов представляют некоторую угрозу для безопасности пациентов. Реализован план мероприятий по устранению этих инцидентов, который делает их безопасными в течение 24 ч. Другие страны либо не имеют конкретных данных, либо находятся на ранних стадиях сбора и проверки данных об инцидентах связанного с безопасностью медицинского программного обеспечения, или действительно имеют научные знания, основанные на исследованиях [4], [5]. Данные НСЗ указывают на возможность причинения вреда пациентам, а также на возможность возникновения непредвиденных последствий для безопасности пациентов, исходящих от медицинского программного обеспечения. Вероятность того и другого была бы гораздо выше, если бы НСЗ не разработала и не провела активную кампанию по менеджменту рисков для безопасности программного обеспечения.

Примеры инцидентов, связанных с безопасностью, из Великобритании и других стран включают в себя следующее:

- система либо не может передать пациенту сигнал тревоги, либо не поддерживает и не обновляет такие сигналы так, чтобы они отражали новые протоколы лечения пациента;
- ошибки отображения названия препарата и другие ошибки, связанные с клинической терминологией, особенно в тех случаях, когда данные интегрированы из различных лечебных учреждений, информационных систем или организаций;
- неверно вычисленный возраст пациентов, например для предродовой рентгеноскопии или иммунизации;
- дозы лучевой терапии либо лекарственного препарата, которые рассчитаны, представлены либо неправильно сообщены в связи с расчетом или ошибкой при переводе единиц измерения;
- врачи неправильно интерпретируют клинические данные, представленные им через интерфейс другой системы без предоставления полного контекста этих данных;
- аннотации к медицинскому изображению, которое отображено в неправильном положении;
- потеря данных из профилей пациентов без уведомления врачей из-за недоступности или неправильной технической поддержкой исходных систем или интерфейсов;
- изображения не были своевременно извлечены врачами из системы хранения и передачи изображений (PACS);
- ошибки миграции данных при приведении в действие новых систем или обновлении основных систем;
- ошибки технической поддержки программного обеспечения, приводящие к изменению идентификации пациента, что впоследствии приводит к тому, что результаты лабораторных обследований направляются не к тем врачам;

- правила поддержки принятия клинических решений не были инициированы в правильном порядке, так как некоторые исходные данные были записаны в другом контексте или неправильно преобразованы;

- нарушения безопасности, которые повреждают целостность или доступность системы;

- повышенная неготовность работы системы.

Так как инциденты, касающиеся безопасности пациента и связанные с медицинским программным обеспечением, выступающим в качестве основного или сопутствующего фактора, зачастую не регистрируются никакой системой, то в настоящее время разработка передовых практических методов, систем оповещения и формирование повышенной культуры безопасности медицинского программного обеспечения так же важны для информатизации здоровья, как были важны для обеспечения безопасности пациентов в клинической деятельности еще в 2000-е годы. Учитывая возрастающую сложность медицинского программного обеспечения, связанную с компонентно-ориентированными подходами, с ориентированными на сервис архитектурами, интеграцией систем между организациями, сложной терминологией и с более высоким уровнем локальной конфигурируемости и алгоритмов поддержки принятия решений, — эффективность, а также сопутствующие риски, скорее всего, будут продолжать расти. В связи с необходимостью четких руководящих указаний и согласованного набора стандартов для медицинских организаций, поставщиков и других заинтересованных сторон крайне важно действовать согласованно для обеспечения безопасных, поддерживаемых реализаций программного обеспечения, а также для создания и развития высокой культуры безопасности медицинского программного обеспечения.

4.2 Определения медицинского программного обеспечения

Определения программного обеспечения, в частности программных элементов, программных систем и программных модулей, предоставлены на основе нескольких стандартов, включая ИСО/МЭК 90003:2004 и МЭК 62304:2006. Эти общие определения особенно эффективны при решении проблем построения структур, однако существует постоянная дихотомия, появляющаяся при применении определений программного обеспечения к медицине. Это деление проводит различие между программным обеспечением, которое по определению является медицинским прибором, и медицинским программным обеспечением, которое не является медицинским прибором:

- первое из вышеупомянутых является определением *программного обеспечения медицинского прибора*: «Система программного обеспечения, которая разработана с целью включения в медицинский прибор или предназначена для использования в качестве медицинского прибора самостоятельно» (см. IEC/TR 80001-1:2010 с изменениями 3.12 МЭК 62304:2006), и

- второе является определением медицинского программного продукта: «Программное обеспечение, предлагаемое для применения в сфере здравоохранения в целях защиты здоровья, но за исключением программного обеспечения, необходимого для надлежащего применения медицинского прибора» (см. 2.3 ISO/TS 25238:2007).

Если исходить из правил применения медицинского оборудования во всем мире, определение программного обеспечения как медицинского прибора может отличаться в определенных регламентах и меняться с течением времени.

Подход настоящего стандарта состоит в применении определения программного обеспечения, используемого в здравоохранении, которое охватывает любое программное обеспечение, оказывающее влияние на обслуживание пациента, независимо от того, считается ли оно программным обеспечением для медицинского прибора. Как отмечалось Европейским координационным комитетом по радиологической, электромедицинской отрасли и информационным технологиям в здравоохранении (COCIR) о медицинском программном обеспечении в контексте международной стандартизации, комитет COCIR требует, чтобы комитеты, например МЭК/ТК 62 и ИСО/ТК 215, разрабатывали свои стандарты и другие публикации с максимально широкой областью применения.

Настоящий стандарт предназначен для медицинского программного обеспечения со следующими характеристиками:

- программное обеспечение в своей канонической форме, которая включает в себя системы, элементы и модули (см. МЭК 62304), которые включает в себя связанные с ними данные, хранящиеся в цифровой форме, например таблицы данных или наборы правил, системы кодирования, контентные модели, механизмы логических выводов, архетипы, онтологии, и связанные документы, необходимые для эксплуатации и обслуживания программного обеспечения;

- программное обеспечение, которое используется в сфере здравоохранения, то есть программное обеспечение, которое в любой стадии его жизненного цикла используется, потребляется, приносит выгоду или применяется в любой области сферы здравоохранения. В то же время понятие «предназначено для использования» также может быть применимо, понятие «используется» предполагает более широкое применение. Сфера здравоохранения включает в себя все государственные и частные организации или предприятия, которые обеспечивают охрану здоровья и медицинскую помощь лицам, в том числе медицинские услуги для потребителей (личные медицинские карты, приложения для смартфонов/планшетов и т. д.);

- программное обеспечение, которое включает в себя то, что является коммерчески и не коммерчески доступным.

Наглядными примерами медицинского программного обеспечения являются:

- реестры пациентов и база данных основных показателей пациентов, ЭМА и ЭМК;
- ЛИС;
- информационная система лекарственных препаратов;
- рентгенологическая информационная система;
- информационная система больницы;
- система назначения лечения и составления отчета о результатах;
- системы отслеживания и регистрации вакцинации;
- система планирования для пациентов, врачей или клинических ресурсов (например, для кабинетов врачей);
- системы коммунальной медико-социальной помощи;
- системы медицинской помощи на дому;
- личные медицинские карты;
- системы, связанные с психическим здоровьем, и системы для определенных заболеваний; и
- системы здравоохранения населения в той мере, в которой они ориентированы на отдельных лиц (например, прививки, оповещения, эпидемии и т. д.).

Необходимо отметить, что, так как среда электронной медицины все больше интегрируется, определение медицинского программного обеспечения, принятое в настоящем стандарте, включает системы администрирования пациентов, например планирование назначений и управление ресурсами.

Наглядными примерами программного обеспечения, которое не относится к медицинскому программному обеспечению в настоящем стандарте, являются:

- системы управления финансами, кадрами, материалами;
- обследование населения и системы обследования населения;
- системы стандартной обработки текста, электронных таблиц или системы программного обеспечения баз данных;
- системы телекоммуникаций и сетей.

4.3 К более безопасному медицинскому программному обеспечению

Группа стандартов, выявленных и оцененных в настоящем стандарте, рассматривает средства, позволяющие снизить риск и стремиться к более безопасному медицинскому программному обеспечению по мере применения этих стандартов. Программное обеспечение, являющееся безопасным для всех взаимодействий с пациентом, наряду с соответствующей целью и желательным конечным состоянием, никогда не обеспечивается гарантией ввиду невозможности устранения всех рисков. Поэтому подход, основанный на менеджменте рисков, используется для снижения всех рисков, связанных с медицинским программным обеспечением, до приемлемых уровней. Таким образом, основное внимание в подходе, основанном на риске, уделяется снижению, но необязательно устранению, рисков на протяжении всего жизненного цикла медицинского программного обеспечения. Это применимо к полному жизненному циклу медицинского программного обеспечения, как описано в 4.4, и способствует разработке, внедрению и эксплуатации более безопасного медицинского программного обеспечения.

4.4 Жизненный цикл медицинского программного обеспечения

Подход для оценки применимости и практической пользы стандартов, посвященных безопасности медицинского программного обеспечения, необходим для того, чтобы определить применимость, а также выявить пробелы среди стандартов, имеющихся в настоящее время.

Как правило, в роли моделей жизненного цикла программного обеспечения выступают концептуальные общие схемы, используемые для организации и управления разработками, эксплуатацией,

техническим обслуживанием и действиями по выводу из эксплуатации программного продукта с начала появления до окончательного прекращения работы программного обеспечения (см. ИСО/МЭК 12207:2008). Такие модели жизненного цикла предоставляют средства для проведения всеобъемлющего, полного исследования и оценки стандартов, содействующих повышению безопасности медицинского программного обеспечения.

В настоящем стандарте для содействия такому исследованию и оценке принят прагматический подход к моделям жизненного цикла. Следующие вопросы являются основополагающими при определении стадий жизненного цикла программного обеспечения:

- существует ли изменение риска на разных стадиях;
- существуют ли другие: профиль риска, характеристика менеджмента рисков или необходимость минимизации его последствий между стадиями; и
- существует ли вероятность распространения риска от одной стадии к другой.

Если ответ на любой из трех вышеперечисленных пунктов оказался положительным, то это может означать, что существует необходимость в использовании других стандартов, таким образом, существует необходимость в рассмотрении вышеуказанных вопросов при анализе рисков.

Стадии жизненного цикла, используемые в настоящем стандарте, основаны либо как минимум на одном или на нескольких стандартах, в которых уже определены такие стадии, либо если стадии не определены в известном стандарте, то он рассматривает изменения риска или другой профиль менеджмента рисков, характеристик, либо возникает необходимость в использовании разных стандартов, или констатируем наличие пробела в текущих используемых стандартах.

Процесс определения стадий жизненного цикла повторяется путем использования результатов анализа, взятых из «жизненного цикла работающего программного продукта» для разработки окончательного готового к использованию жизненного цикла программного обеспечения. В целом, наиболее полезно и эффективно выявление минимального количества стадий жизненного цикла, которых достаточно для осуществления достоверной оценки стандартами, содействующими безопасности медицинского программного обеспечения.

Необходимо отметить, что жизненный цикл программного обеспечения отличается от ЦРПО, несмотря на то что стандарты по ЦРПО предоставляют информацию для настоящего стандарта. Эти стадии жизненного цикла программного обеспечения не предполагают никакого конкретного ЦРПО.

Также в соответствии с целями настоящего стандарта следует отметить, что жизненный цикл программного обеспечения имеет как стадии, так и события:

- стадиями являются те компоненты жизненного цикла программного обеспечения, которые сопровождаются сопутствующими видами работ, назначенными ресурсами и результатами, и
- событиями считаются те компоненты, которые являются существенными явлениями, происходящими в данном месте и в данное время.

Стадии жизненного цикла медицинского программного обеспечения включают сложный набор последовательных и повторяющихся действий, которые вместе формируют непрерывный менеджмент этого программного обеспечения, осуществляемый всеми заинтересованными сторонами:

- разработчики отвечают за проектирование, разработку, производство и техническую поддержку медицинского программного обеспечения (также в некоторых стандартах называемые «производитель» или «поставщик»);
- специалисты по внедрению отвечают за установку и интеграцию программного обеспечения в клинических условиях (специалист по внедрению может быть разработчиком или владельцем),
- владельцами являются медицинские организации, закупающие программное обеспечение (и/или специалисты по внедрению управляемых услуг);
- операторы отвечают за предоставление медицинской услуги за счет использования медицинского программного обеспечения,
- пользователями являются лица, использующие медицинское программное обеспечение в клинических условиях, они могут включать, например, потребителей, если речь идет о личных медицинских картах.

Основываясь на вышеописанном подходе и информации, изложенной в приложении В, для оценки стандартов, обеспечивающих безопасность медицинского программного обеспечения, в следующих стадиях жизненного цикла предоставлено соответствующее разделение профиля рисков, характеристик, потребностей и допущений (см. таблицу 1).

Примечания

1 Данные стадии необязательно подразумевают линейное упорядочивание или строгую последовательность во времени.

2 По возможности, для описаний стадий жизненного цикла приведены ссылки; там, где это недоступно, описания стадий жизненного цикла носят лишь информативный характер.

Таблица 1 — Описания жизненного цикла в стандартах

Стандартная стадия жизненного цикла	Подстадия(и)[a]	Определение	Участник(и)[b]
Концепция	Документ	Формулировка, представление и определение исходного проекта, эстетики и основные функции программного обеспечения	Р, П
Требования	Документ	Требование является необходимостью, условием или обязательством. Оно может устанавливаться или предполагаться организацией, покупателями или другими заинтересованными сторонами [см. ИСО 9000]	Р
Проектирование	Документ	Является фазой разработки программного обеспечения, следующей за анализом, которая определяет, как должна быть решена проблема [SKMT — Глоссарий организации Canada Health Infoway]	Р
Разработка	Код, испытание, документ[c]	Проектирование и разработка представляет собой процесс (или набор процессов), использующий ресурсы для преобразования требований (входов) в характеристики или спецификации (результаты) изделий, процессов и систем[d]	Р
Производство		Обеспечение наличия изделия для покупателя или пользователя	Р
Выпуск	Распространение	Выпуск — это определенная версия конфигурационной единицы, которая предоставлена или выпущена для конкретной цели[e] [ИСО/МЭК 90003]	Р, В
Закупка		Покупка коммерчески доступного продукта или привлечение организации к производству «программного обеспечения, сделанного по заказу, или собственной разработки»	Р, В, ВО
Внедрение	Конфигурация оборудования, интеграция, размещение	Проверка на совместимость программного обеспечения и сертификация также могут быть включены в этап внедрения либо как первый этап, либо как этап перед установкой	Р, В, ВО
Ввод в действие		Полная активация некоторой системы, которая находилась на стадии разработки или функционировала в ограниченном тестовом режиме, так чтобы предполагаемые пользователи могли получить к ней доступ [Интернет-сайт AllWords.com]	В, П, ВО
Эксплуатация		Любое использование медицинского программного обеспечения при любых настройках, не предназначенных для испытания. Существует вероятность того, что для нового программного обеспечения может возникнуть интервал между вводом его в эксплуатацию и полным применением в клинических условиях	П, ВО
Клиническое применение		Стадия клинического применения программного обеспечения, на которой в клинике в полном объеме используется программное обеспечение, установленное в соответствии с определением медицинского программного обеспечения из настоящего стандарта, и ее «..влияние на здоровье и здравоохранение субъекта оказания медицинской помощи»	П, ВО
Техническая поддержка		Техническая поддержка при разработке программного обеспечения является модификацией программного продукта после поставки, с целью исправления ошибки, улучшения производительности и других характеристик [ИСО/МЭК 14764]	Р, В, П, ВО

Окончание таблицы 1

Стандартная стадия жизненного цикла	Подстадия(и)[a]	Определение	Участник(и)[b]
Вывод из эксплуатации		Система выводится из среды эксплуатации, и результаты работы системы и данные архивируются соответствующими способами[f]	Р, П, ВО
Окончательное удаление		Удаление и завершение работы имеющихся программных продуктов или служб системы, сохраняя при этом целостность работы организации [по материалам ИСО/МЭК 12207]	Р, П, ВО

[a] Не каждая стадия жизненного цикла имеет подстадию.
[b] Р — разработчик; В — специалист по внедрению; ВО — владелец-оператор; П — пользователь.
[c] Также именуемый «производитель».
[d] Проектирование и разработка могут рассматриваться как разные стадии отдельного интегрированного процесса проектирования и разработки или как два (или более) отдельных процесса (см. ИСО 9000, ИСО 9001 или ИСО 9004).
[e] Для данной стадии система и все связанные с ней продукты передаются покупателю или пользователю.
[f] Данные также могут быть перемещены или перенесены из одной системы в другую при сохранении семантической целостности.

Авторами настоящего стандарта признается, что «язык» жизненного цикла программного обеспечения, особенно в части, касающейся обеспечения безопасности медицинского программного обеспечения, не фиксирован. Признано считать, что формулировки и определения (если они отсутствуют в каком-либо документе ИСО или другом утвержденном стандарте) могут быть уточнены при дальнейшей разработке стандартов. Также принято считать, что имеются и другие модели программного обеспечения, например модель базовых компонентов (GCM) и связанный с ней комплекс стандартов [6]. Будущий или дальнейший анализ и представление группы применимых стандартов по безопасности медицинского программного обеспечения, например тех, что приведены в данном стандарте, могут быть осуществлены при последующей разработке стандартов, используя классификацию GCM.

Далее представлена сводная информация о жизненном цикле по пяти категориям стадий жизненного цикла, необходимая для настоящего стандарта:

1) проектирование: включает концепцию, требования и этапы проектирования;

2) разработка: включает этапы разработки, производства и выпуска;

3) внедрение: включает этапы установки, настройки, интеграции и ввода в действие;

4) функционирование: включает этапы функционирования, клинического использования и технической поддержки;

5) вывод из эксплуатации: включает этапы вывода из эксплуатации и удаления.

Тем не менее с точки зрения оценки вышеупомянутые стадии жизненного цикла как на детальном, так и на обобщенном уровне являются приемлемым подходом к жизненному циклу программного обеспечения для выполнения оценки безопасности медицинского программного обеспечения на основе набора стандартов.

4.5 Метод выбора стандартов для оценки

Существует множество стандартов, которые могут быть полезны для разработчиков, специалистов по внедрению и пользователей медицинского программного обеспечения для обеспечения его безопасности. В поддержку настоящего стандарта и его указаний из различных источников в рамках определенного набора критериев была выбрана идентификация стандартов для оценки.

Источники включают:

- изданные стандарты и текущую программу работ ИСО/ТК 215 «Информатизация здоровья» (ISO/TC 215 Health informatics);

- изданные стандарты и текущую программу работ ИСО/ТК 210 «Менеджмент качества и общие аспекты медицинского оборудования» (ISO/TC 210 Quality management and corresponding general aspects for medical devices);

- изданные стандарты и текущую программу работ МЭК/ТК 62 КК62А «Общие аспекты электрооборудования, используемого в медицинской деятельности» (IEC/TC 62 SC62A Common aspects of electrical equipment used in medical practice);

- изданные стандарты и текущую программу работ ИСО/ТК 176 «Менеджмент качества и обеспечение качества» (ISO/TC 176 Quality management and quality assurance);
- изданные стандарты и текущую программу работ ИСО/МЭК СТК 1 и его подкомитетов и работа технической консультативной группы ИСО/МЭК «Безопасность»;
- заключения экспертизы общих стандартов, стандартов рынка информационных технологий и ИЗ, относящиеся к надлежащей практике разработки и безопасности продукта.

Для определения того, должен ли стандарт находиться среди тех, что рассмотрены в настоящем стандарте, применялось несколько критериев. Стандарт рассматривался, если:

- стандарт разработан международной или многонациональной организацией по разработке стандартов;
- стандарт может быть использован в ходе одного или более этапов жизненного цикла медицинского программного обеспечения;
- стандарт применялся более чем в одной стране (как определено в ходе неформальной проверки стандартов, перечисленных выше);
- стандарт применим или рассматривает программное обеспечение или медицинское программное обеспечение, как это определено или выявлено в настоящем стандарте;
- стандарт рассматривает проблемы риска и безопасности.

Примечание — Все общепримени мые стандарты, например стандарты качества, стандарты, посвященные рискам, или стандарты на системы и проектирование систем (например, СТК 1), определяются как применимые основы надлежащей практики для стадий жизненного цикла программного обеспечения, менеджмента рисков и повышения безопасности и в указанном качестве сгруппированы для упрощения поиска.

Существует ряд других стандартов, которые применяются для успешного выполнения проектирования, разработки, реализации и эксплуатации медицинского программного обеспечения, например атрибутивные стандарты, т. е. те, которые определяют (и предоставляют соответствующую информацию) характеристики программного обеспечения или необходимые функции, которые являются тестируемыми и полезными для разработчиков, специалистов по внедрению и пользователей медицинского программного обеспечения при обеспечении его безопасности. В частности, стандарты на функционал и данные, применяемые по мере необходимости в течение жизненного цикла медицинского программного обеспечения, также являются основополагающими для обеспечения безопасности медицинского программного обеспечения. Отказ в использовании применимых, предназначенных для конкретных целей атрибутивных стандартов может привести к повышению риска на любой стадии жизненного цикла медицинского программного обеспечения.

У нескольких стандартов, которые применяются к безопасному медицинскому программному обеспечению, существуют сопровождающие их информативные руководства по применению этих стандартов. Если у соответствующих стандартов по безопасности медицинского программного обеспечения есть такое руководство, то такая информация дана в подразделе «Отношения» для каждого конкретного оцениваемого стандарта (см. 5.1).

4.6 Стандарты, оценка которых выполнена в настоящем стандарте

В таблицах 2 и 3, приведенных ниже, предоставлен список стандартов, рассмотренных в настоящем стандарте. Таблицы включают номер, название стандартов и организации, ответственные за их разработку (в том числе указание технического комитета/подкомитета). В таблице 2 перечислены основополагающие серии стандартов по безопасности медицинского программного обеспечения (серии стандартов, которые имеют общее применение). В таблице 3 перечислены те стандарты, которые имеют общие положения для медицинских устройств или специального медицинского программного обеспечения.

Таблица 2 — Основополагающие стандарты, относящиеся к безопасности медицинского программного обеспечения

Область применения	Стандарты(ы), руководства и отчеты	Организация-разработчик
Менеджмент качества	ИСО 9000:2005 Системы менеджмента качества. Основные положения и словарь (ISO 9000:2005 Quality management systems — Fundamental and vocabulary) ИСО 9001:2008 Системы менеджмента качества. Требования (ISO 9001:2008 Quality management systems — Requirements)	ИСО/ТК 176 и ИСО/МЭК СТК 1 ПК7

Окончание таблицы 2

Область применения	Стандарты(ы), руководства и отчеты	Организация-разработчик
Менеджмент качества	ИСО 10005:2005 Системы менеджмента качества. Руководящие указания по планам качества (ISO 10005:2005 Quality management systems — Guidelines for quality plans) ИСО 10006:2003 Системы менеджмента качества. Руководящие указания по менеджменту качества проектов (ISO 10006:2003 Quality management systems — Guidelines for quality management in projects) ИСО 10007:2003 Системы менеджмента качества. Руководящие указания по управлению конфигурацией (ISO 10007:2003 Quality management systems — Guidelines for configuration management) ИСО 90003:2004 Техника программного обеспечения. Рекомендации по применению ИСО 9001:2000 к компьютерному программному обеспечению (ISO/IEC 90003:2004 Software engineering — Guidelines for the application of ISO 9001:2000 to computer software)[a)]	ИСО/ТК 176 и ИСО/МЭК СТК 1 ПК7
Разработка систем и программного обеспечения	ИСО/МЭК 12207:2008 Разработка систем и программного обеспечения. Процессы жизненного цикла программного обеспечения (ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes) ИСО/МЭК 20000 Информационные технологии. Управление услугами (ISO/IEC 20000 Information technology — Service management) (серия из нескольких частей) ИСО/МЭК 25000 Разработка программного обеспечения. Требования и оценка качества программного продукта (SQuaRE). Руководство по SQuaRE [ISO/IEC 25000 Software Engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Guide to SquaRE] (часть из серии) ИСО/МЭК 15026 Разработка систем и программного обеспечения. Обеспечение систем и программного обеспечения. (ISO/IEC 15026 Systems and software engineering — Systems and software assurance) (серия из нескольких частей) ИСО/МЭК 15504 Информационные технологии. Оценка процессов. (ISO/IEC 15504 Information technology — Process assessment) (серия из нескольких частей) Также серия ИСО/МЭК 27000 (ISO/IEC 27000) именуемая «Серия стандартов ISMS»	ИСО/МЭК СТК 1 КК 7 и КК27
Управление риском	ИСО 31000:2009 Менеджмент рисков. Принципы и руководство (ISO 31000:2009 Risk management — Principles and guidelines) Руководство ИСО 73:2009 Менеджмент рисков. Термины и определения. (ISO Guide 73:2009 Risk management — Vocabulary)	Техническое руководящее бюро ИСО (ТМВ)
Эргономика взаимодействия человека и системы	ИСО 9241-129:2010 Эргономика взаимодействия человека и системы. Часть 129. Руководство по индивидуализации программного обеспечения (ISO 9241-129:2010 Ergonomics of human-system interaction — Part 129: Guidance on software individualization) ISO/TR 16982:2002 Эргономика взаимодействия человека и системы. Методы, основанные на удобстве применения, для обеспечения проектирования, ориентированного на человека (ISO/TR 16982:2002 Ergonomics of human-system interaction — Usability methods supporting human-centred design)	ИСО/ТК 159
Безопасность	Руководство ИСО/МЭК 51:1999 Аспекты безопасности. Руководящие указания по включению в стандарты (ISO/IEC Guide 51:1999 Safety aspects — Guidelines for their inclusion in standards)	Объединенная техническая консультативная группа ИСО/МЭК по безопасности

[a)] В настоящее время в ИСО/МЭК СТК 1/ПК 7 разрабатывается ИСО/МЭК ТО 90003 с целью замены ИСО/МЭК 90003:2004.

Таблица 3 — Стандарты для медицинских устройств или специального медицинского программного обеспечения

Стандарт	Название	Организация-разработчик
Менеджмент качества	ИСО 13485:2003 Медицинские приборы. Системы менеджмента качества. Требования для целей регулирования (ISO 13485:2003 Medical devices — Quality management systems — Requirements for regulatory purposes)	ИСО/ТК 210
Процесс жизненного цикла программного обеспечения	МЭК 62304:2006 Программное обеспечение медицинских приборов. Процессы жизненного цикла программного обеспечения (IEC 62304:2006 Medical device software — Software life cycle processes)	ИСО/ТК 62 ПК 62А ИСО/ТК 210
Менеджмент рисков	ИСО 14971:2007 Медицинские приборы. Применение менеджмента рисков к медицинским приборам (ISO 14971:2007 Medical devices — Application of risk management to medical devices)	ИСО/ТК 210
Менеджмент рисков	МЭК 80001-1:2010 Менеджмент рисков для информационных сетей с медицинскими приборами. Часть 1. Роли, ответственности и деятельность (IEC 80001-1:2010 Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities)	МЭК/ТК 62 ПК 62А ИСО/ТК 215
Менеджмент безопасности	ИСО 27799:2008 Информатизация здоровья. Менеджмент информационной безопасности в здравоохранении по стандарту ИСО/МЭК 27002 (ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002)[a]	ИСО/ТК 215
Безопасность	ИСО/ТР 27809:2007 Информатизация здоровья. Меры обеспечения безопасности пациента при использовании программных средств (ISO/TR 27809:2007 Health informatics — Measures for ensuring patient safety of health software)	ИСО/ТК 215
Безопасность	ИСО/ТС 25238:2007 Информатизация здоровья. Классификация рисков для безопасности, связанных с медицинским программным обеспечением (ISO/TS 25238:2007 Health informatics — Classification of safety risks from health software)	ИСО/ТК 215
Проектирование эксплуатационной пригодности	МЭК 62366:2007 Медицинские приборы. Проектирование медицинских приборов с учетом эксплуатационной пригодности (IEC 62366:2007 Medical devices — Application of usability engineering to medical devices)	ИСО/ТК 210

[a] Включает ссылки на ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005.

4.7 Менеджмент рисков

Определяющим для оценки стандартов, предназначенных для обеспечения безопасности медицинского программного обеспечения, является вопрос: заключается ли цель стандарта в снижении риска на всех этапах жизненного цикла или только для этапов, связанных с программным обеспечением.

Менеджмент рисков подразумевает под собой систематическое применение менеджмента политик, процедур и методик при выполнении задач по анализу, оценке и управлению риском. В ИСО 31000 менеджмент рисков определяется как «скоординированная деятельность по руководству и управлению организацией в отношении рисков. Менеджмент рисков обычно включает оценку, обработку, принятие и предупреждение рисков».

Общий подход к менеджменту рисков определяется в общепризнанном ИСО 31000 и в связанных с ним стандартах:

- ИСО 31000:2009 Принципы и руководящие указания по реализации (ISO 31000:2009, Principles and guidelines on implementation);
- МЭК 31010:2009 Менеджмент рисков. Методы оценки риска (IEC 31010:2009, Risk management — Risk assessment techniques); и
- Руководство ИСО 73:2009 Менеджмент рисков. Словарь (ISO Guide 73:2009, Risk management — Vocabulary).

ИСО 31000 является исходной точкой для разработки стандартов по менеджменту рисков и служит руководством, применяемым в течение функционирования организации для широкого круга деятельности. Он может быть применен к любому типу риска, независимо от его природы и от того, положительные или отрицательные последствия он имеет. Данный стандарт не предназначен исключительно для рассмотрения вопросов безопасности. Инструкции по введению аспектов безопасности в стандарты указаны в Руководстве 51 ИСО/МЭК.

Менеджмент рисков, связанный со здравоохранением, включен в стандарт по медицинским приборам: ИСО 14971:2007 Медицинские приборы. Применение менеджмента риска к медицинским приборам (ISO 14971:2007, Medical devices — Application of risk management to medical devices) и сопровождающий его МЭК/ТР 80002-1, Руководство по применению ИСО 14971 к программному обеспечению медицинских приборов (IEC/TR 80002-1, Guidance on the application of ISO 14971 to medical device software). ИСО 14971 и IEC/TR 80002-1 предназначены для производителей медицинских приборов и программного обеспечения медицинских приборов, включая ЛИС и PACS.

Менеджмент рисков, связанный со здравоохранением, также изложен в IEC/TR 80001-1:2010 Применение менеджмента рисков к ИТ-сетям с медицинскими приборами. Часть 1. Роли, ответственности и деятельность (IEC/TR 80001-1:2010 Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities), в котором рассматривается риск, возникающий во время внедрения системы и во время ее эксплуатации.

Дополнительный полезный материал по менеджменту рисков, в частности, как он относится к медицинскому программному обеспечению, можно найти в ISO/TR 27809:2007 Информатизация здоровья. Меры обеспечения безопасности пациента при использовании медицинского программного обеспечения (ISO/TR 27809:2007 Health informatics — Measures for ensuring patient safety of health software), и ISO/TS 25238 Классификация рисков безопасности, связанных с медицинским программным обеспечением (ISO/TS 25238 — Classification of safety risks from health software).

Другой ключевой проблемой менеджмента рисков при обеспечении безопасности медицинского программного обеспечения является необходимость решения вопросов, связанных с распределением рисков и определением остаточного риска в медицинском программном обеспечении на всех стадиях его жизненного цикла. Руководство ИСО 73 определяет распределение рисков как «форму обработки рисков, включающую согласованное распределение рисков с другими заинтересованными сторонами».

При выпуске медицинского программного продукта (т. е. в момент выпуска) на рынок производителем программного обеспечения остается некоторый уровень риска для пациентов, который является остаточным риском.

Примечание — С нормативной точки зрения выпуск медицинского программного обеспечения также является точкой, когда можно применить послепродажные нормативные положения в отличие от нормативных положений перед выпуском в продажу.

Стороны, ответственные за остаточный и распределяемый риск, меняются на протяжении всего жизненного цикла программного обеспечения. Например, когда специалист по внедрению покупает коммерчески доступный продукт или заказывает создание программного обеспечения собственной разработки, он неявно (а иногда и явно) принимает на себя часть ответственности за известные остаточные риски. С этой точки зрения несмотря на остаточный риск, независимо от способа приобретения, специалист по внедрению соглашается с тем, что медицинское программное обеспечение производителя отвечает (или будет отвечать) заявленным требованиям.

При внедрении медицинского программного обеспечения собственной разработки или приобретенного возникают новые риски (например, связанные с настройкой, интеграцией, качеством данных и клиническим использованием системы). Затем ответственность за управление полным набором рисков для безопасности распределяется среди всего множества заинтересованных сторон, каждая из которых несет определенную ответственность и зависит от других, начиная от разработчика, специалиста по внедрению и кончая владельцем/оператором, а также от организаций по оказанию медицинской помощи и до пользователей системы.

При переходе от одной стадии жизненного цикла к другой и с привлечением новых сторон передача этих исков очень важна: например, должны быть четко определены соответствующие обязательства по управлению рисками и механизмами реагирования. Организации, привлеченные на последующих этапах жизненного цикла программного обеспечения, должны быть в курсе этих обязательств и связанных с ними рисков, а также мер, которые они могут предпринять, для эффективного менеджмента этих обязательств и рисков.

В процессе рассмотрения медицинского программного обеспечения распределение рисков является важным элементом при рассмотрении стандартов с целью понять, охватывает ли область применения стандарта точки перехода, в которых риски распределяются между сторонами, и если это так, то какая из сторон (разработчик, специалист по внедрению, владелец-оператор и/или пользователь) должна предпринять действия по менеджменту рисков.

4.8 Человеческий фактор

Дисциплина, изучающая человеческие факторы, рассматривает физическое и психологическое взаимодействие людей с изделиями, инструментами, процедурами и процессами. Ее главная цель состоит в адаптации технологии так, чтобы она функционировала естественным для человека образом.

Сложность систем здравоохранения резко возросла за последние несколько лет. В результате работники здравоохранения должны теперь взаимодействовать со многими системами, которые зачастую не учитывают возможности человека. При работе с такими сложными системами существует вероятность возникновения ошибок. Интеграция вопросов, связанных с человеческими факторами, с культурой организации, и применение подхода проектирования с ориентацией на пользователя (UCD) при разработке систем здравоохранения помогут уменьшить вероятность возникновения ошибок и повысить безопасность медицинского программного обеспечения.

Дисциплина, изучающая человеческие факторы, является важной частью в разработке медицинского программного обеспечения, и ее использование гарантирует, что медицинское программное обеспечение разрабатывается с постоянным привлечением реальных конечных пользователей. Рассматриваемая дисциплина также устанавливает организационные процессы, которые ориентированы на доказательство того, что медицинское программное обеспечение хорошо адаптировано к человеку и к окружающей его среде.

ИСО 9241 — это стандарт, состоящий из нескольких частей, предоставляющий всестороннюю основу для решения вопросов, связанных с различными элементами эргономики взаимодействия человека с компьютером.

Следующие два дополнительных стандарта выделяют принципы, связанные с человеческими факторами, которым необходимо следовать при разработке медицинских приборов:

- МЭК 62366:2007 Медицинские приборы. Применение эргономического проектирования для медицинских приборов (IEC 62366:2007 Medical devices — Application of usability engineering to medical devices);

- ANSI/AAMI HE75.2009 Проектирование с учетом человеческого фактора. Проектирование медицинских приборов (Human factors engineering — Design of medical devices).

Несмотря на то что эти два стандарта посвящены медицинским приборам, те же важные принципы применимы к медицинскому программному обеспечению и включают:

a) привлечение пользователей заранее и часто в процесс проектирования. Привлечение пользователей с самого начала процесса проектирования поможет продвижению подхода проектирования с ориентацией на пользователя. Оба стандарта описывают способы, с помощью которых это может быть достигнуто;

b) рассмотрение разработчиками характеристик, возможностей и предпочтений пользователей. С целью обеспечения эффективности и безопасности медицинского программного обеспечения, возможности пользователей и их ограничения должны быть учтены в разработке. HE75 выделяет принципы проектирования, которые следует учитывать разработчикам с целью обеспечения надлежащей разработки и безопасности в использовании медицинского программного обеспечения. Руководство по проектированию, связанное со зрительным восприятием, слуховым восприятием, обработкой информации, памятью, способностью к ответным действиям и эргономикой, должно быть принято во внимание для повышения безопасности медицинского программного обеспечения. Для оценки соответствия медицинского программного обеспечения основным принципам проектирования [7] могут быть использованы эвристические подходы (см. ZHANG);

c) управление риском возникновения ошибок эксплуатации. Методы, помогающие управлению рисками возникновения ошибок эксплуатации, представлены в HE75. Также рассмотрен процесс менеджмента рисков ошибок эксплуатации. Этот процесс является важной частью структуры человеческих факторов для повышения безопасности медицинского программного обеспечения и дает эффект при интеграции с системами менеджмента рисков;

d) влияние руководящих указаний, связанных с человеческим фактором, на принципы проектирования, экологические требования, документацию пользователя, межкультурные факторы,

возможности доступа, интерфейсы пользователя программного обеспечения, эргономику и медико-санитарную помощь на дому. Существует множество аспектов, связанных с человеческим фактором, которые необходимо учитывать для повышения безопасности медицинского программного обеспечения. HE75 описывает некоторые из них и содержит руководящие указания, которые должны соблюдаться проектировщиками для обеспечения хорошей приспособленности системы к человеку;

e) следование процессу эргономического проектирования и итерационного проектирования. Эргономическое проектирование является ключевым в подходе, основанном на учете человеческих факторов. Оно активно использует подход итерационного проектирования путем испытания и проверки систем с привлечением конечных пользователей. Результаты, полученные благодаря этому процессу, отправляются обратно на этап проектирования, позволяя во много раз снизить возможность возникновения рисков и проблем, связанных с безопасностью.

Примечание — В различных работах, включая [8] и [9], появляются дополнительные ссылки на подходы и модели, учитывающие человеческие факторы и объединяющие применимость и расширение взаимодействия с пользователем в медицинских организациях.

4.9 Уровень детализации

В контексте стандартов, содействующих безопасности в медицинском программном обеспечении, уровень детализации означает уровень сложности или уровень, до которого система декомпозируется на более мелкие части. В контексте разработки программного обеспечения это означает обеспечение такого уровня, на котором четко определено поведение критических частей и при этом обеспечена возможность кодирования на нем. Этими частями могут быть части начиная от отдельного элемента программного обеспечения (например, значение данных систолического давления крови) до интегрированного решения, реализованного между юрисдикциями.

МЭК 62304 предоставляет один подход к детализации программного обеспечения, сконцентрировав внимание на стадии разработки программного обеспечения на трех уровнях: системы, элемента и модуля. С целью оценки уровня применимости стандарта к безопасности медицинского программного обеспечения и учитывая некоторые наглядные примеры медицинского программного обеспечения, настоящий стандарт использует следующие три уровня детализации:

- уровень компонентов. Уровень модуля медицинского программного обеспечения, который включает в себя данные, объекты или другие субъекты, сформированные и используемые как внутри компьютерной программы, так и вне ее.

Примечание — Этот уровень включает разработку модуля и элемента по МЭК 62304:2006;

- уровень приложений. Компьютерная программа или набор компьютерных программ, которые служат для определяемых и конкретных служебных целей. В медицинском программном обеспечении приложения служат для определяемых и конкретных медицинских бизнес-целей.

Примечание — Этот уровень включает разработку системы по МЭК 62304:2006;

- уровень корпоративного приложения. Субъект или организация, объединяющая людей, процессы, информацию и технологии, которые используют приложение или ряд приложений для поддержания деятельности всего предприятия.

5 Оценка стандартов и руководящие указания

5.1 Оценка стандартов

Для оценки стандарта, использование которого может содействовать обеспечению безопасности медицинского программного обеспечения, необходимо ответить на следующие вопросы:

a) Полезен ли стандарт для повышения уровня безопасности пациентов при разработке, внедрении или эксплуатации медицинского программного обеспечения (то есть для снижения рисков)?

b) На каком уровне структурированности медицинского программного обеспечения применяется стандарт?

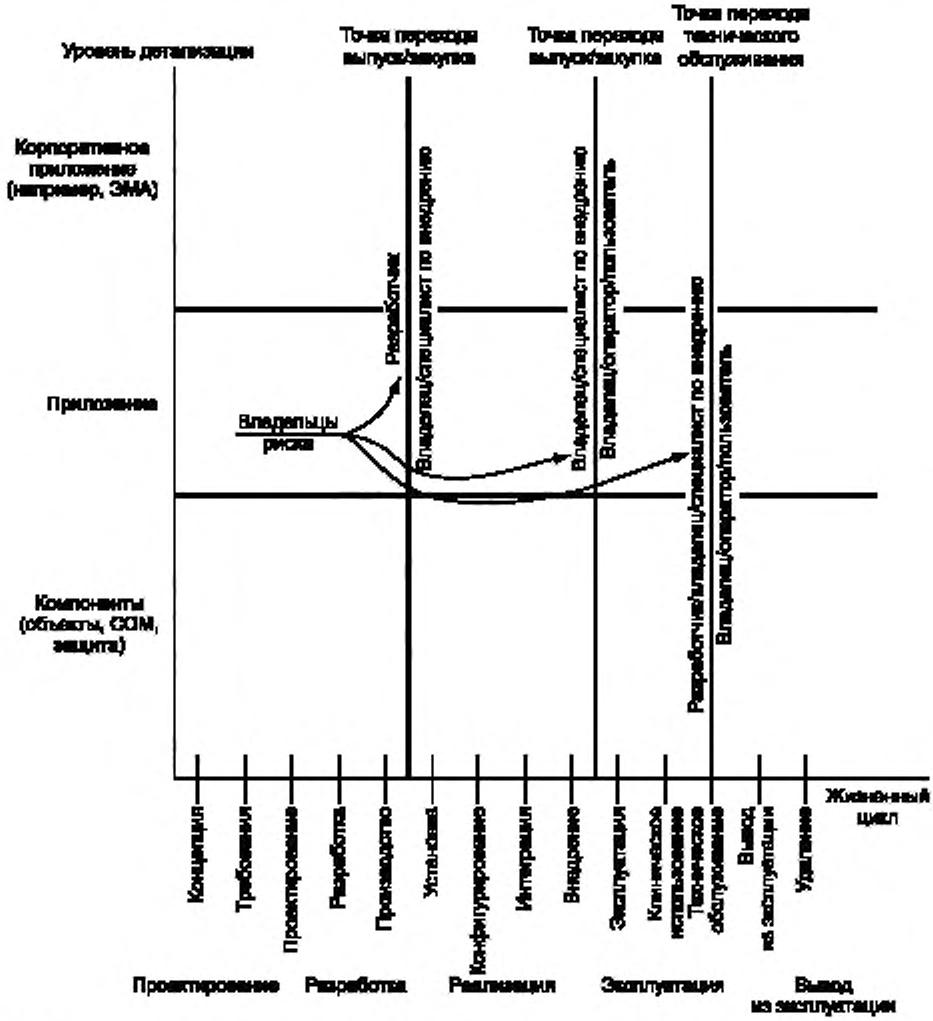
c) На какой(их) стадии(ях) жизненного цикла медицинского программного обеспечения применяется стандарт?

При ответе на эти вопросы используется следующая информация, относящаяся к стандартам:

- идентификационный номер стандарта, дата выпуска (или статус разработки, если стандарт еще не выпущен) и название;

- область применения стандарта;
- применимость и приемлемость риска (с отметкой о средствах управления);
- подтверждение использования стандарта (при наличии);
- информация о жизненном цикле программного обеспечения и информация о степени структурированности программного обеспечения;
- связь стандарта с другими стандартами.

Общий подход для оценки и отображения стандартов основан на двумерной матрице или таблице детализации и стадий жизненного цикла. На рисунке 1 представлены элементы матрицы и идентификация точек перехода, где риск разделяется разными сторонами.



Примечание — Несмотря на то что стадии жизненного цикла медицинского программного обеспечения на рисунке расположены последовательно, они включают в себя сложный набор последовательных и повторяющихся действий для того, чтобы обеспечить непрерывный менеджмент этого программного обеспечения всеми участвующими сторонами. Например, техническое обслуживание включает многократные, повторяющиеся точки разделения рисков.

Рисунок 1 — Риск, разделяемый множеством заинтересованных сторон в процессе жизненного цикла медицинского программного обеспечения

Первые пять оценок дают указания об основных сериях стандартов и охватывают всю область применения. Эти стандарты являются основой для специальных стандартов по медицинскому программному обеспечению, а также основой и для решения вопросов, касающихся рисков и безопасности медицинского программного обеспечения. Данные стандарты предоставляют важные передовые практические методы для программного обеспечения в целом, которое включает медицинское программное обеспечение, и сами по себе являются частью последовательного процесса рассмотрения стандартов, которые могут быть использованы для разработки, внедрения и применения медицинского программного обеспечения, безопасного для пациента. Пять последующих серий являются «организационными» или выполненными «на уровне предметной области ИКТ», или «риск предприятия или общая безопасность» в области применения, и их использование должно быть основано на этих точках зрения.

После основных серий (см. 5.1.6 и далее) выполняется оценка специальных стандартов, которые применяются при разработке, внедрении и использовании медицинского программного обеспечения, безопасного для пациента.

5.1.1 Стандарты менеджмента качества

5.1.1.1 Область применения

Стандарты менеджмента качества ИСО связаны с системами менеджмента качества и предназначены для того, чтобы помочь организациям обеспечить соответствие потребностям покупателей. Стандарты включают в себя:

- ИСО 9000:2005 Системы менеджмента качества. Основные положения и словарь (ISO 9000:2005, Quality management systems — Fundamentals and vocabulary);
- ИСО 9001:2008 Системы менеджмента качества. Требования (ISO 9001:2008 Quality management systems — Requirements);
- ИСО 10005:2005 Системы менеджмента качества. Руководящие указания по планам качества (ISO 10005:2005 Quality management systems — Guidelines for quality plans);
- ИСО 10007:2003 Системы менеджмента качества. Руководящие указания по управлению конфигурацией (ISO 10007:2003 Quality management systems — Guidelines for configuration management).

Примечание — ISO/IEC TR 90003 Руководство по применению ИСО 9001 к компьютерному программному обеспечению (ISO/IEC 900034, Guidelines for the application of ISO 9001:2000 to computer software) является основополагающим стандартом для применения систем менеджмента качества к процессам жизненного цикла программного обеспечения. Сейчас он находится на стадии разработки в СТК 1/ПК 7 и предназначен для замены ИСО/МЭК 90003 Техника программного обеспечения. Рекомендации по применению ИСО 9001 к компьютерному программному обеспечению (ИСО/МЭК 90003:2004 Software engineering — Guidelines for the application of ISO 9001:2000 to computer software) в начале 2013 г.

5.1.1.2 Применимость/приемлемость риска

Несмотря на то что эта серия стандартов не применяется специально к безопасности медицинского программного обеспечения, ИСО 9001 является стандартом де-факто о создании и технической поддержке системы менеджмента качества. Следование процессам и методам, определенным в системе менеджмента качества организации, вероятно, приведет к закупке продукции и услуг, которые будут соответствовать потребности покупателей и применимым законодательным и нормативным требованиям.

5.1.1.3 Подтверждение использования

Эти стандарты широко применяются и используются во всех предметных областях деятельности.

5.1.1.4 Информация о жизненном цикле и уровне детализации

Не применимо для жизненного цикла программного обеспечения или детализации программного обеспечения.

5.1.1.5 Связь (отношение)

ИСО 13485 является эквивалентом ИСО 9001 в сфере производства медицинских приборов и был создан на основе ИСО 9001 для того, чтобы позволить его использование для нормативных целей.

5.1.2 Стандарты на разработку программного обеспечения и систем

5.1.2.1 Область применения

ИСО/МЭК СТК 1 (ISO/IEC JTC 1) «Информационные технологии» разрабатывает и поддерживает стандарты в широком спектре областей ИКТ, включает 19 полностью сформированных подкомитетов (ПК) [каждый имеет несколько соответствующих рабочих групп (РГ)] и две РГ, которые подчиняются непосредственно СТК 1. СТК 1, и его ПК/РГ в настоящее время несут ответственность за более чем 2500 изданных стандартов. ИСО/МЭК/СТК 1/ПК 7 «Разработка программного обеспечения и систем» (ISO/IEC JTC 1/SC 7 Software and systems engineering) является главным ПК в СТК 1, связанным с безопасностью программного обеспечения в широком смысле.

Примечание — Далее приведены ссылки на главную страницу СТК 1 для получения последней информации gost.e-ecolog.ru и http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020.

5.1.2.2 Применимость/приемлемость риска

Безопасность программного обеспечения основана на соответствующем управлении всем жизненным циклом программного обеспечения в рамках общего подхода управления и соответствия, который поддерживает и обеспечивает качество системы программного обеспечения. Основные соответствующие стандарты, взятые из СТК 1, включают в себя:

5.1.2.2.1 ИСО/МЭК 12207 Разработка систем и программного обеспечения. Процессы жизненного цикла программного обеспечения (ISO/IEC 12207 Systems and software engineering — Software life cycle processes)

Применение этого стандарта (и связанного с ним ИСО/МЭК 15288 по процессам жизненного цикла системы) в настоящее время разрабатывается в трех технических отчетах документа ИСО/МЭК 24748 Разработка систем и программного обеспечения. Управление жизненным циклом (Systems and software engineering — Life cycle management), включающих:

- Часть1. Руководство по управлению жизненным циклом.
- Часть 2. Руководство по применению ИСО/МЭК 15288 [ранее ISO/IEC TR 19760].
- Часть 3. Руководство по применению ИСО/МЭК 12207 [ранее ISO/IEC TR 15271].

Примечание — Часть 4 к ИСО/МЭК 24748 находится в стадии подготовки и в дальнейшем заменит ИСО/МЭК 26702 Разработка системы. Применение и управление процессами разработки систем (ISO/IEC 26702:2007, Systems engineering — Application and management of the systems engineering process), в котором особое внимание уделено факторам здравоохранения и безопасности в контексте разработки системы.

5.1.2.2.2 ИСО/МЭК 15504 Информационные технологии. Оценка процесса (ISO/IEC 15504 Information technology — Process assessment)

Безопасность программного обеспечения и систем продвинулась на шаг вперед в этом стандарте, состоящем из нескольких частей, который включает в себя стандарты, технические спецификации и технические отчеты, в том числе:

- Часть 1. Понятия и словарь.
- Часть 2. Выполнение оценки.
- Часть 3. Руководство по выполнению оценки.
- Часть 4. Руководство по использованию для усовершенствования и определения возможностей процесса.
- Часть 5. Типовая модель оценки процесса жизненного цикла программного обеспечения.
- Часть 6. Типовая модель оценки процесса жизненного цикла системы.
- Часть 7. Оценка зрелости организации.
- Часть 8. Типовая модель оценки процесса для управления ИТ-службой.
- Часть 9. Профили целевого процесса.
- Часть 10. Расширение безопасности.

5.1.2.2.3 ИСО/МЭК 15026 Проектирование систем и разработка программного обеспечения. Гарантирование систем и программного обеспечения. Часть 1. Понятия и словарь (ISO/IEC 15026 Systems and software engineering — Systems and software assurance)

Подходы, гарантирующие определенный риск и целостность программного обеспечения как искусственных объектов разработки программного обеспечения, рассматриваются в ИСО/МЭК 15026, который появился сначала в IEEE и обеспечивает гарантированный случай, который является целевым для «случая безопасности». ИСО/МЭК 15026 включает в себя:

- Часть 1. Понятия и словарь.
- Часть 2: Гарантированный случай.
- Часть 3. Уровни целостности системы.
- Часть 4. Гарантии в жизненном цикле.

5.1.2.2.4 ИСО/МЭК 20000 Информационные технологии. Управление услугами ИСО/МЭК 20000 рассматривает вопросы управления услугами в области информационных технологий и представляет организационный эквивалент сертификации по ITIL. Он включает в себя следующие основные части:

- Часть 1. Требования к системе управления услугами.
- Часть 2. Руководство по применению системы управления услугами.
- Часть 3. Руководство по определению области применения и применимости ИСО/МЭК 20000-1.

- Часть 4. Базовая модель процесса.
- Часть 5. Типовой план реализации для ИСО/МЭК 20000-1.
- Часть 7. Применение ИСО/МЭК 20000-1 к удаленной среде (не завершена).
- Часть 10. Понятия и словарь для ИСО/МЭК 20000-1 (не завершена).
- Часть 11. Руководство по связи между ИСО/МЭК 20000-1 и относящимся к нему общим подходам (не завершена).

Примечание — ISO/IEC TR 20000-11 предоставляет руководящие указания по связи между ИСО/МЭК 20000-1 и ITIL.

5.1.2.2.5 ИСО/МЭК 25000, Разработка программного обеспечения. Требования и оценка качества программного обеспечения (ISO/IEC 25000 Software Engineering — Software product Quality Requirements and Evaluation)

ИСО/МЭК 25000:2005 рассматривает процесс «формирования требований и оценки качества программного обеспечения». Другие ключевые стандарты и спецификации, имеющие отношение к ИСО/МЭК 25000, включают:

- ИСО/МЭК 25001:2007 Разработка программного обеспечения. Требования и оценка качества программного обеспечения. Планирование и управление (ISO/IEC 25001:2007 Software engineering — Software product quality requirements and evaluation — Planning and management);
- ИСО/МЭК 25010:2011 Разработка систем и программного обеспечения. Требования и оценка качества программного обеспечения. Модели качества систем и программного обеспечения (ISO/IEC 25010:2011 Software engineering — Software product quality requirements and evaluation — System and software quality models);
- ИСО/МЭК 25012:2008 Разработка систем и программного обеспечения. Требования и оценка качества программного обеспечения. Модель качества данных (ISO/IEC 25012:2008 Software engineering — Software product quality requirements and evaluation — Data quality model);
- ИСО/МЭК 25012:2008 Разработка систем и программного обеспечения. Требования и оценка качества программного обеспечения. Измерительная эталонная модель и руководство (ISO/IEC 25020:2007 Software engineering — Software product quality requirements and evaluation — Measurement reference model and guide);
- ИСО/МЭК 25021:2012 Разработка систем и программного обеспечения. Требования и оценка качества программного обеспечения. Элементы показателя качества (ISO/IEC 25021:2012 Software engineering — Software product quality requirements and evaluation — Quality measure elements);
- ИСО/МЭК 25040:2011 Разработка систем и программного обеспечения. Требования и оценка качества программного обеспечения. Процесс оценки (ISO/IEC 25040:2011 Software engineering — Software product quality requirements and evaluation — Evaluation process) (пересмотренное издание ISO/IEC 14598-1:2009);
- ИСО/МЭК 25045:2010 Разработка систем и программного обеспечения. Требования и оценка качества программного обеспечения. Типовая модель проведения оценивания восстанавливаемости (ISO/IEC 25045:2010 Software engineering — Software product quality requirements and evaluation — Evaluation module for recoverability).

ИСО/МЭК 25010, который заменяет ИСО/МЭК 9126, Разработка программного обеспечения. Качество изделия (ISO/IEC 9126, Software engineering — Product quality), помогает при оценке и определении качества системы и программного продукта. Он имеет четкую область применения в том смысле, что он предоставляет общую методологию оценки и определения качества программного обеспечения, но не распространяет ее на оценку рисков. Следовательно, ИСО/МЭК 25010 может быть применен ко всем программным продуктам и применен для идентификации рисков с указанием некоторой метрики или для распространения результатов, определенных для такой деятельности. Он применим к безопасности медицинского программного обеспечения особенно при оценке мер «качества при использовании», т. е. эффективности, результативности, удовлетворенности, безопасности и удобства использования. Он предоставляет как общие, так и конкретные параметры оценки. Эти параметры определяют соответствующую терминологию для определения, измерения и оценки качества системы и программного продукта. ИСО/МЭК 25010 также предоставляет набор характеристик качества, по которым можно сравнить установленные требования качества для полноты.

5.1.2.3 Подтверждение использования

Эти стандарты широко применяются и используются во всех предметных областях промышленности.

5.1.2.4 Информация о жизненном цикле и уровне детализации

Эти стандарты СТК 1/ПК 7 рассматривают программное обеспечение, в первую очередь как компоненты и приложения, с различной применимостью к корпоративным приложениям. Жизненный цикл полностью охватывает стадии проектирования и разработки, но не полностью стадии реализации и эксплуатации.

5.1.2.5 Связь (отношение)

Несмотря на то что стандарты СТК 1/ПК 7, на которые приведены ссылки в настоящем стандарте, не решают, в частности, вопросы программного обеспечения, но они рассматривают программное обеспечение в целом в общей предметной области ИКТ, а также связанные с ним процессы, риск и требования к безопасности.

Примечание — См. приложение В для получения дополнительной информации об области применения ключевых стандартов СТК 1/ПК 7, указанных выше.

5.1.3 Стандарты по менеджменту рисков

5.1.3.1 Область применения

ИСО 31000:2009 Менеджмент рисков. Принципы и руководящие указания (ISO 31000:2009, Risk management — Principles and guidelines) дает общий подход к менеджменту рисков предприятия. Стандарт не является специализированным для сектора здравоохранения или любого другого сектора. ИСО 31000 рассматривает вопросы определения, оценки и обработки, предупреждения и обсуждения, а также контроля и рассмотрения рисков.

5.1.3.2 Применимость/приемлемость риска

ИСО 31000 предоставляет общепризнанную модель для практикующих специалистов и компаний, использующих процессы менеджмента рисков, с целью заменить огромное количество существующих стандартов, методологий и моделей, которые различаются в разных отраслях, дисциплинах и областях.

5.1.3.3 Подтверждение использования

Это относительно новый стандарт, который в настоящее время широко используется во всех отраслях промышленности.

5.1.3.4 Информация о жизненном цикле и уровне детализации

Стандарт можно применять для всех стадий жизненного цикла системы или программного обеспечения. Он предоставляет руководящие указания на высоком уровне.

5.1.3.5 Связь (отношение)

ИСО 31000 связан со следующими документами:

- МЭК 31010:2009 Управление риском. Методы оценки риска (IEC 31010:2009, Risk management — Risk assessment techniques),

- Руководство ИСО 73:2009 Управление риском. Словарь (ISO Guide 73:2009, Risk management — Vocabulary).

Принципы, руководство и методы, описанные в данных стандартах, являются хорошей исходной точкой в тех случаях, когда должны быть рассмотрены риски в дополнение к безопасности пациента (см. 4.7 ИСО 31000:2009). Они согласуются с методами менеджмента рисков и с использованием метаязыка при выявлении физических причин в ИСО 14971:2007 для медицинских приборов, а также аналогично соответствуют МЭК/ТО 80002-1 Руководство по применению ИСО 14971 к программному обеспечению медицинских приборов (IEC/TR 80002-1, Guidance on the application of ISO 14971 to medical device software).

5.1.4 Стандарт по эргономике взаимодействия человека и системы

5.1.4.1 Область применения

Стандарты ИСО 9241 первоначально имели название «Эргономические требования для офисной работы с терминалами визуального отображения (ВТ)». С 2006 г. стандарты приобрели более общее название «Эргономика взаимодействия человека и системы». Они не являются специальными для здравоохранения или другого сектора. ИСО 9241 и связанные с ним стандарты являются стандартами, которые удобно и легко использовать, и в первую очередь они затрагивают использование продукта, интерфейс и взаимодействие с пользователем, процессы разработки изделий и проектирование с ориентацией на пользователя.

5.1.4.2 Применимость/приемлемость риска

Стандарты ИСО 9241 ориентированы на проектировщиков и разработчиков аппаратных средств и программного обеспечения и предоставляют общепризнанную основу для взаимодействия человека с аппаратными средствами и программным обеспечением. В качестве прототипа для проектирования с учетом конкретного человеческого фактора в медицинском программном обеспечении и признавая,

что низкая пригодность к использованию может увеличить риск непреднамеренного возникновения опасности, эти стандарты являются полезной основой для проектирования, учитывающего человеческие факторы в медицинском программном обеспечении.

5.1.4.3 Подтверждение использования

Эти стандарты широко распространены и используются во всех отраслях промышленности.

5.1.4.4 Жизненный цикл и уровень детализации

Эти стандарты в первую очередь применимы к проектированию и разработке жизненного цикла системы или программного обеспечения.

5.1.4.5 Связь (отношение)

ИСО 9241 состоит из серий стандартов, каждая из которых состоит из нескольких частей, включая:

- Серия 100. Эргономичность программного обеспечения.
- Серия 200. Процессы взаимодействия человека и системы.
- Серия 300. Устройства отображения и аппаратное обеспечение для устройств отображения.
- Серия 400. Физические входные устройства. Принципы эргономики.
- Серия 500. Производственная эргономика.
- Серия 600. Эргономика окружающей обстановки.
- Серия 700. Прикладные предметные области. Диспетчерские.
- Серия 900. Тактильные и сенсорные взаимодействия.

Данные стандарты, включая, например, ИСО 9241-210:2010, предоставляют некоторые из наиболее актуальных выводов о принципах и процессах проектирования на основе человеческих факторов, уделяя особое внимание применениям интерактивного программного обеспечения, которые отличают эти стандарты от других стандартов, ориентированных на медицинские приборы.

5.1.5 Руководство по безопасности

5.1.5.1 Область применения

Руководство ИСО/МЭК 51 предоставляет разработчикам стандартов руководящие указания по включению аспектов безопасности в стандарты. Руководство ИСО/МЭК 51 является общим руководством к разработке стандартов, связанных с безопасностью. Оно применимо к любому аспекту безопасности людей, имущества или окружающей среды либо к комбинации одного или более этих аспектов (например, безопасность только людей; людей и имущества; людей, имущества и окружающей среды).

5.1.5.2 Применимость/приемлемость риска

Руководство ИСО/МЭК 51 использует подход, направленный на снижение риска, связанного с использованием изделия, процессов или услуг. Рассмотрен полный жизненный цикл изделия, процесса или услуги, в том числе как предназначенного использования, так и обоснованно предсказуемого неправильного использования. Руководство уделяет внимание проблеме безопасности и достижения безопасности путем снижения риска до приемлемого уровня.

5.1.5.3 Подтверждение использования

Понятия и определения безопасности и риска широко используются в стандартах, связанных с медицинскими приборами, включая ИСО 14971 и др.

Следует отметить, что Руководство ИСО/МЭК 51 находится на стадии проверки и что связанные с ним руководства (например, Руководство ИСО/МЭК 63:2012), доступны и затрагивают определенные применения медицинских приборов в контексте Руководства ИСО/МЭК 51.

5.1.5.4 Информация о жизненном цикле и уровне детализации

В силу самого определения его области применения, Руководство ИСО/МЭК 51 можно применять для разработки стандартов для всех стадий жизненного цикла программного обеспечения и уровней структурированности. Оно дает указания на уровне общих положений и определений.

5.1.5.5 Связь (отношение)

Руководство ИСО/МЭК 51:1999 является вторым изданием, заменяющим первое, опубликованное в 1990 г. ИСО/МЭК 51 было первым из серии руководств, предназначенных для обеспечения согласованного подхода к понятию безопасности при подготовке международных стандартов. Руководство ИСО/МЭК 51 предвидело необходимость руководства для области, для которой было создано Руководство ИСО/МЭК 63. В соответствии с Руководством ИСО/МЭК 51 могут потребоваться дополнительные руководства для тех областей, в которых работает широкая категория медицинских приборов.

Руководство подробно останавливается на разработанных понятиях.

Примечания

1 Область применения Руководства ИСО/МЭК 63 заключается в предоставлении рекомендаций для создателей стандартов по включению проблем безопасности в разработку стандартов по безопасности медицинских приборов, предназначенных для использования в структуре менеджмента рисков, установленной в ИСО 14971.

Это подробно изложено в концепциях, разработанных в Руководстве ИСО/МЭК 51, по включению в стандарты, связанные с безопасностью, выполняемые функции и доступность для использования.

2 Руководство ИСО 73:2009 Менеджмент рисков. Словарь (ISO Guide 73:2009, Risk management — Vocabulary), несмотря на то что не является руководством по безопасности, дает определения общих терминов, связанных с менеджментом рисков. Оно направлено на поддержание взаимного и прочного понимания и согласованного подхода, описание деятельности, связанной с менеджментом рисков, и использование единой терминологии по менеджменту рисков в процессах и структурах, имеющих отношение к менеджменту рисков.

5.1.6 ИСО 13485:2003 Медицинские изделия. Системы менеджмента качества. Требования для целей регулирования (ISO 13485:2003 Medical devices — Quality management systems — Requirements for regulatory purposes)

5.1.6.1 Область применения

Данный международный стандарт определяет требования к системе менеджмента качества в тех случаях, когда организации необходимо продемонстрировать способность поставлять медицинские изделия и предоставлять связанное с ними обслуживание, отвечающее требованиям потребителя и установленным требованиям, применимым к этим медицинским изделиям и сопутствующим услугам.

5.1.6.2 Применимость/приемлемость риска

Так как цель данного стандарта заключается в содействии внедрения в системы менеджмента качества гармонизированных установленных требований к медицинским изделиям, он в первую очередь касается снижения риска путем последовательного применения процессов менеджмента качества. Он применяется производителем программного обеспечения для производства или проектирования/разработки и производства изделия(ий), удовлетворяющего(их) установленным требованиям к медицинским приборам.

5.1.6.3 Подтверждение использования

ИСО 13485 и его варианты (например, Требования к системе качества FDA) используются для регулирования применимого программного обеспечения медицинских устройств и специально определенных приложений и компонентов медицинского программного обеспечения в Европейском союзе, Канаде и США.

5.1.6.4 Информация о жизненном цикле и уровне детализации

Применяется к проектированию (от разработки концепции до проектирования) и разработке (разработка и производство), включая компоненты и приложения.

5.1.6.5 Связь (отношение)

ИСО 13485:2003 основан на ИСО 9001:2000 (он имеет тот же формат, что и ИСО 9001:2000, и большинство тех же требований), но при этом требования относительно «удовлетворения требований заказчика» и «постоянного улучшения» были изменены.

ИСО 13485:2003 имеет сопутствующий руководящий стандарт, ISO/TR 14969:2004, по применению требований для систем менеджмента качества. Он не добавляет или иным образом не изменяет требования ИСО 13485. Данный технический отчет не включает требования, которые должны использоваться в качестве основы для надзорных проверок или деятельности по оценке сертификации. ISO/TR 14969 не разработан специально для программного обеспечения, но распространяется на все медицинские приборы и предоставляет рекомендации, которые могут быть использованы для разъяснения требований ИСО 13485 и для иллюстрации некоторых из множества методов и подходов, доступных для удовлетворения требований ИСО 13485.

5.1.7 МЭК 62304:2006 Программное обеспечение медицинских приборов. Процессы жизненного цикла программного обеспечения (IEC 62304:2006, Medical device software — Software lifecycle processes)

5.1.7.1 Область применения

Данный стандарт определяет требования к жизненному циклу программного обеспечения медицинского оборудования. Набор процессов, действий и задач, описанных в данном стандарте, устанавливает общий подход для процессов жизненного цикла программного обеспечения медицинского оборудования.

5.1.7.2 Применимость/приемлемость риска

МЭК 62304 предназначен именно для программного обеспечения медицинского оборудования, включая программное обеспечение, которое, само по себе, является медицинским прибором. Стандарт определяет атрибуты СМК, которые производитель программного обеспечения будет применять к жизненному циклу программного обеспечения, включая проектирование, разработку, производство и техническое обслуживание. Эти атрибуты процесса используются для оценки и анализа риска, который будет выполнять производитель программного обеспечения — процесс, который также определен в стандарте.

5.1.7.3 Подтверждение использования

МЭК 62304 все чаще используется и упоминается в ссылках компаний-поставщиков в ЕС и США.

5.1.7.4 Жизненный цикл и уровень детализации

Применяется к проектированию (от разработки концепции до проектирования) и разработке (разработка, производство и послепроизводственные стадии), включая компоненты и приложения.

5.1.7.5 Связь (отношение)

Стандарты по менеджменту медицинских устройств, такие как ИСО 13485 и ИСО 14971, предоставляют среду менеджмента, которая закладывает основу для организаций по разработке изделий. Стандарты по безопасности, такие как МЭК 60601-1 и МЭК 61010-1, формируют специальное направление для создания безопасных медицинских приборов. Если программное обеспечение является частью таких медицинских приборов, то МЭК 62304 предоставляет более детальное описание действий, которое требуется для разработки и поддержки безопасного программного обеспечения медицинских приборов. МЭК 62304 был создан на основе ИСО/МЭК 12207 и содержит таблицу перекрестных ссылок, которая объединяет два стандарта.

5.1.8 ИСО 14971:2007 Медицинские приборы. Применение менеджмента риска к медицинским приборам (ISO 14971:2007, Medical devices — Application of risk management to medical devices)

5.1.8.1 Область применения

ИСО 14971 устанавливает для производителя процесс определения опасностей, связанных с медицинскими устройствами, в том числе с медицинскими приборами в диагностических лабораториях (IVD), а также процессы оценки и вычисления связанных рисков, управления этими рисками, включая контроль эффективности таким управлением.

5.1.8.2 Применимость/приемлемость риска

Стандарт устанавливает процесс, который производитель использует для идентификации, количественной оценки рисков и управления ими. На него приведены ссылки в МЭК 62304, и он часто используется производителями для подтверждения соответствия элементам менеджмента рисков ИСО 13485.

5.1.8.3 Подтверждение использования

В ряде ведомств было законодательно оформлено, что требования ИСО 14971 должны соблюдать. Некоторые из них (незакрытый перечень) включают в себя Южную Африку, Аргентину и Бразилию.

5.1.8.4 Информация о жизненном цикле и уровне детализации

ИСО 14971 применяется к проектированию (от разработки концепции до проектирования) и разработке (разработка и производство) для использования проектировщиками на постпроизводственных стадиях жизненного цикла и к компонентам и некоторым приложениям.

5.1.8.5 Связь (отношение)

ИСО 14971 предоставляет требования к процессу менеджмента рисков для МЭК 62304 и дополняется МЭК 62304.

ИСО 14971 имеет сопутствующий руководящий стандарт IEC/TR 80002-1:2009, в котором даны указания по применению требований, содержащихся в ИСО 14971, к программному обеспечению медицинского оборудования с дополнительными ссылками на МЭК 62304:2006 Программное обеспечение медицинского прибора. Процессы жизненного цикла программного обеспечения (IEC 62304:2006, Medical device software — Software life cycle processes). IEC/TR 80002-1 не добавляет и каким либо иным образом не изменяет требования ИСО 14971:2007 или МЭК 62304:2006.

Руководство в IEC/TR 80002-1 предназначено для практикующих специалистов по менеджменту рисков, которым необходимо осуществлять менеджмент рисков, если программное обеспечение включено в медицинский(ую) прибор (систему), а также для инженеров программного обеспечения, которые должны понимать, как соблюдать требования по менеджменту рисков в соответствии с ИСО 14971.

Следует отметить, что даже несмотря на то, что ИСО 14971 и сопутствующий IEC/TR 80002-1 сосредоточены на медицинских приборах, IEC/TR 80002-1 может быть использован для реализации процесса менеджмента рисков безопасности для любого медицинского программного обеспечения в медицинской среде независимо от того, классифицируется ли медицинское программное обеспечение как медицинский прибор. IEC/TR 80002-1 предоставляет превосходное руководство по оценке и количественному определению рисков безопасности медицинского программного обеспечения на стадиях проектирования и разработки и включает полезные приложения с примерами.

5.1.9 IEC/TR 80001-1:2010 Менеджмент рисков для ИТ-сетей с медицинскими приборами. Часть 1. Роли, ответственности и деятельность (IEC 80001-1:2010, Application of risk management for IT networks incorporating medical devices — Part 1: Roles, responsibilities and activities)

5.1.9.1 Область применения

IEC/TR 80001-1:2010 определяет роли, ответственности и действия, необходимые для менеджмента рисков ИТ-сетей, включающих медицинские приборы, для рассмотрения основных свойств безопасности, эффективности и защищенности данных и систем. Этот стандарт не определяет приемлемые уровни риска.

5.1.9.2 Применимость/приемлемость риска

Этот стандарт относится только к менеджменту рисков, поскольку он применяется на предмет включения медицинского устройства в ИТ-сети. Этот стандарт имеет исключительное значение, так как он относится к владельцу/оператору или другой стороне как к ответственной организации.

В частности, IEC/TR 80001-1:2010 определяет процесс, который ответственная организация использует для идентификации, количественной оценки и менеджмента рисков, включая обязательное распределение ролей в организации: ответственная организация обязана назначить людей на роли, определенные в этом стандарте. Данный стандарт определяет обязанности, стоящие за этими ролями. Наиболее важной из этих ролей является роль менеджера по рискам медицинских ИТ-сетей. На данную роль может быть назначен один из членов ответственной организации или внешний подрядчик.

Например, включение в сеть или удаление из сети медицинского устройства или других компонентов в ИТ-сетях является задачей, которая требует плана действий; она может находиться вне контроля производителя медицинского устройства.

5.1.9.3 Подтверждение использования

IEC/TR 80001-1 относится к внедрению (и эксплуатации, в том числе клиническому использованию), а также только к корпоративным приложениям.

5.1.9.4 Связь (отношение)

Действия по менеджменту рисков в IEC/TR 80001-1 в значительной степени основаны на тех, что указаны в ИСО 14971, но выходят за рамки безопасности, как это определено в последнем. Действия по управлению жизненным циклом, описанные в IEC/TR 80001-1, очень похожи на те, что описаны в ИСО/МЭК 20000-2 Информационные технологии. Управление услугами. Часть 2. Руководство по применению систем управления услугами (ISO/IEC 20000-2, Information technology — Service management — Part 2: Guidance on the application of service management systems). Дополнительные части серии 80001 предоставляют руководство по IEC/TR 80001-1 и инструменты для применения этого стандарта. Были завершены четыре руководящих документа (другие находятся на стадии разработки), а именно:

- Часть 2-1. Пошаговое управление риском в медицинских ИТ-сетях; Практическое применение и примеры (*Step by step risk management of medical IT-networks; Practical applications and examples*) предоставляет пошаговое руководство по применению менеджмента рисков при создании и изменении медицинских ИТ-сетей. Данная часть показывает это с помощью примеров и информации по идентификации и управлению соответствующими рисками. Следует отметить, что это не полная интерпретация IEC/TR 80001-1:2010, так как она предоставляет подробную информацию только для стадии выполнения IEC/TR 80001-1 (см. 4.4).

- Часть 2-2. Руководство по раскрытию и предоставлению информации о нуждах, рисках и средствах управления медицинскими приборами (*Guidance for the disclosure and communication of medical device security needs, risks andcontrols*) предоставляет руководство относительно того, как средства безопасности, указанные в IEC/TR 80001-1, могут быть раскрыты и рассмотрены между заинтересованными сторонами в проектах ИТ-сетей медицинских устройств. Оно предоставляет основу для диалога по вопросам безопасности.

- Часть 2-3. Руководство по беспроводным сетям (*Guidance for wireless networks*) дает практические рекомендации по менеджменту рисков, необходимые для использования медицинских приборов с поддержкой беспроводной связи и сетевых медицинских приборов. Оно не следует методологии, но отдельно рассматривает каждое свойство беспроводной связи и потенциальный риск.

- Часть 2-4. Общее руководство по применению для медицинских организаций (*General implementation guidance for healthcare delivery organizations*) помогает организациям, оказывающим медицинские услуги, оценить действие IEC/TR 80001-1 на организации и создать серию бизнесов в виде обычных процессов для управления риском на стадиях создания, сопровождения и поддержания в рабочем состоянии медицинских ИТ-сетей.

5.1.10 ИСО 27799:2008 Информатизация здоровья. Менеджмент информационной безопасности в здравоохранении по ИСО/МЭК 27002 (ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002)

5.1.10.1 Область применения

ИСО 27799 содержит руководящие указания, необходимые для интерпретации или внедрения ИСО/МЭК 27002 в области ИЗ, и является дополнением к этому стандарту. ИСО 27799 определяет подробный набор элементов управления для менеджмента информационной безопасности и содержит руководящие указания для обеспечения наилучших практических результатов и обязательные требования для защиты конфиденциальности, целостности и доступности персональной медицинской информации. ИСО 27799 также включает требования к проектированию, разработке, внедрению и технической поддержке информационных систем.

5.1.10.2 Применимость/приемлемость риска

ИСО/МЭК 27002 является сводом правил, который определяет средства управления для СМИБ. ИСО/МЭК 27002 является масштабным, сложным стандартом, и его рекомендации не разработаны специально для сферы здравоохранения. ИСО 27799 поддерживает внедрение ИСО/МЭК 27002 в сфере здравоохранения последовательно и уделяя особое внимание уникальным задачам, которые возникают в здравоохранении. Средства управления признаются обязательными, если они считаются необходимыми для защиты безопасности пациентов. Следуя ИСО 27799, медицинские организации обеспечивают поддержку конфиденциальности и целостности данных, за которые они несут ответственность, доступность ключевых систем медицинской информации и поддержку возможности учета медицинской информации.

5.1.10.3 Информация о жизненном цикле и уровне детализации

Применяется к проектированию, разработке, реализации и эксплуатации (т. е. клиническому использованию и текущему обслуживанию), а также к приложениям и корпоративным приложениям.

5.1.10.4 Связь (отношение)

Выбор и применение средств управления защитой в ИСО/МЭК 27002:2013 будут основаны на оценке рисков в конкретной среде. Таким образом, ИСО 27799:2008 ограничивает некоторые средства управления путем проведения общей оценки медицинской информации.

ИСО 27799 является специализированной для здравоохранения версией ИСО/МЭК 27002 Информационные технологии. Средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (ISO/IEC 27002 Information technology — Security techniques. — Code of practice for information security management), которая предоставляет перечень общепринятых задач управления и наилучших средств управления, используемых в качестве руководства при выборе и внедрении средств управления для достижения информационной безопасности. ИСО/МЭК 27002 является частью семейства стандартов ИСО/МЭК 27000.

Главным стандартом семейства ИСО/МЭК 27000 является ИСО/МЭК 27001 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements), который определяет требования к созданию, эксплуатации, контролю, анализу, технической поддержке и совершенствованию формализованной информации систем менеджмента безопасности в контексте общих деловых рисков организации.

ИСО/МЭК 27005 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (ISO/IEC 27005, Information technology — Security techniques — Information security risk management) предоставляет руководство по менеджменту рисков информационной безопасности, в том числе советы по оценке рисков, обработке рисков, принятию риска, предупреждению о рисках, контролю рисков и анализу рисков.

Примечания

1 ИСО/МЭК 27001 формально определяет обязательные требования к СМИБ. Он использует ИСО/МЭК 27002, чтобы указать соответствующие средства управления информационной безопасностью в рамках СМИБ. В организации может быть проведен аудит по ИСО/МЭК 27002, но нет способа пройти «сертификацию» на его основании, так как он является сводом правил. Организация может пройти аудит по ИСО/МЭК 27001 и получить сертификат соответствия.

2 Стандарты по информационной безопасности непосредственно применяются для управления безопасностью при использовании и эксплуатации медицинского программного обеспечения, обеспечивая целостность информации и гарантированную доступность.

5.1.11 ISO/TR 27809:2007 Информатизация здоровья. Меры обеспечения безопасности пациента при использовании медицинского программного обеспечения (ISO/TR 27809:2007, Health informatics — Measures for ensuring patient safety of health software)

5.1.11.1 Область применения

Данный технический отчет рассматривает меры управления, необходимые для обеспечения безопасности пациентов для медицинского программного обеспечения. Это не относится к программному обеспечению, которое:

- необходимо для надлежащего применения медицинского прибора,
- является вспомогательным средством для медицинского прибора,
- является самостоятельным медицинским прибором.

Тем не менее технический отчет начинается с рассмотрения средств управления жизненным циклом программного обеспечения, которые применяются к медицинским устройствам, предлагающим практические решения, и способов применения этих элементов управления к медицинскому программному обеспечению.

Одна из важных целей технического отчета заключается в определении того, какой из стандартов лучше всего использовать или создать, если медицинское программное обеспечение необходимо регламентировать или контролировать некоторым способом.

5.1.11.2 Применимость/приемлемость риска

Особое внимание в данном техническом отчете сосредоточено на менеджменте рисков, как на одном из средств управления. В этом отношении документ рассматривает ряд имеющихся стандартов по менеджменту рисков (в том числе немедицинские стандарты, например МЭК 61508) и включает классификацию рисков из ISO/TS 25238.

5.1.11.3 Информация о жизненном цикле и уровне детализации

Наряду с тем, что «средства управления проектированием» явно определены как одна из возможных мер, стандарт косвенно уделяет внимание начальным стадиям жизненного цикла (проектирование и разработка). Технический отчет, однако, признает, что такие шаги должны быть предприняты для устранения рисков, возникающих и на более поздних стадиях жизненного цикла. Область применения технического отчета распространяется преимущественно на приложения, хотя можно считать, что и на компоненты.

5.1.11.4 Связь (отношение)

Технический отчет ссылается на значительное количество соответствующих стандартов. ISO/TR 27809 ссылается на настоящий стандарт и охватывает аналогичные области применения и проблемы. Предполагается, что ISO/TR 17791 предоставляет обновленное и современное представление проблем стандартов, которые лучше всего использовать для обеспечения безопасности пациентов в медицинском программном обеспечении.

5.1.12 ISO/TS 25238:2007 Информатизация здоровья. Классификация рисков безопасности, связанных с медицинским программным обеспечением (ISO/TS 25238:2007, Health informatics — Classification of safety risks from health software)

5.1.12.1 Область применения

Данная техническая спецификация связана с безопасностью пациентов и дает рекомендации по анализу и классификации опасностей и рисков для пациентов, возникающих в медицинском программном обеспечении, с целью предоставить возможность присвоения одной из пяти категорий риска любому изделию. Это относится и к опасностям, и к рискам, которые могут причинить вред пациенту. Другие риски, такие как финансовые или организационные, выходят за рамки данной технической спецификации, если они не наносят вред пациенту.

ISO/TS 25238 применяется к любому медицинскому программному обеспечению независимо от того, доступно ли оно на рынке и имеется в продаже или предоставляется бесплатно. Приведены примеры применения схемы классификации. Данная техническая спецификация не распространяется на программное обеспечение, которое необходимо для надлежащего применения или функционирования медицинского прибора.

5.1.12.2 Применимость/приемлемость риска

Данная техническая спецификация уделяет особое внимание классификации рисков, где уровень рисков можно представить в виде матрицы рисков. Эта классификация строится на вероятности и последствии, образующих два измерения матрицы. ISO/TS 25238 создан для медицинских программ и обеспечивает процесс распределения риска.

5.1.12.3 Информация о жизненном цикле и уровне детализации

Так как анализ, выполняемый для назначения риска, охватывает все участвующие стороны от проектирования до разработки, реализации, эксплуатации и обслуживания, данный стандарт уделяет особое внимание всем стадиям жизненного цикла, за исключением вывода из эксплуатации. Он применяется главным образом к приложениям, хотя также может рассматривать и компоненты приложений.

5.1.12.4 Связь (отношение)

ISO/TS 25238 является самостоятельной технической спецификацией, но она тесно связана с ISO/TR 27809.

Примечание — Планируется отменить ISO/TS 25238 и включить его в МЭК 80001.

5.1.13 МЭК 62366:2007 Медицинские приборы. Применение эргономического проектирования для медицинских приборов (IEC 62366:2007, Medical devices — Applicability of usability engineering to medical devices)

5.1.13.1 Область применения

Данный стандарт определяет процесс, который позволяет производителю проанализировать, установить, спроектировать, верифицировать и подтвердить соответствие пригодности к использованию при обеспечении безопасности медицинского прибора. Данный процесс эргономического проектирования

оценивает и смягчает последствия рисков, связанных с проблемами использования, а также с правильным использованием и ошибками при использовании, то есть с обычным использованием. Он может быть применен для идентификации, но не для оценки или снижения рисков, связанных с ненадлежащим использованием.

Примечание — В соответствии с целями настоящего стандарта пригодность к эксплуатации сводится к характеристикам пользовательского интерфейса. Этот стандарт не распространяется на принятие решений в клинических условиях, связанных с использованием медицинского устройства.

Если процесс эргономического проектирования, подробно описанный в настоящем стандарте, выполнен, и критерии приемки, указанные в плане проверки эксплуатационной пригодности, соблюдены, то остаточные риски, связанные с пригодностью к использованию медицинского оборудования, считаются приемлемыми, если отсутствуют объективные доказательства обратного согласно определению ИСО 14971.

5.1.13.2 Применимость/приемлемость риска

МЭК 62366 описывает процесс эргономического проектирования на очень высоком уровне и аналогичен подходу к менеджменту рисков, например описанному в ИСО 14971.

МЭК 62366 предназначен для производителей и разработчиков стандартов, а не для организаций-исполнителей, поэтому основное внимание уделяется прежде всего предпродажным стадиям жизненного цикла.

В традиционном смысле данный стандарт в наибольшей степени предназначен для медицинских приборов. Программное обеспечение упоминается только один раз в основной части стандарта (за исключением «программного обеспечения», являющегося частью определения медицинского устройства). Приложение D [которое по существу является ANSI/AAMI HE74.2001 Процесс проектирования для медицинских устройств с учетом человеческих факторов (Human factors design process for medical devices)] обеспечивает лучшую применимость, однако все приведенные примеры являются традиционными, ориентированными на устройства.

В центре внимания МЭК 62366 находится взаимодействие пользователя с автономным устройством, однако недостаточное внимание уделяется отношению пользовательского интерфейса к «информации» во взаимодействующих экосистемах, которая будет часто поступать из других объединенных систем. Он также ограничивает свое внимание «нормальным» использованием устройства, так как данный документ ориентирован на производителя. Обзор рисков человеческого фактора в более широком смысле, чем описано в МЭК 62366, будет полезен для стадий жизненного цикла.

5.1.13.3 Информация о жизненном цикле и уровне детализации

Данный стандарт распространяется на этапы проектирования и разработки жизненного цикла и применим на уровне компонентов и приложений программного обеспечения.

5.1.13.4 Связь (отношение)

Этот стандарт использует ИСО 14971:2007 для идентификации опасностей, остаточных рисков и других понятий, связанных с риском, а также заменяет МЭК 60601-1:2012 Общие требования к основной безопасности и неотъемлемым характеристикам медицинского электрооборудования (IEC 60601-1:2012, Medical electrical equipment requirements for basic safety and essential performance).

Примечание — ANSI/AAMI HE75.2009 Проектирование с учетом человеческого фактора. Проектирование медицинских приборов (Human factors engineering — Design of medical devices) дополняет HE74 (который является приложением МЭК 62366 и уделяет внимание процессам проектирования с учетом человеческого фактора, существующего на месте) и содержит рекомендации из области учета человеческого фактора/пригодности к эксплуатации. Представление, контекст и примеры являются преимущественно общепринятыми, ориентированными на медицинские приборы. Полезные элементы HE75, которые являются достаточно большими (около 475 с.), можно обнаружить во всех процессах испытания и обзоре принципов эргономического проектирования.

5.2 Распределение стандартов по их применению для стадий жизненного цикла и уровню детализации, рассматриваемого в них программного обеспечения

Рисунки 2—4 кратко описывают и позиционируют каждый стандарт по осям стадии жизненного цикла и уровню детализации. Для удобства просмотра стандарты распределены между двумя рисунками (рисунки 2 и 3), а на третьем рисунке представлены полностью (рисунок 4).

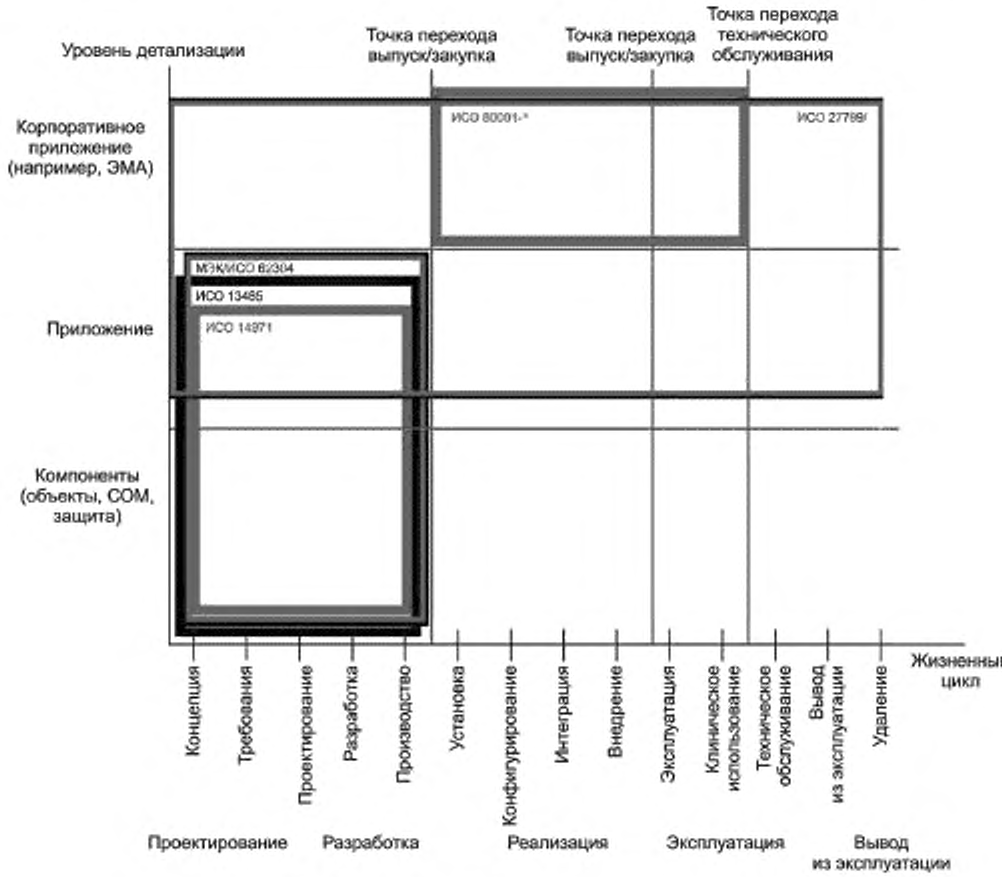


Рисунок 2 — Карта оценки стандартов (охватывает 5.1.6—5.1.10)

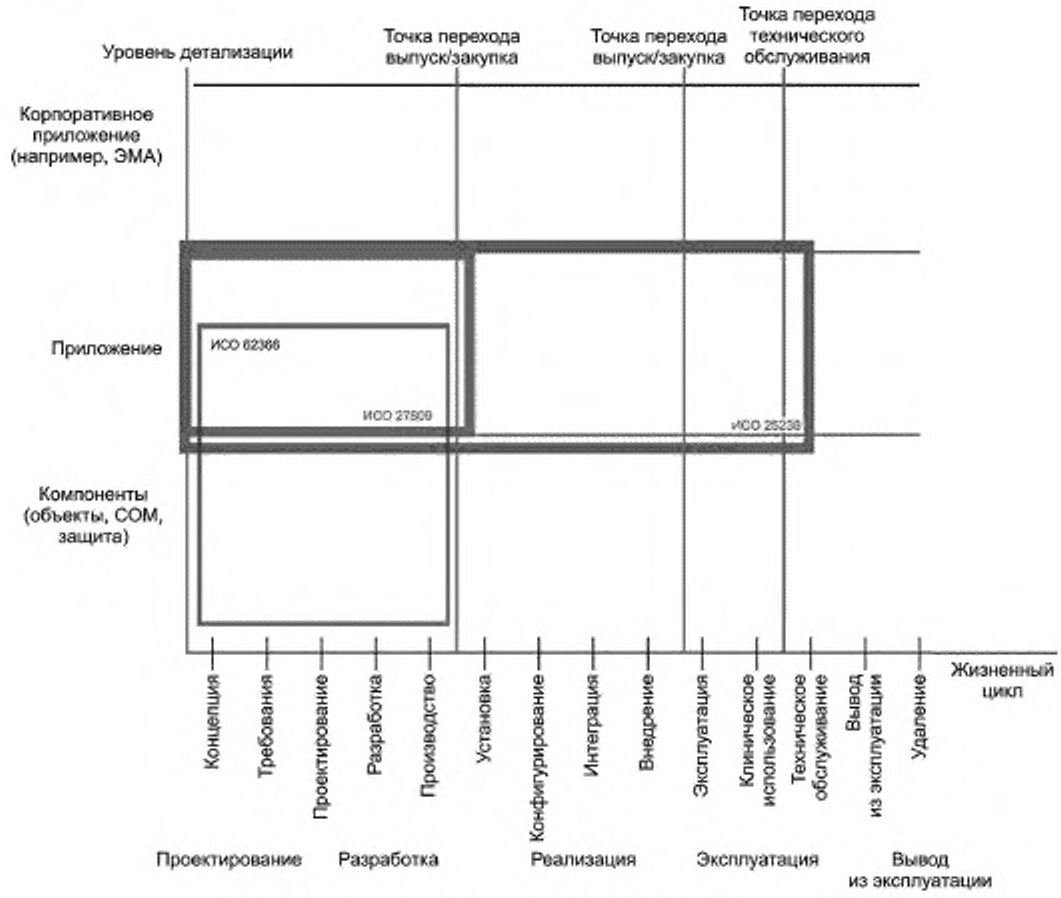


Рисунок 3 — Карта оценки стандартов (охватывает 5.1.11—5.1.13)

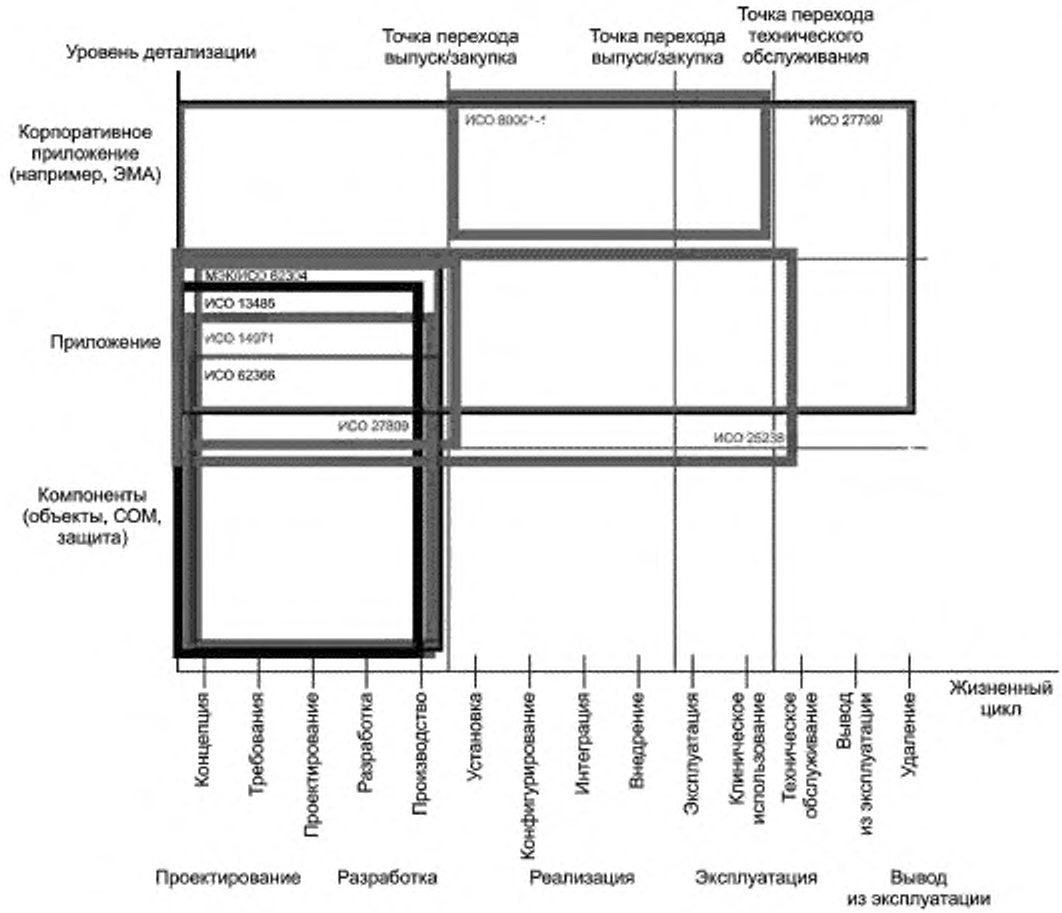


Рисунок 4 — Карта оценки стандартов (охватывает 5.1.6—5.1.13)

5.3 Анализ неохваченных и повторно рассмотренных вопросов при оценке стандартов

5.3.1 Общие положения

В настоящем подразделе описаны совпадения и пробелы в стандартах, указанных на рисунке 4, с целью обеспечить основу для общей оценки развития структуры стандартов для того, чтобы предоставить более согласованный подход к созданию безопасного медицинского программного обеспечения, в котором:

- повторно рассмотренные вопросы описаны в 5.3.2—5.3.4, обращая внимание на то, где множество стандартов рассматривают общие этапы жизненного цикла и имеют общую область применения программного обеспечения, и
- неохваченные вопросы описаны в 5.3.5—5.3.11, формируя руководящие указания по приоритету дальнейшей разработки стандартов.

Примечание — На момент подготовки настоящего стандарта специальная группа ИСО/ТК 215 и МЭК/ТК 62 ПК 62А активно работала над стандартами, связанными с медицинским программным обеспечением, посредством формирования и согласования принципов, терминов и определений.

5.3.2 Семейство стандартов ИСО 13485, МЭК 62304 и ИСО 14971, связанное с медицинским программным обеспечением

Эта группа стандартов связана между собой целью и стадией проектирования программного обеспечения медицинского оборудования. ИСО 13485 и ИСО 14971 решают вопросы среды управления,

которая является основополагающей для организаций, разрабатывающих продукты для медицинских устройств. ИСО 13485 сосредоточен на требованиях к менеджменту качества, при этом МЭК 62304 сосредоточен на требованиях к жизненному циклу. В центре внимания ИСО 14971 находится применение менеджмента рисков (идентификация опасностей, определение и оценка рисков и управление рисками).

Если все эти стандарты вместе применить к общим стадиям проектирования и разработки жизненного цикла медицинского программного обеспечения, то это семейство стандартов позволит сформировать руководящие указания по обеспечению безопасности медицинского программного обеспечения.

5.3.3 Жизненный цикл в МЭК 62304 и ИСО/МЭК 12207

Эти два стандарта рассматривают вопросы жизненного цикла, предоставляя две разные цели. ИСО 62304 в целом нацелен на применение системы менеджмента качества к стадиям жизненного цикла, связанным с производителем программного обеспечения медицинского оборудования, а ИСО/МЭК 12207 предоставляет широкий, общий подход к процессам, действиям и задачам, применимым к любому программному обеспечению, т. е. некоторую «дорожную карту» для организационных процессов, необходимых на всем жизненном цикле программного обеспечения. Оба стандарта применяются для обеспечения безопасности медицинского программного обеспечения.

5.3.4 Вопросы рисков в ISO/TS 25238, ISO/TS 27809 и ИСО 14971

Эти три стандарта предоставляют как специальные, так и общепринятые меры по менеджменту рисков, которые обеспечивают безопасность медицинского программного обеспечения.

ИСО 14971 ориентирован на процесс и включает в себя процессы выявления опасностей, определения, оценки и управления рисками, а также контроля эффективности средств управления программным обеспечением медицинского оборудования.

ISO/TR 27809 ориентирован на меры управления медицинским программным обеспечением и идентификацию соответствующих стандартов по менеджменту рисков, обеспечивающих меры управления для приложений медицинского программного обеспечения. Настоящий стандарт предоставляет дополнительный и обновленный материал к ISO/TR 27809.

ISO/TR 25238 является стандартом по менеджменту рисков, предоставляющим руководящие указания по классификации (на основе анализа и категоризации) опасностей и рисков для пациентов, связанных с использованием приложений медицинского программного обеспечения.

5.3.5 Неохваченные вопросы в стандартах, рассматривающих риски и процессы корпоративного приложения

В то время как стандарты серии МЭК 80001 помогают решать вопросы, связанные с применением менеджмента рисков для ИТ-сетей, объединяющих медицинские приборы, предметные области процесса обеспечения безопасности и совокупного риска для медицинского программного обеспечения только выиграют за счет специального(ых) стандарта(ов), отражающего(их) передовые практические методы, применимые к более сложным и развитым средам приложений масштаба предприятия, с серьезным акцентом на клинические риски и связанные с ними процессы. Аналогично, несмотря на то что ИСО/МЭК 15288:2008 Проектирование систем и программного обеспечения. Процессы жизненного цикла системы (ISO/IEC 15288:2008, Systems and software engineering — System lifecycle processes), разработанный СТК 1/ПК 7, является основополагающим стандартом по жизненному циклу системы, он не был разработан специально для медицинского программного обеспечения.

5.3.6 Отсутствие руководств, связанных с применением менеджмента рисков для реализации, эксплуатации и вывода из эксплуатации медицинского программного обеспечения

В то время как ISO/TS 25238 и ISO/TR 27809 описывают риски, связанные с медицинским программным обеспечением, существует необходимость в конкретном стандарте, в котором были бы представлены руководящие указания по применению общих стандартов по менеджменту рисков специально для стадии реализации медицинского программного обеспечения, а также руководящие указания по расширению и применению ИСО 14971 для реализации, эксплуатации и вывода из эксплуатации компонентов и приложений медицинского программного обеспечения (дополнительно к руководящим указаниям уже имеющимся в IEC/TR 80002-1). Кроме того, такое руководство должно делать упор на клиническую сферу.

5.3.7 Отсутствие руководств, связанных с учетом человеческих факторов при реализации и эксплуатации медицинского программного обеспечения

Существующие стандарты, рассматривающие человеческие факторы, как международные, так и национальные, как правило, ориентированы на предоставление указаний по организации процессов, которым необходимо следовать для успешной интеграции итеративного метода проектирования с ориентацией на пользователя в проектировании и разработке систем здравоохранения.

Интеграция метода, основанного на человеческих факторах, в культуру проектирования и разработки организации направлена на увеличение безопасности продуктов.

ИСО 9241 является стандартом, состоящим из нескольких частей, которые всесторонне описывают различные элементы эргономики взаимодействия человека с компьютером.

МЭК 62366:2007 Медицинские приборы. Применение эргономического проектирования для медицинских приборов (IEC 62366:2007, Medical devices — Application of usability engineering to medical devices) и связанный с ним ANSI/AAMI HE75.2009 Проектирование с учетом человеческого фактора. Проектирование медицинских приборов (Human factors engineering — Design of medical devices) определяют для производителя процесс для анализа, определения, проектирования, верификации и подтверждения соответствия пригодности к эксплуатации, так как он относится к безопасности медицинского прибора. Те же процессы применимы и к медицинскому программному обеспечению.

Однако учет человеческих факторов на этапах реализации и эксплуатации медицинского программного обеспечения является важным для других заинтересованных сторон (системных интеграторов, организаций, предоставляющих медицинские услуги, и т. д.) для решения вопросов, касающихся человеческих факторов в таких областях, как менеджмент рисков, подготовка, обучение и в области должностных функций. В частности, аспекты человеческого фактора, касающиеся команды, организации и политики, применимы на стадиях реализации и эксплуатации жизненного цикла медицинского программного обеспечения. Также полезно создание руководств по учету таких человеческих факторов для указанных стадий.

5.3.8 Отсутствие руководств по безопасности при проектировании, разработке, реализации и эксплуатации клинического рабочего процесса

Проектирование и разработка клинического программного обеспечения могут выполняться, используя общие стандарты по пригодности к эксплуатации, применяемые к медицинским приборам, но, как отмечалось выше, отсутствуют руководства по менеджменту рисков, процессам проектирования с учетом человеческих факторов и менеджменту качества, применимые для модернизации клинического рабочего процесса. Существуют значительные риски, связанные с применением медицинского программного обеспечения к неоцененным (и в некоторых случаях непроанализированным) клиническим рабочим процессам. При оценке клинического рабочего процесса необходимо учитывать широкий, многоуровневый набор человеческих факторов. Дополнительные указания по документальному оформлению клинического рабочего процесса, по анализу и модернизации, а также по безопасным методам будут полезны для всех стадий жизненного цикла медицинского программного обеспечения.

5.3.9 Отсутствие руководств по своду правил для содействия безопасности системы электронного здравоохранения

Должен быть идентифицирован и описан полный набор передовых практических методов, с соответствующим упором на клиническую сферу, что охватывает социально технологический или экосистемный подход к безопасности медицинского программного обеспечения. Такой набор будет включать принципы и процессы, эффективные для повышения безопасности медицинского программного обеспечения, и предоставлять необходимые руководящие указания для этой все более важной области безопасности пациента, включая применение руководящих указаний, представленных в настоящем стандарте. Кроме того, это руководство должно сосредоточиваться на клинической сфере.

В отчете IOM 2011 (Международная организация по миграции) Информационные технологии в здравоохранении и безопасность пациента. Строительство безопасных систем для обеспечения лучшего ухода (Health IT and Patient Safety: Building Safer Systems for Better Care) отмечено, что безопасность является характеристикой социально-технической системы и что отказы на уровне системы почти всегда возникают вследствие случайных комбинаций отказов компонентов [10]. Эта комбинация отказов компонентов подчеркивает сложность медицинского программного обеспечения и важность использования универсального подхода к применению передовых методов на всех стадиях жизненного цикла программного обеспечения и для всех доступных предметных областей (люди, процесс, внешняя среда, организация и технологии).

5.3.10 Отсутствие руководств по верификации и испытанию конфигурации программного обеспечения

В ходе исследования и оценки существующих стандартов, которые могли бы быть использованы для повышения безопасности медицинского программного обеспечения, обнаружилось, что руководств по верификации и испытанию конфигурации программного обеспечения недостаточно. Программное обеспечение может обладать широким набором параметров, которые должны быть сконфигурированы в соответствии с конкретными потребностями организации, отвечающей за внедрение.

Так как во время разработки не все возможные варианты параметров могут быть проверены, существует остаточный риск для безопасности, который должен быть снижен. Для специалистов по внедрению необходимо руководство по верификации и проведению испытаний конкретной конфигурации на ее безопасность для пациента.

5.3.11 Отсутствие руководств по дополнительным аспектам разработки, реализации и эксплуатации безопасного программного обеспечения

В настоящее время отсутствует специальный стандарт для медицинского программного обеспечения, который дает указания о том, что требуется для обеспечения безопасности медицинского программного обеспечения по отношению к следующему:

- функциональные свойства, относящиеся к безопасности;
- нефункциональные характеристики, например стабильность, надежность;
- маркировка, включая инструкции по применению.

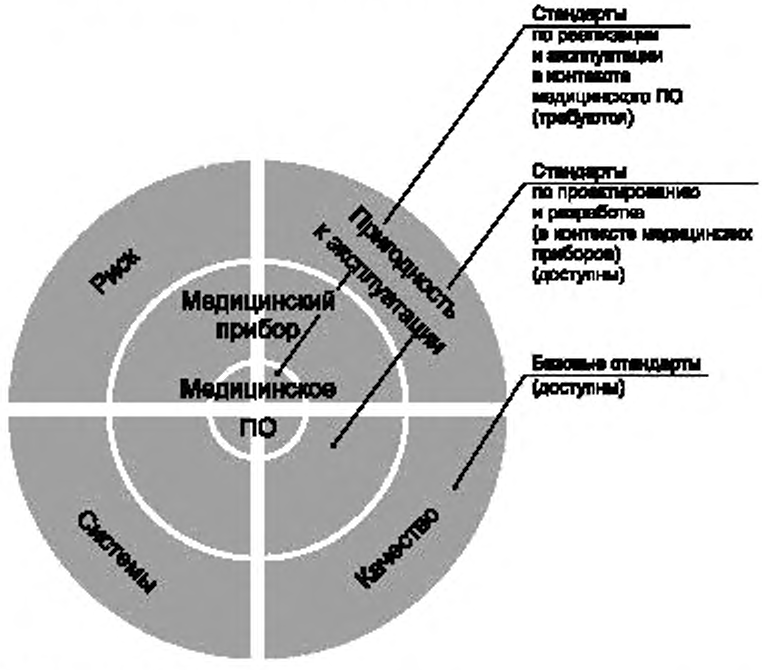
Все это дает гарантию безопасности медицинского программного обеспечения.

5.4 Стандарты по обеспечению безопасности медицинского программного обеспечения. Руководство по реализации и использованию

5.4.1 Общие положения

Руководство по имеющимся стандартам для обеспечения безопасности в медицинском программном обеспечении, т. е. информация, которая является практической, содержательной, реализуемой и полезной, непременно будет обширным, и, естественно, кратким. Можно дать окончательный ответ на вопрос, «какие стандарты нужно использовать для обеспечения безопасности медицинского программного обеспечения», но необходимо решить вопросы (перечисленные в 5.3) перед тем, как ясное(ые), комплексное(ые) решение(я) будет(ут) реализовано(ы). В ожидании данного результата отдельные лица и организации уже могут использовать информацию, содержащуюся в настоящем стандарте, и применять ее к своим конкретным ситуациям и обстоятельствам, чтобы способствовать пониманию и повышению безопасности медицинского программного обеспечения.

Такое руководство достаточно полно охарактеризовано на рисунке 5.



ПО – программное обеспечение.

Рисунок 5 — Руководство по стандартам безопасности программного обеспечения

Рисунок 5 отражает следующее:

- базовые стандарты доступны и предоставляют комплексную основу для обеспечения безопасности медицинского программного обеспечения. Эти стандарты в первую очередь используют разработчики стандартов для контекстных сфер, а также разработчики крупномасштабного программного обеспечения;

- стандарты, разработанные для медицинских приборов, предоставляют рабочую основу для обеспечения безопасности при проектировании и разработке медицинского программного обеспечения;

- существует множество пробелов в стандартах, необходимых для обеспечения безопасности при реализации и эксплуатации медицинского программного обеспечения;

- несмотря на то что некоторые общие подходы к жизненному циклу (ИСО/МЭК 12207), классификации опасностей и рисков (ISO/TS 25238), стандарты по менеджменту безопасности (ИСО 27799), а также стандарты для медицинских устройств по менеджменту рисков в ИТ-сети (IEC/TR 80001-1) поддерживают стадии реализации и эксплуатации жизненного цикла, все они являются конкретными и целенаправленными «частями» процесса обеспечения безопасности медицинского программного обеспечения. Они полезны, но их недостаточно для решения всех проблем в контексте реализации и эксплуатации медицинского программного обеспечения (см. 5.4.2 для получения дополнительной информации).

Остальная часть данного подраздела содержит дополнительные важные рекомендации, полученные в ходе разработки настоящего стандарта.

5.4.2 Стандарты, рассматривающие неохваченные вопросы, послужат основой для руководства по обеспечению безопасности медицинского программного обеспечения.

Существует большое количество базовых стандартов по жизненному циклу медицинского программного обеспечения, в том числе по менеджменту качества, разработке программного обеспечения, управлению ИТ-службами, а также стандартов по медицинским приборам, ориентированных на определенную область применения (в том числе соответствующее программное обеспечение медицинского оборудования), и менеджменту рисков. Тем не менее основные принципы и методы для обеспечения безопасности медицинского программного обеспечения либо доступны только в масштабе одной страны, например клинические стандарты по менеджменту рисков в Великобритании (5.4.4), либо отсутствуют. Сторонам, заинтересованным в безопасности медицинского программного обеспечения, приходится создавать собственные нормы и практики, основанные на вышеуказанных категориях стандартов. Важной функцией разработчиков международных стандартов является предоставление этих принципов и методов на международном уровне для общего использования, в области медицинского программного обеспечения, уделяя особое внимание стадиям реализации и эксплуатации жизненного цикла медицинского программного обеспечения.

5.4.3 Стандарты, рассматривающие неохваченные вопросы, связанные со стадиями реализации и эксплуатации жизненного цикла

Существующие стандарты по безопасности медицинского программного обеспечения серьезно помогли производителям программного обеспечения, но существуют пробелы для стадий реализации и эксплуатации жизненного цикла.

Стандарты по рискам и процессам в основном сосредоточены на производстве программного обеспечения, по сравнению с другими стадиями жизненного цикла. В противоположность этому стандарты, которые применяются ко всему спектру жизненного цикла, часто предоставляют более общие подходы и не рассматривают риски или значительно сосредоточенные на свою область определения и цель. Например, ИСО/МЭК 12207 достаточно подробно рассматривает весь жизненный цикл, а ИСО 27799 и серия IEC/TR 80001 сосредоточены на безопасности и подключении медицинских устройств к ИТ-сети, соответственно.

Основные положения ИСО 31000 являются исходной точкой для разработки стандартов по менеджменту рисков и руководством, «выходящим за пределы» стадий проектирования и разработки жизненного цикла, что существенно шире того, что рассматривалось в ИСО 14971 и в сопутствующем IEC/TR 80002-1.

5.4.4 Недостаток клинических стандартов по безопасности

Стандарты по менеджменту клинических рисков, а также по проектированию и разработке клинического рабочего процесса отсутствуют. Существует два национальных стандарта НЗС Великобритании, которые применяют менеджмент рисков как к производству, так и к внедрению и использованию медицинского программного обеспечения. Этими стандартами являются:

- ISB 0129 Управление клиническими рисками. Его применение при производстве медицинских ИТ-систем. Руководство по внедрению [11] (ISB 0129 Clinical Risk Management — Its Application in the Manufacture of Health IT Systems — Implementation Guidance);

- ISB 0160 Управление клиническими рисками. Его применение при внедрении и использовании ИТ-систем. Руководство по внедрению [12] (ISB 0160 Clinical Risk Management — Its Application in the Deployment and Use of Health IT Systems — Implementation Guidance).

Первые последователи программ обеспечения безопасности медицинского программного обеспечения могут использовать методы и принципы этих двух национальных стандартов в процессе выполнения разработки, проводимой международными организациями, разрабатывающими стандарты.

5.4.5 Полезность и применимость «экосистемного» подхода к стандартам, обеспечивающим безопасность медицинского программного обеспечения

Работа, которая следует за разработкой стандартов, направлена на создание медицинского программного обеспечения и связанных с ним стандартов по безопасности для различных предметных областей или секторов всей экосистемы. Следуя отчету IOM (ноябрь 2011) по информационным технологиям в здравоохранении и безопасности пациентов, аналогичным образом сосредоточенном на социально-технологической системе, лежащей в основе нежелательных явлений, связанных с информационными технологиями в здравоохранении, становится ясно, что любые разработки стандартов, относящихся к медицинскому программному обеспечению, включая программное обеспечение для медицинских приборов, должны быть построены на правильном представлении «системы», которая выходит за пределы технологии. Области окружающей среды, организация, процесс и люди, наряду с технологией разработки аппаратных средств и программного обеспечения, должны рассматриваться как целостный, интерактивный подход на протяжении всех стадий проектирования, разработки, реализации и эксплуатации.

5.4.6 Терминология медицинского программного обеспечения нуждается в дальнейшей доработке

Существует множество терминов и связанных определений, которые определяются, обновляются или обсуждаются при разработке стандартов и в организациях по разработке стандартов (SDO) и в соответствующих комитетах. Такие термины, как «автономное программное обеспечение», «программное обеспечение систем здравоохранения», «программное обеспечение медицинских приборов» и «медицинский программный продукт» и все другие связанные с ними понятия, имеют различные значения в зависимости от страны и даже от организации по разработке стандартов.

Для органов здравоохранения как международных, так и национальных комитет-членов, соответствующих технических комитетов ИСО (ТК 215 и ТК 62) и связанных с ними координационных организаций (СТК 1) было бы важно создать целостную, общую и приемлемую совокупность терминов, используемых в контексте медицинского программного обеспечения. Эта созданная совокупность терминов также может быть соединена и хорошо увязана с «экосистемным» или «социально-технологическим» подходом, описанным в 5.4.5.

5.4.7 Стандарты, связанные с риском, процессом и предметной областью, служат точкой отсчета.

В настоящем стандарте были определены как применимые для рассмотрения рисков, связанных с безопасностью медицинского программного обеспечения, следующие стандарты:

- ИСО 13485;
- ИСО 14971 и/или ISO/TS 25238;
- МЭК 62304;
- ИСО/МЭК 12207;
- МЭК 62366;
- IEC/TR 80001-1;
- ИСО 27799.

Несмотря на то что данный список стандартов является исходной точкой, для многих заинтересованных сторон он все еще кажется слишком неупорядоченным. Углубленное изучение стандартов, указанных в этом списке, может обеспечить ценные сведения по защите безопасности пациентов, однако видна необходимость в том, чтобы лучше рассмотреть специфику медицинского программного обеспечения, и в том, чтобы обеспечить взаимное соответствие между различными стандартами. Кроме того, эти стандарты не уделяют большого внимания безопасности пациента и не полностью согласуются друг с другом. К сожалению, это демонстрирует характер развития стандартов во времени, так как их разработка осуществляется несколькими рабочими группами и заинтересованными лицами.

Важно, что стратегическое планирование деятельности ИСО/ТК 215 учитывало информацию, представленную в настоящем стандарте, в частности в 5.3, при рассмотрении приоритетов своих рабочих групп, планов и новых рабочих тем. Кроме того, тесное сотрудничество этих ТК в ИСО и МЭК, которые уже принимали участие в создании существующих стандартов, особенно ИСО ТК 210, ИСО ТК 215 и МЭК ТК 62, должно продолжаться.

Приложение А
(справочное)

Повышение безопасности пациентов благодаря инвестициям в разработку медицинских программ

На данный момент гораздо больше известно о первопричинах нарушений безопасности пациентов, благодаря проведению постоянных и усовершенствованых исследований, улучшенной системе уведомления (составления отчетов) и более ориентированной на безопасность клинической культуры, которая сложилась за последнее десятилетие с момента выпуска отчета IOM под названием «Человеку свойственно ошибаться. Создание более надежной системы здравоохранения». Акцентирование внимания на повышении безопасности пациента и качестве с целью избежать ненужных смертей, связанной с необходимостью улучшения качества, а также на эффективности и доступности систем здравоохранения многих стран привело к значительным инвестициям в медицинские информационные проекты. К ним относятся клинические информационные системы, электронные медицинские карты, которые объединяют информацию о пациенте из различных медицинских учреждений и организаций, и усовершенствованная поддержка принятия решений для клинических функций (например, назначений препаратов), которые являются общими источниками инцидентов, связанных с безопасностью пациентов.

Эти информационные системы здравоохранения предоставляют множество возможностей для повышения безопасности пациентов, в том числе:

- сокращение фармакологических ошибок путем предупреждения врачей о клинических рисках, таких как известные аллергии и противопоказания к применению лекарственных препаратов посредством системы поддержки принятия решения по лекарственным препаратам;
- сокращение «путаницы» и «дублирования информации» путем своевременной и точной идентификации пациентов;
- улучшение обмена клинической информацией;
- эффективное упорядочивание диагностических испытаний, а также эффективная отчетность и обмен результатами;
- увеличение продолжительности ухода за пациентом;
- сокращение географических барьеров для получения доступа с помощью телемедицины;
- улучшение результатов за счет поддержки протоколов по медицинскому уходу;
- своевременное предоставление данных для рентгеноскопии, выявление эпидемий, исследование и распределение ресурсов;
- мотивирование людей на улучшение своего здоровья.

Приложение В
(справочное)

Анализ стандартов с позиции жизненного цикла программного обеспечения

Таблица В.1 — Стандарты, рассмотренные с позиции жизненного цикла программного обеспечения

Стандарт	IEEE 1074:2006	МЭК 62304:2006	ИСО/МЭК 12207:2008	ISO/TR 27809:2007	IEC/TR 80001-1
Предметная область	Общая	Медицинские приборы	Общая	Общая	Медицинские приборы
Тип	Программное обеспечение	Программное обеспечение	Программное обеспечение (стадии системы не учитывались)	Программное обеспечение	ИТ-сети
Концепция	Исследование концепции				Запрос на внесение изменений или создание медицинской ИТ-сети (применимое разрешение на внесение изменений)
Требования	Требования к программному обеспечению	План разработки программного обеспечения. Анализ требований к программному обеспечению	Анализ требований к программному обеспечению		
Проектирование	Проектирование	Проектирование архитектуры программного обеспечения. Детальное проектирование программных средств	Проектирование архитектуры программного обеспечения. Детальное проектирование программных средств	Проектирование	План проекта (документ ответственной организации)
Разработка	Реализация	Реализация программного модуля. Интеграция программного обеспечения и испытание интеграции	Конструирование программного обеспечения. Интеграция программного обеспечения. Квалификационное испытание программного средства. Принятие программного обеспечения	Разработка	
Производство				Производство. Создание дистрибутива	

Окончание таблицы В.1

Стандарт	IEEE 1074:2006	МЭК 62304:2006	ИСО/МЭК 12207:2008	ISO/TR 27809.2007	IEC/TR 80001-1
Предметная область	Общая	Медицинские приборы	Общая	Общая	Медицинские приборы
Тип	Программное обеспечение	Программное обеспечение	Программное обеспечение (стадии системы не учитывались)	Программное обеспечение	ИТ сети
Установка	Установка	Тестирование системы программного обеспечения	Установка программного обеспечения (интеграция системы) (квалификационные испытания системы)	Установка	Выполнение менеджмента рисков (MP). Обновленный файл MP. Оценивание остаточных рисков
Конфигурирование					Разрешение на внесение изменений. Управление конфигурациями
Интеграция					
Реализация		Выпуск программного обеспечения			Ввод в действие
Эксплуатация	Эксплуатация и поддержка		Эксплуатационное использование программного обеспечения		Контроль и управление событиями
Клиническое применение					
Техническая поддержка	Техническая поддержка	Техническая поддержка программного обеспечения	Техническая поддержка программного обеспечения	Усовершенствование/ управление версиями/ обновление	
Вывод из эксплуатации	Удаление				
Уничтожение			Уничтожение программного обеспечения		

В.1 Анализ общего подхода

Следующий анализ основан на использовании вышеупомянутых стандартов с точки зрения жизненного цикла.

В.1.1 Концепция

- Стадия описана как минимум в одном стандарте.
- Является исходной точкой для разработки программного обеспечения с элементами риска, если крайне заинтересованные стороны не участвуют в начальном построении концепции.

В.1.2 Требования

- Стадия описана в нескольких стандартах.
- Должны быть использованы стандартные процессы: примеры использования, карты событий, диаграммы взаимодействия и т. д.
- Стадия должна начинаться с рассмотрения требований к данным (начинается на этой стадии и продолжается на последующих).
- Выбор/определение элементов данных, методов моделирования данных, определений, кодировок, шаблонов и т. д.

В.1.3 Проектирование

- Стадия является общепринятой во многих стандартах.
- Должна включать архитектуру, алгоритмы, компоненты, исходную документацию, подтверждение соответствия.
- Должна включать словарь для идентификации (перевода, преобразования) (снижать риски путем обеспечения регистрации клинических данных точным, структурированным и своевременным образом или, по крайней мере, перевода этих данных, осуществляемого таким образом, чтобы их значение сохранялось при разделении/передаче рисков).

В.1.4 Разработка

- Стадия описана в других стандартах или кратко описывает множество других стадий.
- Нормативный сектор управляемого устройства рассматривает разработку программного обеспечения как производственное действие (промышленное, или механическое, или машинное производство).
- Слово «производство» (manufacture) согласовано с языком, используемым для нормативных положений, особенно тех, которые основаны на семействе стандартов ИСО 9000.
- Программное обеспечение (информационные системы) может регулироваться с целью защиты безопасности пациента разными способами, но информационные системы не просто произведенные устройства.
- Государственный сектор рассматривает разработку программного обеспечения как гибкое, сложное, программируемое и обладающее множеством настроек действие.
- Подходы к разработке программного обеспечения включают в себя: нисходящий/восходящий принцип, каскадную модель, спиральную модель, хаотичную модель, прототипирование, эволюционирующее прототипирование, итеративную и инкрементальную разработку, экстремальное программирование и т. д.

В.1.5 Производство, создание дистрибутива, выпуск и поставка

- Стадия описана как минимум в одном стандарте.
- В некоторых случаях рассматривается как часть «ввода в эксплуатацию».
- Имеет первостепенное значение с точки зрения выпуска, причем выпуск и поставка являются двумя смежными ключевыми событиями, где существует переход риска (между организацией, которая предоставляет программное обеспечение и покупателем программного обеспечения).
- Стандарты по рискам и применимые стандарты для каждого отдельного выпуска и поставки различаются.

В.1.6 Установка, конфигурирование, интеграция, реализация и ввод в эксплуатацию

- Стадия установки описана в нескольких стандартах.
- Стадии между выпуском и поставкой и приемкой и вводом в действие могут быть объединены. Необходимо различать установку, конфигурирование, интеграцию, реализацию и ввод в эксплуатацию, чтобы не придать им иного значения.
- Маловероятно, что разные стандарты будут применяться к подстадиям реализации или ввода в эксплуатацию.
- Степень персонификации и конфигурирования между поставкой и вводом в действие в большинстве случаев является значительной и затратной. Существует часть этой стадии жизненного цикла, которая также включает в себя подготовку документации для вводимой в эксплуатацию системы и обучение пользователей.
- Компоненты обучения и поддержки особенно важны для снижения рисков безопасности и должны использовать подходы, представленные:
- в специальных стандартах, связанных с безопасностью, которые включают сертификационные испытания, обмен сообщениями, словарь, конфиденциальность и безопасность, установление личности пользователя/аутентификацию/авторизацию, управление согласованием; и
- стандартах на системы для обеспечения соответствия стандартам медицинских организаций по эксплуатации и уходу, рабочим процессам, персоналу, требованиям к составлению отчетности и учету, природоохранным требованиям, требованиям к совместимости, а также управлению, технической поддержке, обучению и т. д.

В.1.7 Приемка и ввод в эксплуатацию

- Не описывается ни в одном из известных стандартов, связанных с жизненным циклом.
- Является событием, в отношении которого существует мнение, связанное с передачей риска, о том, что на этапе ввода в эксплуатацию заказчик берет на себя большую часть от общего риска. Кроме того, на этапе ввода в эксплуатацию существует кардинальное изменение профиля риска. Теперь программное обеспечение используется в клинической практике, поэтому присутствует возможность возникновения потенциального вреда для пациентов.

В.1.8 Эксплуатация

- Стадия описана в нескольких стандартах.
- Различие между эксплуатацией и технической поддержкой состоит не в том, что они являются разными стадиями жизненного цикла, а в том, что в ходе этих стадий жизненного цикла существуют различные функции, которые выполняют оператор и разработчик.
- Таким образом, существуют два разных «получателя» риска.

В.1.9 Клиническое использование

- Стадия не описывается ни в одном из известных стандартов.
- На данной стадии происходит кардинальное изменение профиля риска (характеристик: пригодности к использованию, семантической, основанных на данных исследований и т. д.), а также переход рисков от специалиста по реализации медицинской информационной технологии/оператора к пользователю медицинской информационной технологией, обычно к врачу.

- Существует необходимость следить за тем, чтобы клиническая информация, т. е. «информация о человеке, касающаяся его здоровья или здравоохранения» (см. ИСО 13606-1:2008), была точно, структурированно и своевременно зафиксирована или преобразована так, чтобы смысл надлежащим образом сохранялся при ее совместном использовании/передаче.

В.1.10 Техническая поддержка

- Стадия описана во многих стандартах.
- Различие между эксплуатацией и технической поддержкой состоит не в том, что они являются разными этапами жизненного цикла, а в том, что в ходе этих этапов жизненного цикла существуют различные функции, которые выполняют оператор и разработчик.
- Таким образом, существуют два разных «получателя» риска.
- Важно понимать, что «обычный ход деятельности» включает в себя значительные эволюционные изменения в системах, которые могут присутствовать в них на протяжении десятилетий, но вовсе не обязательно будет выглядеть так же в том случае, когда системы впервые начали использоваться. Техническое обслуживание (как разработка) является важной стадией.

В.1.11 Вывод из эксплуатации

- Стадия описана как минимум в одном стандарте.
- Стадия требует передачи обслуживания пациента и клинической информации из одной системы в другую.
- Вопросы безопасности на данной стадии касаются возможности переносимости, т. е. передачи данных из одной системы в другую.

В.1.12 Удаление

- Стадия описана как минимум в одном стандарте.

Приложение С
(справочное)

Информация об области применения стандартов СТК 1, касающихся безопасности

С.1 ИСО/МЭК 15026 Разработка систем и программного обеспечения. Обеспечение систем и программного обеспечения (ISO/IEC 15026, Systems and software engineering — Systems and software assurance)

С.1.1 Часть 1. Понятия и словарь

Часть 1 определяет термины, понятия и их связь, создавая основы для общего понимания понятий и принципов, важных для ИСО/МЭК 15026. ИСО/МЭК 15026 не содержит информацию о непрерывном использовании и управлении службами.

С.1.2 Часть 2. Обоснование гарантии

Часть 2 определяет минимальные требования к структуре и содержанию обоснования гарантии. Обоснование гарантии включает требования высокого уровня о свойствах системы или изделия, систематическое обоснование относительно каждого из этих требований, а также доказательства и явно выраженные допущения, лежащие в основе этого обоснования. Рассуждая о многоуровневой иерархии требований, данное структурированное обоснование объединяет требования высокого уровня с доказательствами и допущениями.

Обоснования гарантии, как правило, разработаны для поддержки требований в таких областях, как безопасность, надежность, ремонтная технологичность, учет человеческих факторов, функциональность и защита, хотя эти обоснования гарантии часто называются более конкретными названиями, например обоснование безопасности или обоснования надежности и ремонтопригодности (R&M).

С.1.3 Часть 3. Уровни целостности системы

Часть 3 определяет понятие уровней целостности и соответствующие требования к уровню целостности, которые необходимо соблюдать, с целью показать, что уровень целостности достигнут. Она устанавливает требования и рекомендует методы определения и использования уровней целостности и требований к ним, включая присвоение уровней целостности системам, программным продуктам, их элементам и соответствующим внешним связям.

Стандарт применим к системам и программному обеспечению и предназначен для использования следующими лицами:

- юридические лица, определяющие уровни целостности, например отраслевые и профессиональные организации, организации по стандартизации и государственные учреждения;
- пользователи уровней целостности, например разработчики и специалисты по техническому обслуживанию, поставщики и покупатели, пользователи и эксперты по оценке систем или программного обеспечения, а также организационной и технической поддержке систем и/или программных продуктов;
- поставщики и покупатели, подписавшие соглашения, например для оказания помощи в обеспечении характеристик безопасности, экономического положения или защиты после установки системы или продукта.

ИСО/МЭК 15026-3 не задает определенный набор уровней целостности или требований к уровню целостности либо то, каким образом использование уровней целостности будет интегрировано с целой системой или процессами стадии разработки программного обеспечения его жизненного цикла.

Часть 3 может использоваться отдельно или с другими частями ИСО/МЭК 15026. Она может быть использована с различными техническими или специализированными методами анализа рисков и подходами к разработке. Использование уровней целостности в соответствии с указаниями, приведенными в данной части, не требует обоснования гарантии, как указано в части 2. Тем не менее уровни целостности и обоснования гарантии могут взаимодействовать, и пути для достижения этого описаны.

С.2 ИСО/МЭК 12207:2008 Разработка систем и программного обеспечения. Процессы жизненного цикла программного обеспечения (ISO/IEC 12207:2008, Systems and software engineering — Software life cycle processes)

Настоящий международный стандарт устанавливает общую структуру для процессов жизненного цикла программного обеспечения и применим к приобретению систем и программных продуктов и служб, закупке, разработке, эксплуатации, технической поддержке и утилизации программных продуктов и части программного обеспечения системы несмотря на то, осуществляется ли это внутри или извне для организации.

Он также предоставляет процесс, который может быть использован для определения, управления и совершенствования жизненного цикла программного обеспечения. Включает 123 страницы и является вторым изданием, впервые опубликованным в рамках ИСО в 1995 г. Многое в данном стандарте заимствовано из предыдущих изданий US-DoD MIL-STD и работы, проведенной в IEEE.

С.3 ИСО/МЭК 26702:2007 Разработка системы. Управление и применение процессов разработки систем (ISO/IEC 26702:2007, Systems engineering — Application and management of the systems engineering process)

Данный международный стандарт, состоящий из 87 страниц и являющийся первым изданием, определяет межотраслевые задачи, которые требуются в ходе всего жизненного цикла системы для преобразования потребностей покупателей, а также требований и ограничений в системные решения.

Кроме того, он определяет требования для процесса проектирования системы и его применение на протяжении всего жизненного цикла продукта. ИСО/МЭК 26702 уделяет большое внимание инженерно-техническим мероприятиям, необходимым для руководства разработкой изделия, обеспечивая при этом надлежащую разработку изделия для того, чтобы сделать его доступным для производства, приобретения, эксплуатации, обслуживания и в конечном итоге удаления без излишнего риска для здоровья или окружающей среды.

С.4 ИСО/МЭК/ТС 15504-10:2011 Информационные технологии. Оценка процессов. Часть 10. Расширение безопасности (ISO/IEC/TS 15504-10:2011, Information technology — Process assessment — Part 10: Safety extension)

ИСО/МЭК 15504 предоставляет общий подход для оценки процессов. Этот общий подход может использоваться организациями, участвующими в планировании, менеджменте, контроле, управлении и в улучшении процессов приобретения, закупки, разработки, эксплуатации, развития и поддержки изделий и услуг.

Опубликованные в ИСО/МЭК 15504 модели оценки процесса для систем и программного обеспечения в настоящее время не предоставляют достаточную основу для осуществления оценки возможностей процессов при разработке сложных систем, связанных с безопасностью.

Разработка систем, связанных с безопасностью, требует специализированных процессов, методов, навыков и опыта. Необходимо расширение процесса (расширение безопасности) в области менеджмента безопасности, проектирования средств обеспечения безопасности и квалификации по эксплуатационной безопасности. ISO/IEC/TS 15504-10 представляет эти расширения в качестве трех описаний процессов:

- менеджмента безопасности;
- проектирования средств безопасности;
- сертификации безопасности.

Цель ISO/IEC/TS 15504-10 не состоит ни в обеспечении способа для верификации соблюдения одного или нескольких стандартов по безопасности, специализированных для определенной области, ни в расширении ИСО/МЭК 15504 с целью использования его в качестве стандарта по безопасности, согласно которому следует выполнять проверку соответствия. Его цель состоит в том, чтобы предоставить специалистам по оценке необходимые средства и информацию для измерения возможностей процессов, а также определить возможные действия по улучшению процесса, если программное обеспечение/система, находящееся/находящаяся в разработке, связана с безопасностью.

ISO/IEC/TS 15504-10 как отдельный документ может быть использован в сочетании с моделями оценки процесса (из ИСО/МЭК 15504-5 и/или ИСО/МЭК 15504-6) опытными специалистами по оценке с минимальной поддержкой экспертов по безопасности в проблемной области. Эта техническая спецификация была разработана независимо от любых конкретных стандартов по безопасности, которые определяют принципы, методы, технические средства для обеспечения безопасности и результаты работы. Тем не менее элементы соответствующих стандартов по безопасности могут быть использованы для расширения безопасности, а расширение безопасности направлено на возможность расширения для включения конкретных требований в стандарты по безопасности.

Влияние расширения безопасности на оценку процессов в ИСО/МЭК 15504-5 и ИСО/МЭК 15504-6 описывается в ISO/IEC/TS 15504. Для каждого процесса, приведенного в ИСО/МЭК 15504-5 и ИСО/МЭК 15504-6, есть указание на дополнительные проблемы, которые учитываются во время оценки. Проблемы представляются в виде указаний на конкретные отношения между процессами ИСО/МЭК 15504-5 и процессами ИСО/МЭК 15504-6 и ISO/IEC/TS 15504-10, а также путем выделения соответствующих аспектов, которые должны быть рассмотрены для улучшения полноты сбора данных на стадии оценки. Таким образом, эксперт по оценке может использовать ISO/IEC/TS 15504-10 для того, чтобы проверить, не были ли утеряны некоторые важные аспекты, связанные со средой разработки безопасности, во время оценки процессов, основанных на ИСО/МЭК 15504-5 или ИСО/МЭК 15504-6.

Библиография

[1] Summary Report from the Task Force on Patient Safety and Quality, ISO/TC 215 Health informatics, p.2010

[2] Kohn I.T., Corrigan J.M., Donaldson M.S. To Err is Human: Building a Safer Health System. USA Institute of Medicine, National Academy Press, 1999

[3] Personal communication. July 31 2013, Dr. Maureen Baker, CBE DM FRCGP, Clinical Director for Patient Safety, Clinical Safety Team, Health & Social Care Information Centre, HC3 England

[4] Magrabi F. et al. Using FDA reports to inform a classification for health information technology safety problems. J. Am. Med. Inform. Assoc. 2012, 19 pp. 45—53

[5] Bliznakov Z., Mitalas G., Pallikarakism N. Analysis and classification of medical device recalls in S.I. Kim and T.S. Suh, eds., World Congress of Medical Physics and Biomedical Engineering 2006 — IFMBE Proceedings Volume 14 (Springer, 2007), pp. 3782—3785

[6] Blobel B., Stassinopoulos G., Pharow P. Application of the component paradigm for analysisand design of advanced health system architectures. Int. J. Med. Inform. 2000, 60 (3) pp. 281—301

[7] Zhang J. et al. Using usability heuristics to evaluate patient safety of medical devices. J. Biomed. Inform. 2003, 36 (1-2) pp. 23—30

[8] Vicente K. The Human Factor: Revolutionizing the Way People Live with Technology. Routledge, New York, NY, 2004

[9] Staggers N. et al. Promoting usability in Health Organizations: Initial Steps and Progress Toward a Healthcare Usability Maturity Model, Chicago, IL, Healthcare Information Management Systems Society (HIMSS), 2011 [viewed 29 July 2013]. Available from: http://www.himss.org/files/HIMSSorg/content/files/HIMSS_Promoting_Usability_in_Health_Org.pdf

[10] Committee on Patient Safety and Health Information Technology. Health IT and Patient Safety: Building Safer Systems for Better Care. USA Institute of Medicine, National Academy Press, 2011

[11] ISB 0129 Clinical Risk Management — Its Application in the Manufacture of Health IT Systems, HC3 England Connecting for Health, 2013

[12] ISB 0160 Clinical Risk Management — Its Application in the Deployment and Use of Health IT Systems, HC3 England Connecting for Health, 2013

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, информационная безопасность, менеджмент безопасности, медицинское программное обеспечение, руководство по стандартам

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 17.01.2019. Подписано в печать 24.01.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 5,58 Уч.-изд. л. 5,05.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru