ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/ТО 27809— 2009

Информатизация здоровья

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПАЦИЕНТА ПРИ ИСПОЛЬЗОВАНИИ МЕДИЦИНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

(ISO/TR 27809:2007, IDT)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Росздрава» (ЦНИИОИЗ Росздрава) и Государственным научным учреждением «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики» на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 сентября 2009 г. № 405-ст

4 Настоящий стандарт идентичен международному документу ISO/TR 27809:2007 «Информатизация здоровья. Меры по обеспечению безопасности пациента при использовании медицинского программного обеспечения» (ISO/TR 27809:2007 «Health informatics — Measures for ensuring patient safety of 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 (www.gost.ru)

Содержание

Введение

Угроза безопасности пациента

В прошлом программное обеспечение, связанное со сферой здравоохранения, в основном исполняло относительно некритичные административные функции, где риск нанесения вреда пациенту, в отличие от нарушения функционирования организации, был низким. Клинические системы были, в общем, несложными, имели скорее административное, чем клиническое содержание и не имели развитых программных средств поддержки принятия решений. Даже системы поддержки клинических решений были относительно простыми, обладали понятной логикой и использовались как вспомогательные средства, а не как основной инструмент при принятии решений. В настоящее время это положение изменилось и будет постоянно изменяться и в будущем. Сущность происходящих изменений увеличивает потенциальные риски для пациентов.

В сфере медицинского программного обеспечения имели место неблагоприятные происшествия, например в сфере скрининга, вызова и повторного вызова врача пациентами сбои программного обеспечения приводили к тому, что врачи не выезжали к серьезно больным пациентам. Подобные случаи не только становились причиной страданий пациентов, но также могли привести к преждевременному летальному исходу. В результате подрывалось доверие населения к медицинскому обслуживанию.

Объем скрининга, проводимого в отношении заболеваний, существенно возрастает и в настоящее время охватывает большое число субъектов, что требует высокой степени доверия к программному обеспечению на административном и клиническом уровнях, чтобы зафиксировать отклонения от нормы и «вызвать» или «обработать» пациентов с повышенным риском. Такое программное обеспечение должно быть безопасным в отношении своей области применения.

Руководители и другие лица, ответственные за организации здравоохранения, должны понимать следующее:

- медицинское программное обеспечение потенциально может нанести вред пациентам;
- данная возможность возрастает по мере увеличения сложности внедряемого программного обеспечения;
- организации здравоохранения все больше зависят от медицинского программного обеспечения.

Из этого следует, что пока риски не будут идентифицированы и взяты под контроль, пациенты будут находиться под угрозой, а репутация организации здравоохранения будет страдать, что приведет к существенным финансовым и юридическим последствиям.

В мире существует повышенное внимание к большому числу клинических инцидентов, которые можно было предотвратить, но которые оказали неблагоприятное воздействие на пациентов, включая летальный исход и инвалидность. Это отмечено в разных источниках (см. [1], [2], [3], [4], [5] и [6]). К таким предотвратимым инцидентам относятся неточные или неверные диагнозы и другие решения. Влияющим фактором часто является отсутствие или неполнота информации, или просто незнание, например, о медицинских возможностях в трудных случаях или побочных реакциях на лекарственные препараты.

Все чаще утверждается, что информационные системы, реализующие поддержку принятия решений, протоколирование, электронные руководства и подсказки, могли бы существенно снизить подобные неблагоприятные воздействия. Даже если бы не было других причин (а они существуют), это приведет (и приводит) к возрастанию применения систем поддержки принятия решений и управления лечением, что, в свою очередь, неизбежно приведет к усложнению и совершенствованию таких систем. Также можно предположить, что под воздействием времени и судебно-медицинских факторов врачи будут все больше полагаться на такие системы, все меньше обращая внимание на их производительность. Действительно, поскольку подобные системы интегрируются в сферу медицинского обслуживания, любая неудача при применении стандартных средств поддержки может быть осуждена на юридических основаниях.

Расширенная поддержка принятия решений может ожидаться не только при лечении, но и в других областях, также значимых для безопасности пациентов, таких как принятие решения о направлении к специалистам, когда ошибка в выдаче «правильного» направления или в своевременной выдаче направления может иметь серьезные последствия.

Экономические факторы также способствуют увеличению числа систем поддержки принятия решений. Сфера группового и/или экономичного назначения лекарств является наиболее очевидной, но еще одной является экономия средств на количестве и стоимости клинических испытаний.

Системы, подобные системам для поддержки принятия решений, способны привести к снижению риска врачебных ошибок и улучшению врачебной практики. Например, большое число опубликованных сведений подтверждает снижение числа ошибок и негативных случаев, имевших место в результате применения электронных предписаний. Однако все подобные системы потенциально могут нанести вред. Причиной вреда, конечно, может стать непроверенное и/или непрофессиональное использование, хотя разработчики и поставщики могут снизить вероятность этого посредством, например, разработки инструкций по применению, средств обучения, компьютерных презентаций, руководств или предписаний. Причина нанесения вреда может быть связана и с проектированием системы, например:

- плохая доказательная база для проектирования;
- ошибки в логике проектирования, не позволяющие правильно представить цели проектирования;
- логические ошибки, не позволяющие представить правильные решения или доказательства на стадии проектирования;
- плохое или запутывающее представление информации или плохие средства поиска;
- проблемы с обновлениями, соответствующими современному уровню знаний.

Некоторые из недостатков таких систем проявляются не сразу и могут быть незаметны для пользователя.

Проблемы и недостатки медицинского программного обеспечения могут, конечно, оказывать и другие негативные воздействия помимо непосредственного причинения вреда пациентам. Например, они могут создавать административные неудобства или даже административный хаос в целом ряде случаев, включая финансовые потери. Вред, нанесенный пациенту, также может оказать опосредованное влияние на медицинскую организацию, например финансовые потери в результате судебного разбирательства. Хотя подобные негативные воздействия могут быть весьма существенными для медицинской организации, они не рассматриваются в настоящем стандарте, если только они не приводят к нанесению вреда пациенту. Например, сбой в центральной системе учета пациентов больницы, несомненно, создаст ряд административных неудобств, но данное негативное воздействие не относится к сфере применения настоящего стандарта, если только оно не может нанести вред пациенту (что в принципе возможно). Именно возможное нанесение вреда пациенту является предметом рассмотрения в настоящем стандарте.

Контроль рисков

Безопасность лекарств и медицинских приборов обеспечивается во многих странах за счет разнообразных юридических и административных мероприятий. Подобные мероприятия зачастую подкрепляются рядом стандартов, связанных с обеспечением безопасности, как национальных, так и международных, включая стандарты Международной организации по стандартизации (ИСО), Международного электротехнического комитета (МЭК) и Европейского комитета по стандартизации (CEN). Некоторое программное обеспечение, например необходимое для правильного применения или функционирования медицинского прибора, часто относится к области применения таких нормативных документов. Однако другие виды медицинского программного обеспечения автономного характера обычно не охватываются данными нормативными документами либо охватываются только в общем плане. Настоящий стандарт регламентирует программное обеспечение, применяемое в здравоохранении, за исключением того, которое регламентируется нормативными документами для медицинских приборов.

Необходимым условием для определения и внедрения соответствующих нормативных документов по проектированию и производству, чтобы минимизировать риски для пациентов от сбоев или неправильного функционирования программных продуктов, является точное понимание опасностей для пациентов, скрытых в программном продукте, в случае возникновения сбоя или непредусмотренного события и вероятности такого сбоя или непредусмотренного события, вызывающего нанесение вреда пациенту. Кроме того, при формировании задания для разработчиков и производителей медицинского программного обеспечения в части проектного и производственного контроля (и выработки соответствующих стандартов) необходимо отметить, что средства контроля для программных продуктов с низким уровнем риска будут отличаться от средств контроля для программных продуктов с высоким уровнем риска. Средства контроля должны соответствовать уровню риска, который программный продукт представляет для пациента. С этой целью многие стандарты, законодательные акты и спецификации, связанные с контролем рисков при проектировании и производстве, группируют программные продукты

в ограниченное число классов или типов в зависимости от степени риска, который они представляют. Средства контроля затем настраиваются для определенного класса или типа. Настоящий стандарт отражает данный принцип.

Существует широкий диапазон средств контроля, которые могут быть применены при проектировании, разработке, производстве, распространении, установке, модернизации и управлении версиями медицинского программного продукта. Настоящий стандарт начинается с рассмотрения того, как средства контроля применяются в медицинских приборах, и определяет практические решения по адаптации данных средств контроля для медицинских программных продуктов.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПАЦИЕНТА ПРИ ИСПОЛЬЗОВАНИИ МЕДИЦИНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Health informatics. Measures for ensuring the patient safety of health software

Дата введения — 2010—07—01

1 Область применения

Настоящий стандарт определяет контрольные мероприятия, необходимые для обеспечения безопасности пациента при использовании программного обеспечения в сфере здравоохранения.

Требования настоящего стандарта не распространяются на:

- программное обеспечение, необходимое для правильного применения медицинского прибора;
- программное обеспечение, являющееся дополнением к медицинскому прибору;
- программное обеспечение, являющееся само по себе медицинским прибором.

Целью настоящего стандарта является определение наиболее подходящих для использования или подлежащих разработке стандартов в том случае, если использование программных продуктов в сфере здравоохранения должно регулироваться или контролироваться каким-либо формальным, неформальным или произвольным образом в национальном, региональном или местном масштабе. Однако целью настоящего стандарта не является установление необходимости регулирования использования программных продуктов в сфере здравоохранения.

Требования настоящего стандарта распространяются на любые программные продукты для сферы здравоохранения независимо от того, присутствуют ли они на рынке и продаются на коммерческой основе или распространяются бесплатно. Настоящий стандарт адресован изготовителям программных продуктов для сферы здравоохранения.

Примечание — Область применения настоящего стандарта распространяется на программные продукты для сферы здравоохранения, которые фактически не охватываются нормативными документами, относящимися к медицинским приборам. В приложении А содержится детальное рассмотрение данного вопроса. В настоящем стандарте признается, что существуют программные продукты для сферы здравоохранения, которые регулируются нормативными документами по медицинским приборам в ряде стран и не регулируются в других странах. Кроме того, некоторые определения медицинских приборов могут охватывать и программные продукты для сферы здравоохранения, хотя в действительности это не так.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **вред** (harm): Смерть, физическая травма и/или повреждение здоровья или самочувствия пациента.

2.2 **опасность** (hazard): Потенциальный источник нанесения вреда [7].

2.3 **программный продукт для сферы здравоохранения** (health software product): Программный продукт, предназначенный для использования в сфере здравоохранения в целях охраны здоровья, за исключением программного обеспечения, которое:

- необходимо для правильного применения медицинского прибора;
- является дополнением к медицинскому прибору;
- само по себе является медицинским прибором.

Издание официальное

Примечание — В настоящем стандарте понятие «программное обеспечение» включает в себя встроенное программное обеспечение.

2.4 **изготовитель** (manufacturer): Физическое или юридическое лицо, отвечающее за разработку, изготовление, упаковку или маркировку программного продукта для сферы здравоохранения, компоновку системы или адаптацию программного продукта до того, как он будет представлен на рынке и/или введен в эксплуатацию, независимо от того, выполняются ли эти действия самим лицом или третьей стороной по его поручению.

2.5 **медицинский прибор** (medical device): Любой инструмент, аппарат, средство, оборудование, приспособление, имплантат, полученный в искусственных условиях реагент или калибратор, программное обеспечение, материал или иное подобное или родственное изделие, которое:

a) предназначено изготовителем для использования людьми автономно или совместно с другими приборами для одной или нескольких из следующих конкретных целей:

- диагностика, профилактика, мониторинг, лечение или облегчение заболевания;
- диагностика, мониторинг, лечение, облегчение или компенсация травмы;
- исследование, замена, модификация или поддержка анатомии или физиологического процесса;
- поддержание жизни;
- контроль оплодотворения;
- дезинфекция медицинских приборов;
- предоставление информации для медицинских или диагностических целей посредством лабораторного исследования образцов, полученных из человеческого тела;

b) не реализует своего главного предназначения в или на человеческом теле посредством фармакологических, иммунологических или метаболических средств, но которому подобные средства могут помочь реализовать его функцию.

Примечание — Данное определение взято из [8]. Однако в отношении сферы действия программного обеспечения в разных странах существуют некоторые различия в ее определении, которые приведены в приложении А.

2.6 **пациент** (patient): Любое лицо, к которому применяется программный продукт для сферы здравоохранения.

Примечание — В настоящем стандарте данный термин относится также к здоровым людям, когда это необходимо (например, здоровый человек обращается к базе знаний для получения информации, связанной со здоровьем).

2.7 **продукт** (product): Вся совокупность материалов и услуг, относящихся к программному обеспечению, предлагаемому пользователю, включая инструкции по применению и, в случае необходимости, обучение.

2.8 **риск** (risk): Комбинация вероятности нанесения вреда и серьезности этого вреда [7].

2.9 **безопасность** (safety): Независимость от недопустимого риска [7].

3 Круг рассматриваемых проблем

Если риск для пациентов со стороны программного обеспечения для сферы здравоохранения существует и может со временем возрастать (см. введение), то возникает вопрос о минимизации подобных рисков.

Контроль рисков может быть осуществлен разными способами и на разных уровнях. На местном уровне он может быть обеспечен посредством требований, установленных на момент покупки, например установленных в тендерной документации. На региональном и национальном уровнях контроль может осуществляться посредством сводов правил или официальных руководств. На национальном или межнациональном уровне, например в пределах Европейского союза (ЕС), контроль может реализовываться посредством законодательной структуры. Настоящий стандарт не определяет конкретных средств контроля, но устанавливает, что независимо от применяемых средств контроля требования должны основываться на нормативных документах. Именно такие документы и рассматриваются в настоящем стандарте.

Риски от медицинских приборов минимизируются во многих странах за счет законодательных мер, направленных на контроль в таких областях, как разработка, производство, распространение и другие этапы жизненного цикла прибора. Эти меры, а также стандарты или требования, на которых они

основаны, весьма схожи в разных странах (см. раздел 4) и имеют широкий охват, подробно документированы и общепризнаны. Программное обеспечение, необходимое для правильного использования медицинского прибора или являющееся дополнением к нему, обычно регулируется законодательными мерами, относящимися к данным медицинским приборам. В определенных обстоятельствах программное обеспечение само по себе может рассматриваться как медицинский прибор, хотя то, что может считаться медицинским прибором в одной стране, в другой стране может таковым не считаться. Риски от программного обеспечения, регулируемого нормативными документами для медицинских приборов, могут рассматриваться как уже проконтролированные и минимизированные, и потому они не относятся к области применения настоящего стандарта (см. раздел 1).

Однако в настоящее время существует множество разнообразного доступного и используемого программного обеспечения, которое не регулируется законодательными или нормативными документами для медицинских приборов. Примерами являются компьютерные системы врачей общей практики или терапевтов, системы электронного учета здоровья, системы учета пациентов, приложения, работающие со штрихкодами, например для идентификации пациентов или медицинской продукции, широкий спектр клинического программного обеспечения поддержки принятия решений, диспетчерские системы скорой помощи, программное обеспечение для отслеживания вызовов и повторных вызовов. Все это программное обеспечение определено в настоящем стандарте как программные продукты для сферы здравоохранения. Именно «продукты», подобные перечисленным выше, относятся к области применения настоящего стандарта. Однако поскольку в мире существуют разнообразные определения медицинских приборов и их практической реализации, возможно, что какие-либо из приведенных примеров могут регулироваться в некоторых странах нормами для медицинских приборов (см. раздел 1).

Поскольку программное обеспечение контролируется законодательными актами и соответствующими требованиями или стандартами для медицинских приборов, уместно рассмотреть возможность и/или необходимость применения тех же механизмов и требований контроля к программному обеспечению, которое не контролируется данным образом. В частности, это относится к большому числу программного обеспечения, относящегося к пограничной области между программными продуктами и медицинскими приборами (см. раздел 5). Нет смысла иметь медицинское программное обеспечение, контролируемое разными способами, если существует возможность его гармонизации. В настоящем стандарте рассматривается данная возможность.

Средства контроля, задействованные в контексте медицинских приборов, определяются главным образом потенциальным риском, который прибор представляет для пациента, или клиническим опытом, накопленным при использовании данного изделия. В соответствии с этим приборы классифицируются, а средства контроля выбираются в зависимости от класса, к которому отнесен данный прибор. Очевидно, что применение одних и тех же средств контроля с одинаковой строгостью ко всем приборам было бы нелогичным, поскольку некоторые приборы могут представлять небольшой риск или вообще никакого риска для пациента, тогда как другие приборы могут представлять серьезный риск, включая летальный исход.

Если применить такой же подход к программным продуктам для сферы здравоохранения, то надо классифицировать их в зависимости от степени риска, который они представляют для пациента. В разделе 6 определено, как лучше всего классифицировать программные продукты для сферы здравоохранения, включая рассмотрение процедур классификации медицинских приборов для оценки их пригодности.

Существуют разнообразные средства контроля, применяемые к медицинским приборам в соответствии с их классом, такие как разнообразные требования к регистрации, системы качества, контроль проектирования и управление рисками. В разделе 7 все они рассмотрены в контексте программного обеспечения для сферы здравоохранения, а также определено, какие стандарты могли бы поддержать их применение для медицинского программного обеспечения.

Следует отметить, что будет существовать постоянная потребность разработки стандартов применительно к конкретным рискам (см. раздел 8).

4 Общая информация о средствах контроля медицинских приборов

Программное обеспечение, необходимое для правильного применения медицинского прибора либо являющееся дополнением к нему, в ряде стран регулируется средствами контроля медицинских приборов. Несомненно, в определенных обстоятельствах в ряде стран программное обеспечение само по себе может рассматриваться как медицинский прибор. Хотя такое программное обеспечение не от-

носится к области применения настоящего стандарта, полезно проанализировать сущность средств контроля медицинских приборов в разных странах, уделяя особое внимание программному обеспечению. Данный анализ позволит понять, могут ли средства контроля, применяемые в основном к медицинским приборам, а к программному обеспечению только в частности, быть применены и к программному обеспечению, не регулируемому данными средствами контроля медицинских приборов, то есть к программным продуктам для сферы здравоохранения.

В приложении А рассмотрена ситуация в ЕС, Австралии, Канаде, США и в Рабочей группе по глобальной гармонизации (далее — GHTF). В данном приложении показано, что ЕС, Австралия, Канада и GHTF в значительной степени приняли одинаковые законодательный подход и средства контроля в отношении медицинских приборов. Практически то же произошло и в США. Несмотря на то что программное обеспечение на практике регулируется аналогичным образом, существуют и различия. Таким образом, программное обеспечение, являющееся необходимым для правильного использования медицинского прибора, охватывается средствами контроля во всех этих странах, но регулирование другого программного обеспечения, относящегося к сфере здравоохранения, различно. Например, в США существует руководство по программному обеспечению, «содержащемуся» в медицинском приборе, включая покупное программное обеспечение, используемое в медицинских приборах, потому существует очень мало другой регламентирующей документации, относящейся к программному обеспечению.

Однако какими бы ни были тонкости формулировок, совершенно ясно, что значительная часть программного обеспечения, относящегося к программным продуктам для сферы здравоохранения, практически не регулируется средствами контроля медицинских приборов, хотя обсуждения по изменению данной ситуации уже ведутся. Тем не менее существуют проблемы на границе между медицинскими приборами и программными продуктами для сферы здравоохранения.

5 Граница между программными продуктами для сферы здравоохранения и медицинскими приборами

Программное обеспечение, необходимое для правильного применения медицинского прибора либо являющееся дополнением к нему, рассматривается как регулируемое средствами контроля медицинских приборов в ЕС, Австралии, Канаде, США и GHTF. Некоторое программное обеспечение само по себе рассматривается как медицинский прибор.

Программное обеспечение может быть существенной частью медицинского прибора (например, частью анализатора патологической анатомии, автоматизирующей аналитический процесс) либо его дополнением, реализующим дополнительные функции (например, дополнительный программный модуль, поставляемый отдельно и повышающий возможности или диапазон исследования), либо оно может обрабатывать данные независимо от медицинского прибора.

Программное обеспечение в лабораторной информационной системе может допускать хранение и передачу данных от анализатора на другие удаленные рабочие станции. Если оно обрабатывает данные с целью извлечения информации, которая иначе останется недоступной, и тем самым предоставляет средства или способствует осуществлению диагностики, мониторинга, профилактики или лечения болезненного состояния, то оно, скорее всего, будет рассматриваться как дополнение к медицинскому прибору. Если оно не требуется для нормального функционирования анализатора, а только сохраняет или передает данные, поступающие непосредственно от анализатора, без использования программного обеспечения, то оно, вероятно, не будет отнесено к программному обеспечению, регулируемому средствами контроля медицинских приборов. Однако в каждом случае регулятивный статус программного обеспечения может отличаться в разных странах или может изменяться с течением времени, по мере введения новых или пересмотренных нормативных правил.

Из определений медицинских приборов, принятых в разных странах, не следует четкого понимания того, какое программное обеспечение само по себе относится к медицинским приборам. Даже в случае, как в GHTF, когда определение медицинского прибора явно включает в себя программное обеспечение, его область применения ограничена определенными функциями (см. А.3 приложения А).

Таким образом, существует программное обеспечение, которое может охватываться или не охватываться правилами, установленными для медицинских приборов, в зависимости от специфики определений, принятых в разных странах. Граница будет меняться с течением времени.

Не вызывает сомнений то, что значительный объем программного обеспечения, относящегося к программным продуктам для сферы здравоохранения (в контексте настоящего стандарта), не будет охвачен нормативными правилами для медицинских приборов намеренно или практически.

Тем не менее поскольку часть программного обеспечения регулируется нормативными правилами для медицинских приборов, имеет смысл исследовать, как такое программное обеспечение классифицируется и контролируется, чтобы определить, могут ли те же или подобные нормативные правила быть применены к нерегулируемому программному обеспечению.

6 Классификация программных продуктов для здравоохранения

6.1 Возможные варианты

Средства контроля, применяемые к медицинским приборам, зависят от степени риска, который они могут представлять для безопасности пациента. Подход, применяемый к медицинским приборам, заключается в отнесении каждого прибора к одному из нескольких классов. Чем выше риск, представляемый определенным классом, тем более полными и строгими должны быть средства контроля для данного класса.

Если мероприятия, обеспечивающие безопасность пациента при применении программных продуктов для сферы здравоохранения, также должны быть пропорциональны риску, который они могут представлять для пациента, то программные продукты для сферы здравоохранения также следует классифицировать в зависимости от степени риска.

Первым очевидным вопросом является, можно ли классифицировать программные продукты для сферы здравоохранения в соответствии с правилами классификации медицинских приборов. В приложении В приведена классификация медицинских приборов в разных странах и сделаны соответствующие выводы.

Системы классификации медицинских приборов в ЕС, Австралии, Канаде, США и GHTF не подходят для программных продуктов для сферы здравоохранения.

Классификация «программного обеспечения в медицинских приборах» [9] и «имеющегося на рынке» программного обеспечения [10] Центра по приборам и радиологической безопасности Администрации по контролю за продуктами питания и лекарствами Министерства здравоохранения и социальных служб США может быть применена к программным продуктам для сферы здравоохранения.

Однако в [11] представлена наиболее подходящая система классификации на основе оценки установленных классов риска, представленных в таблице 4 указанного документа. Данная классификация не противоречит подходу Центра по приборам и радиологической безопасности Управления по контролю за продуктами питания и лекарствами Министерства здравоохранения и социальных служб США к «программному обеспечению для медицинских приборов» и «имеющемуся на рынке» программному обеспечению.

6.2 Выводы

Если средства контроля должны быть пропорциональны риску, который продукт может представлять для пациента, то программные продукты для сферы здравоохранения следует классифицировать в соответствии с данными рисками. Системы классификации медицинских приборов не подходят для программных продуктов для сферы здравоохранения. Наиболее подходящим представляется подход ИСО, основанный на оценке установленных классов риска и изложенный в [11].

7 Возможные мероприятия по контролю за программными продуктами для сферы здравоохранения

7.1 Обзор

7.1.1 Общие сведения

После того как программные продукты для сферы здравоохранения распределены по классам в соответствии с риском, который они могут представлять для пациента, следует рассмотреть вопрос о том, какие средства контроля, если таковые требуются, должны быть использованы для данных классов/рисков.

Контролирующие мероприятия, применяемые для медицинских приборов, в основном схожи в разных странах, а различаются только по наименованиям и деталям. Представленный ниже перечень

составлен на основании контролирующих мероприятий, принятых для медицинских приборов в ЕС, Австралии, Канаде, GHTF и США, и обобщает полезные варианты, которые также могут быть применены к программным продуктам для сферы здравоохранения:

- предпродажное извещение с или без предпродажной аттестации;
- регистрация предприятия;
- номенклатура изделий;
- требования к клиническим данным;
- требования к маркировке;
- сведения об инцидентах, которые могли привести или были причиной летального исхода или серьезной травмы;
- требования к системе качества или производственным нормам с или без проверки;
- контроль проектирования;
- управление рисками.

Однако целью настоящего стандарта не является подробное рассмотрение нормативных документов и контролирующих мероприятий, а также выработка рекомендаций по необходимости регулирования программных продуктов для сферы здравоохранения. Настоящий стандарт направлен на определение стандартов, которые наиболее подходят для использования или должны быть созданы, и их положений для того случая, если программные продукты для сферы здравоохранения должны контролироваться или регулироваться каким-либо формальным, неформальным или произвольным способом. Поэтому контролирующие мероприятия приведены только для обеспечения возможности рассмотрения тех стандартов, которые могут подкрепить их, если данные средства контроля будут внедрены.

Таким образом, принятие решения о необходимости контроля безопасности программных продуктов для сферы здравоохранения посредством предпродажного извещения, регистрации предприятия или номенклатуры изделий будет лежать на лицах, ответственных за средства контроля. Если данные лица примут решение о необходимости контроля безопасности, то содержимое нормативной документации или стандартов будет сразу же понятно и разработка стандартов не потребуется.

7.1.2 Выводы

Если потребуются предпродажное извещение, регистрация предприятия и изделия, то это не повлечет за собой необходимость разработки стандартов.

7.2 Маркировка и документация

7.2.1 Общие сведения

К маркировке может относиться не только тара для изделия, но также плакаты, этикетки, проспекты, рекламные листки, буклеты, технические руководства, инструкции и т. п., а также различная реклама.

Требования к маркировке программных продуктов для сферы здравоохранения будут иметь много общего с маркировкой медицинских приборов. Необходимо определить, может ли Европейский норматив, относящийся к медицинским приборам [13], быть полностью применен и к программным продуктам. Однако могут существовать требования, специфичные для программных продуктов для сферы здравоохранения, например требования к аппаратному обеспечению и интерфейсам. В условиях, когда функциональная совместимость и взаимодействие программных продуктов для сферы здравоохранения приобретают все большее значение и когда проблемы с функциональной совместимостью могут иметь серьезные последствия, полная и точная формулировка характеристик программных продуктов для сферы здравоохранения будет иметь большое значение. Такая формулировка должна соответствовать широкому определению маркировки. Следует понимать, что системные характеристики, документация на изделие и инструкции по использованию могут быть предоставлены через Интернет, а не поставляться пользователю в печатном виде.

7.2.2 Выводы

Стандарт на минимум информации, необходимой для представления характеристик программных продуктов для сферы здравоохранения, может быть полезен, в частности, для характеристик, которые важны для взаимодействия и функциональной совместимости. Стандарт на медицинские приборы [13] необходимо проанализировать, чтобы оценить необходимость разработки отдельного стандарта по общей маркировке программных продуктов для сферы здравоохранения.

7.3 Клинические данные

7.3.1 Общие сведения

Предпродажная аттестация преимущественно направлена на медицинские приборы с высокой степенью риска и может включать представление клинических данных для обоснования претензий к прибору. В Австралии нормативные правила требуют наличия для каждого медицинского прибора, отнесенного к любому классу, клинических данных, соответствующих его использованию и классификации.

Предметом обсуждения может быть вопрос о том, должны ли средства контроля, относящиеся к классам программных продуктов для сферы здравоохранения с наивысшими рисками, включать представление клинических данных. При рассмотрении этого вопроса следует учитывать, что безопасность программных продуктов поддержки принятия клинических решений (некоторые из которых могут быть отнесены к классам самого высокого риска) будет зависеть от правильности и распространенности клинических данных, положенных в основу алгоритмов принятия решений. При этом клинические данные могут рассматриваться в двух контекстах:

- сведения о достоверности клинических данных, лежащих в основе поддержки принятия решений, и способ, каким программное обеспечение использует эти сведения;
- клинические данные, полученные в результате практического использования изделия, например в ограниченно контролируемых приложениях.

Здесь возможно применение стандарта ИСО по клиническим исследованиям медицинских приборов на людях [14].

7.3.2 Выводы

Если предоставление клинических данных является частью средств контроля над безопасностью программных продуктов для сферы здравоохранения, то должен быть принят содержащий руководящие указания стандарт, являющийся основой и соответствующий характеристикам программных продуктов для сферы здравоохранения, таких как поддержка принятия решений. Такой стандарт должен охватывать как клинические данные, относящиеся к достоверности данных, положенных в основу принятия решений, так и их использование программным обеспечением, а также клинические данные, полученные в результате использования программного продукта. В данном контексте должна быть рассмотрена возможность применения ИСО 14155 [14].

7.4 Регистрация инцидентов

7.4.1 Общие сведения

К медицинским приборам предъявляется требование регистрировать инциденты, которые могли привести или были причиной летального исхода или серьезной травмы пациента.

Если такое контролирующее мероприятие было предусмотрено для программных продуктов для сферы здравоохранения, то могла бы быть предусмотрена электронная регистрация. Поэтому должен быть рассмотрен вопрос о стандарте по регистрации инцидентов для программных продуктов для сферы здравоохранения. Существуют документированные примеры, которыми можно воспользоваться, например:

- ISO/TS 19218:2005 [15];
- GHTF для медицинских приборов [16];
- MedWatch Управления по контролю за продуктами питания и лекарствами;
- общие требования к регистрации Национального агентства по безопасности пациентов Великобритании [17];
- работа, проводимая в Рабочей группе по вопросам фармацевтики и применения лекарств (РГ 6) ТК 215 ИСО, подготовившей проект стандарта по электронной регистрации неблагоприятных реакций на лекарства [18] на основе национальных и международных документов.

7.4.2 Выводы

Должен быть рассмотрен вопрос о стандарте по электронной регистрации неблагоприятных инцидентов, произошедших при применении программных продуктов для сферы здравоохранения.

7.5 Системы качества

7.5.1 Общие сведения

Любые средства контроля программных продуктов для сферы здравоохранения, особенно для продуктов с высокой степенью риска, будут предъявлять требования к системе качества. Поскольку стандарты по системам качества (например, группа стандартов ИСО 9000) могут регулировать контроль проектирования и управление рисками, то маловероятно, что в них достаточно детально будут

рассмотрены вопросы контроля программных продуктов для сферы здравоохранения. Таким образом, в сфере медицинских приборов существуют отдельные стандарты по системам качества, контролю проектирования и управлению рисками. То же самое будет относиться и к программным продуктам для сферы здравоохранения.

Системы качества могут быть очень эффективными в обеспечении соответствия конечного изделия требуемому качеству, но если исходный проект был плохим, то существует опасность, что все конечные изделия, выполненные по данному проекту, также будут плохими. Таким образом, необходимыми свойствами хороших систем качества являются контроль проектирования, рассмотренный в 7.6, и требование к анализу рисков и управлению рисками или их снижению, рассмотренное в 7.7.

Поскольку системы качества для программных продуктов для сферы здравоохранения во многом схожи по характеристикам с системами качества для медицинских приборов (и изделий в целом), то существующие стандарты, применимые к программному обеспечению, могут быть использованы в качестве отправной точки. Ниже рассмотрены наиболее значимые из них. В общем данные стандарты охватывают следующие аспекты:

- планирование реализации программного продукта, включая жизненный цикл, планирование качества, процессы, связанные с потребителем, контроль проектирования и управление рисками;
- документацию, например руководство по качеству и контроль документов и записей;
- ответственность за управление, включая обязательства по управлению, сфокусированность на потребителя, планирование систем политики в области качества и управления качеством;
- распределение ответственностей и полномочий;
- связь;
- управление ресурсами, включая компетенцию, понимание, обучение и рабочую среду;
- обзоры по управлению.

7.5.2 Стандарты по системам качества, относящиеся к медицинским приборам

Многие изготовители медицинских приборов внедрили систему качества, чтобы соответствовать законодательным нормам.

В большинстве Европейских стран изготовители медицинских приборов внедрили систему качества, чтобы соответствовать директиве ЕС по медицинским приборам [19]. Однако в соответствии с установкой ЕС по директивам нового подхода [20], если система качества изготовителя соответствует «гармонизированным стандартам», но не называет их, то она может ссылаться на допущение соответствия. Однако в листинге руководства по директивам для медицинских приборов [21] строка, относящаяся к системам качества, ссылается на документы от GHTF.

Руководство GHTF до июня 2005 г. было включено в документ «Руководство по системам качества для проектирования и производства медицинских приборов» [22], который, в свою очередь, был создан на основе ИСО 9001 (версия 1994 г.) [23]. В 2005 г. данное руководство было изъято из обращения и заменено на ISO/TR 14969:2004 [24], в разработке проекта которого участвовала GHTF. Настоящий стандарт также основан на ИСО 9001.

В США требования «Успешной производственной практики» представлены в «Положении по системам качества» [25]. В предисловии данного документа представлены полученные общественные комментарии и ответы Управления по контролю за продуктами питания и лекарствами. Из приведенных ответов становится ясно, что требования в основном основаны на ИСО 9001:1994 [23] и разработаны в тесном сотрудничестве с GHTF. В главе 2 «Системы качества» Руководства по системам качества для медицинских приборов для малых предприятий [26] также отмечено, что требования «Успешной производственной практики» «гармонизированы с ИСО 9001:1994 и ИСО 13485 [27]» (который сам основан на ИСО 9001).

Ситуация в Австралии и Канаде сложилась похожим образом. Их требования к системе качества для медицинских приборов также основаны на серии стандартов ИСО 9000.

Ясно, что если программные продукты для сферы здравоохранения были бы предметом контроля со стороны системы управления качеством, то любой стандарт должен быть основан на ИСО 9001:2000 [28]. Встает вопрос, существует ли уже такой стандарт, который мог бы быть применен непосредственно.

Стандарты, применяемые в отношении медицинских приборов, являются очевидными кандидатами на рассмотрение. Как уже отмечалось, стандартом, который упоминался в контексте «Директивы по медицинским приборам» ЕС, является «Руководство по системам качества» GHTF [22], которое было отозвано и заменено на ISO/TR 14969:2004 «Руководство по применению ИСО 13485:2003» [24]. ИСО 13485:2003 «Системы управления качеством. Требования к целям регулирования» [27] является, как видно из наименования, специально разработанным документом для «целей регулирования» и по-

священ медицинским приборам. Он не может подходить для программных продуктов для сферы здравоохранения по двум причинам:

- хотя его определение «медицинского прибора» соответствует GHTF и тем самым включает «программное обеспечение» (см. А.3), совершенно очевидно, что данный стандарт разрабатывался без учета программных продуктов для сферы здравоохранения;
- данный стандарт разработан для целей регулирования, тогда как настоящий стандарт не основан на предположении, что средства контроля не обязательно будут средствами регулирования; ряд дополнений и поправок к ИСО 9001 в ISO/TR 14969:2004 [24] и ИСО 13485:2003 [27] может не поддерживаться в нерегулируемой среде.

Тем не менее основное содержание и требования могут быть применены к программным продуктам для сферы здравоохранения так же, как они применяются к медицинским приборам.

7.5.3 Стандарты по системам качества, относящиеся к программному обеспечению

Другим возможным подходом к стандарту по программным продуктам для сферы здравоохранения на основе ИСО 9001 является рассмотрение существующих стандартов, основанных на ИСО 9001, которые в общем случае применимы к программному обеспечению. Очевидным претендентом на применение является ИСО/МЭК 90003:2004 «Руководства по применению ИСО 9001:2000 к программному обеспечению компьютеров» [29].

Данный стандарт, в свою очередь, ссылается на ряд стандартов ИСО/МЭК, в частности на ИСО/МЭК 12207:1995 «Процессы жизненного цикла программного обеспечения» [30], поправку к нему 2002 г. [31] и руководство по его применению ISO/IEC TR 15271 [32].

Стандарт ИСО/МЭК 9003:2004 мог бы непосредственно быть применен к программным продуктам для сферы здравоохранения и, таким образом, мог бы стать выбранным из существующих стандартов. Его возможным недостатком является отсутствие ссылок на стандарты для медицинских приборов, основанные на ИСО 9001.

7.5.4 Выводы

Если одним из средств контроля для обеспечения безопасности программных продуктов для сферы здравоохранения является требование к системе управления качеством, то все необходимые стандарты должны быть основаны на ИСО 9001:2000 [28].

Если устанавливается, что требуется новый стандарт, регулирующий программные продукты для сферы здравоохранения, то он должен быть создан на основе рассмотрения ИСО/МЭК 90003:2004 [29]:

- в качестве возможного претендента без каких-либо поправок;
- в качестве исходного материала с возможными поправками, отражающими специфику программных продуктов для сферы здравоохранения (с учетом требований к медицинским приборам, установленным в ИСО 13485:2003 [27] и связанном с ним руководстве ISO/TR 14969:2004 [24]).

7.6 Контроль проектирования

7.6.1 Общие сведения

Контроль проектирования включен в большинство законодательных подходов.

В ЕС имеются рекомендации по контролю проектирования, основанные на документах GHTF. Руководство GHTF до июня 2005 г. содержалось в документе «Руководство по контролю проектирования для изготовителей медицинских приборов» [33]. В 2005 г. это руководство было изъято из обращения и заменено на ISO/TR 14969:2004 «Системы управления системами качества. Руководство по применению ИСО 13485:2003» [24]. Оно, по сути, заменило 44 страницы руководства на восемь страниц ISO/TR 14969:2004, раздел 7. Это привело к потере некоторых деталей.

Австралия и Канада применяют подход, аналогичный подходу GHTF.

В США Администрация по контролю за продуктами питания и лекарствами выпустила «Руководство по контролю проектирования для производителей медицинских приборов» [34]. Оно имеет отношение к Правилам 820.30 по «Контролю проектирования» и разделу 4.4 ИСО 9001:1994. Данное руководство охватывает те же аспекты, что и руководство GHTF, а именно:

- планирование проектирования и разработки;
- исходные данные для проектирования;
- экспертизу проекта;
- верификацию проекта;
- аттестацию проекта;
- передачу проекта;
- изменения проекта;
- документирование истории проекта.

Несмотря на то что требования, изложенные в данном руководстве, были разработаны для регулируемой среды (которая не относится к области применения настоящего стандарта), по существу, они могли бы быть применены и к программным продуктам для сферы здравоохранения, как и к медицинским приборам. Тем не менее их нельзя применить полностью, поскольку:

- примеры и текст руководства ориентированы на медицинские приборы и потому не применимы к программным продуктам для сферы здравоохранения;
- некоторые требования могут быть применены к программному обеспечению с изменениями;
- необходимо предоставить более подробную информацию, относящуюся именно к программным продуктам для сферы здравоохранения, например к системам поддержки принятия решений (см. ниже).

Проектирование систем поддержки принятия решений и последующие изменения в проекте основываются на исходных алгоритмах поддержки принятия решений и клинических данных. Так, электронная система назначений лекарств сможет, например, выдавать предупреждения о противопоказаниях применения лекарств малолетними детьми или беременными женщинами, а также предупреждать о взаимных влияниях при применении нескольких лекарств. Такие функции будут сильно зависеть от клинических данных, которые будут меняться с течением времени. Недостаточность данных и невозможность отслеживать их своевременно могут иметь серьезные и даже фатальные последствия. Поэтому усиленный контроль исходного проекта и изменений в проекте, например его обновлений, имеет первостепенное значение для безопасности. Любой стандарт по контролю проектирования программных продуктов для сферы здравоохранения должен учитывать данные особенности, например возможные требования к экспертной оценке клинических данных. Существующие стандарты в этом отношении не являются адекватными.

7.6.2 Выводы

Если контроль проектирования должен быть частью требований для обеспечения безопасности программных продуктов для сферы здравоохранения, то должна быть рассмотрена необходимость разработки стандарта непосредственно для программных продуктов для сферы здравоохранения. Поскольку подобный стандарт должен базироваться на основных требованиях, содержащихся в стандартах по контролю проектирования медицинских приборов [24], [33], [34], то эти требования должны быть адаптированы к программным продуктам для сферы здравоохранения и учитывать специфичные потребности, такие как контроль алгоритмов и использование клинических данных в программных продуктах, например в системах поддержки принятия решений.

7.7 Управление рисками

7.7.1 Общие сведения

Существуют много стандартов, связанных с управлением рисками, которые могли бы претендовать на применение к программным продуктам для сферы здравоохранения. В приложении С приведен обзор ряда наиболее значимых в данном контексте документов, имеющих отношение к следующим областям:

- процессы «управление рисками на предприятиях»;
- продукты для сферы здравоохранения, в частности медицинские приборы;
- другие области, например управление информационной безопасностью.

7.7.2 Выводы

Если управление рисками должно быть частью требований для обеспечения безопасности программных продуктов для сферы здравоохранения, то:

- специально для программных продуктов для сферы здравоохранения необходим новый стандарт, согласованный на высшем уровне с ИСО 31000 [35], ИСО 14971 [36], МЭК 61508-3 [37] и МЭК 61508-5 [38]. Данный стандарт должен реализовывать положения, изложенные в GHTF/SG3/N15R8 [39], и быть основан на опыте использования CRAMM [40] совместно с ИСО/МЭК 17799 [65];
- новый стандарт должен быть подкреплен руководством по реализации, конкретизированным под программные продукты для сферы здравоохранения.

8 Стандарты, относящиеся к рискам определенного характера

8.1 Общие сведения

Конкретный программный продукт для сферы здравоохранения или программные продукты для сферы здравоохранения вообще могут быть объектами рисков определенного характера. Примерами, применимыми к большинству программных продуктов для сферы здравоохранения, и для которых су-

ществуют стандарты ИСО и/или CEN, относящиеся к программным продуктам для сферы здравоохранения, являются следующие:

- безопасность в контексте защиты личной информации;
- аутентификация медицинских работников;
- правильная однозначная идентификация пациентов.

8.2 Выводы

Если для рисков определенного характера существуют стандарты, то программные продукты должны проектироваться в соответствии с этими стандартами.

9 Надзор за безопасностью и рисками в сфере деятельности пользователя

9.1 Общие сведения

Настоящий стандарт ограничен обеспечением безопасности программных продуктов для сферы здравоохранения в производственной сфере (включающей проектирование и разработку). Однако даже если безопасность была обеспечена на производстве, признается, что при внедрении и использовании программных продуктов в сфере деятельности пользователя, например в больнице или врачом общей практики, могут возникать новые риски. Это особенно вероятно в случае, когда предполагаются взаимодействие и взаимосвязь программных продуктов, полученных от разных поставщиков, независимо от того, связаны ли они напрямую или через сеть. То же самое относится и к интерфейсам медицинских приборов, имеющих встроенное программное обеспечение. Данный аспект безопасности должен быть учтен.

9.2 Выводы

Необходимо обратить внимание на стандарты по обеспечению безопасности программных продуктов для сферы здравоохранения в сфере деятельности пользователя.

10 Систематизация

10.1 Общие сведения

Как правило, нет ясности, что заключает в себе программный продукт для сферы здравоохранения. Чтобы преодолеть это, необходимо принять меры посредством систематизации (структурированного списка) медицинского программного обеспечения. Аналогично поддерживающая систематизация была бы полезна при регистрации неблагоприятных событий, например:

- программный продукт для сферы здравоохранения (например, для поддержки принятия решения о назначении лекарств);
- процессы (дозирование лекарств);
- последствия (аллергическая реакция или серьезный вред).

10.2 Выводы

Должна быть проведена систематизация программных продуктов для сферы здравоохранения, а также систематизация для поддержки регистрации неблагоприятных событий.

11 Общие выводы

Если программные продукты для сферы здравоохранения подлежат регулированию или контролю формальными или неформальными методами на национальном, региональном или местном уровне, то средства контроля должны быть основаны на стандартах. Настоящий стандарт определяет необходимые стандарты и их сущность. Ниже приведены общие выводы.

11.1 Если средства контроля должны быть адекватны риску, который программный продукт может представлять для пациента, то программные продукты для сферы здравоохранения классифицируют в соответствии с данными рисками. Системы классификации медицинских приборов не подходят для программных продуктов для сферы здравоохранения. ISO/TS 25238 «Классификация угроз безопасно-

сти от медицинского программного обеспечения» [11] наиболее подходит для принятия определенных в нем классов рисков (см. [11], таблица 4).

11.2 Если требуются предпродажное извещение, регистрация предприятия или продукта, то, по-видимому, они не потребуют разработки стандартов (см. 7.1).

11.3 Стандарт на минимум информации, необходимой для представления характеристик программных продуктов для сферы здравоохранения, может быть полезен, в частности, для характеристик, которые важны для взаимодействия и функциональной совместимости. Стандарт на медицинские приборы [13] необходимо проанализировать, чтобы оценить необходимость разработки отдельного стандарта по общей маркировке программных продуктов для сферы здравоохранения (см. 7.2).

11.4 Предоставление клинических данных может потребоваться некоторым программным продуктам для сферы здравоохранения, например для поддержки принятия решений с наивысшим риском. Если это так, то желательно иметь стандарт в форме руководства, конкретизированного под программные продукты для сферы здравоохранения. Такой стандарт должен охватывать как клинические данные, относящиеся к достоверности данных, положенных в основу принятия решений, так и их использование программным обеспечением, а также клинические данные, полученные в результате использования программного продукта. В данном контексте должна быть рассмотрена возможность применения ИСО 14155 [14] (см. 7.3).

11.5 Регистрация инцидентов может считаться необходимой. В этом случае должен быть рассмотрен вопрос о стандарте по электронной регистрации неблагоприятных инцидентов, произошедших при применении программных продуктов для сферы здравоохранения (см. 7.4).

11.6 Если одним из средств контроля для обеспечения безопасности программных продуктов для сферы здравоохранения является требование к системе управления качеством (см. 7.5), то все необходимые стандарты должны быть основаны на ИСО 9001:2000 [28]. Если устанавливается, что требуется новый стандарт, регулирующий программные продукты для сферы здравоохранения, то он должен быть создан на основе рассмотрения ИСО/МЭК 90003:2004 [29]:

- в качестве возможного претендента без каких-либо поправок;
- в качестве исходного материала с возможными поправками, отражающими специфику программных продуктов для сферы здравоохранения (с учетом требований к медицинским приборам, установленным в ИСО 13485:2003 [27] и связанным с ним руководством ISO/TR 14969:2004 [24]).

11.7 Если контроль проектирования должен быть частью требований для обеспечения безопасности программных продуктов для сферы здравоохранения, то должна быть рассмотрена необходимость разработки стандарта непосредственно для программных продуктов для сферы здравоохранения (см. 7.6). Поскольку подобный стандарт должен базироваться на основных требованиях, содержащихся в стандартах по контролю проектирования медицинских приборов [24], [33], [34], то эти требования должны быть адаптированы к программным продуктам для сферы здравоохранения и учитывать специфичные потребности, такие как контроль алгоритмов и использование клинических данных в программных продуктах, например в системах поддержки принятия решений.

11.8 Если управление рисками должно быть частью требований для обеспечения безопасности программных продуктов для сферы здравоохранения, то:

- специально для программных продуктов для сферы здравоохранения необходим новый стандарт, согласованный на высшем уровне с ИСО 31000 [35], ИСО 14971 [36], МЭК 61508-3 [37] и МЭК 61508-5 [38]. Данный стандарт должен реализовывать положения, изложенные в GHTF/SG3/N15R8 [39], и быть основан на опыте использования CRAMM [40] совместно с ИСО/МЭК 17799 [65];
- новый стандарт должен быть подкреплен руководством по реализации, конкретизированным под программные продукты для сферы здравоохранения.

11.9 Если для рисков определенного характера существуют стандарты, то программные продукты должны проектироваться в соответствии с данными стандартами.

11.10 Необходимо обратить внимание на стандарты по обеспечению безопасности программных продуктов для сферы здравоохранения в среде пользователя.

11.11 Должна быть проведена систематизация программных продуктов для сферы здравоохранения, а также систематизация для поддержки регистрации неблагоприятных событий.

Данные выводы относятся к комплексу стандартов, необходимых для обеспечения безопасности программных продуктов для сферы здравоохранения. Однако не обязательно должен быть разработан один стандарт по каждому выводу. Так, требования к контролю проектирования и управлению рисками могут входить в стандарт по системам качества. Необходим стратегический подход в целом.

Приложение А
(справочное)

Положение с медицинскими приборами в разных странах

Примечание — Настоящий обзор предназначен только для целей настоящего стандарта, затрагивая и резюмируя только вопросы, имеющие к нему отношение. Он не должен использоваться в качестве полного руководства в каком-либо отношении и для какой-либо цели (в случае необходимости следует обратиться к исходным документам и компетентным национальным органам).

А.1 ЕС, Австралия и Канада

А.1.1 Общие сведения

ЕС, Австралия и Канада в значительной степени используют одинаковые законодательные подходы к медицинским приборам и средства их контроля. Поэтому они рассматриваются в одном разделе.

А.1.2 ЕС

В ЕС медицинские приборы контролируются на основании трех директив:

- 90/385/EEC от 20 июня 1990 г. [41] по активным имплантируемым медицинским приборам;
- 93/42/EEC от 14 июня 1993 г. [19] по медицинским приборам;
- 98/79/EC от 27 октября 1998 г. [42] по медицинским приборам лабораторной диагностики.

Директива «по активным имплантируемым медицинским приборам» относится ко всем механизированным или частичным имплантатам, находящимся в теле пациента (например, кардиостимуляторы).

Директива «по медицинским приборам» охватывает большинство других медицинских приборов (не только медицинских электронных приборов), например бандажи первой помощи, протезы тазобедренного сустава, рентгеновское оборудование, ЭКГ, сердечные клапаны.

Директива «по медицинским средствам лабораторной диагностики» охватывает все медицинские приборы, такие как реактивы, продукты реактивов, калибраторы, контрольные материалы, комплекты медицинских инструментов, приборы, аппараты, оборудование или системы, необходимые для лабораторного исследования проб, включая кровь и образцы тканей, полученных из тела человека. Примерами являются реактивы для определения группы крови, тестовые комплекты для определения беременности или гепатита В.

В данных директивах медицинский прибор определен следующим образом:

«Любой прибор, аппарат, материал прибора или иной предмет, используемый автономно или в комбинации, включая программное обеспечение, необходимое для его правильного применения, предназначенный изготовителем для применения на людях с целью:

- диагностики, профилактики, мониторинга, лечения или облегчения заболевания;
- диагностики, контроля, лечения, а также облегчения или компенсации травмы или увечья;
- исследования, замены или изменения анатомии или физиологического процесса;
- контроля оплодотворения

и не реализующий своего основного назначения в или на теле человека с помощью фармакологических, иммунологических или метаболических средств, но которому данные средства могут помогать осуществлять его функции».

Данное определение включает только программное обеспечение, «необходимое для правильного применения» медицинского прибора. Однако данное определение может быть расширено в ближайшем будущем для учета программного обеспечения, которое само по себе является медицинским прибором.

Директивы по медицинским приборам и по медицинским приборам лабораторной диагностики включают систему классификации, на основании которой уровень регулятивного контроля, применяемого к прибору, соотносится с воспринимаемой степенью риска, ассоциированной с прибором.

Средства контроля, применяемые к медицинскому прибору, включают такие мероприятия, как регистрация изготовителей и изделий, требования к проектированию и производству, проверка соответствия всем требованиям.

А.1.3 Австралия

Австралия 4 октября 2002 г. приняла новую систему регулирования медицинских приборов [43], [44], основанную на международной модели регулирования, разработанной GHTF [55]. Данная модель и австралийская система во многом сходны с системами регулирования ЕС. Различия между Австралией и ЕС [45], [46] несущественны в контексте настоящего стандарта. Таким образом, определение медицинского прибора, системы классификации, требования к регистрации и контрольным мероприятиям аналогичны применяемым в ЕС.

Как и в ЕС, программное обеспечение включается в рассмотрение, только когда оно необходимо для «правильного применения» медицинского прибора. В Австралии существует Австралийский реестр терапевтических товаров (ARTG). Поиск в данном реестре терминов «программное обеспечение» и «компьютер» выявил только системы программного обеспечения, необходимые для правильного применения медицинских приборов, но не выявил системы программного обеспечения, представляющие программные продукты для сферы здравоохранения, как они определены в настоящем стандарте (самой близкой к этому определению оказались системы Архивиро-

вания изображений и коммуникаций — программы PACS). Аналогично в австралийской системе классификации присутствует только «программное обеспечение для обработки изображений».

А.1.4 Канада

В Канаде медицинские средства контролируются посредством Положения по медицинским приборам [47] и разделов Акта о пищевых продуктах и лекарствах, применимых к медицинским приборам. Орган «Health Canada» отвечает за соответствие и соблюдение законов в национальном масштабе [48].

Хотя в определении медицинского прибора не упоминается программное обеспечение, в Положение по медицинским приборам включено следующее требование:

«Если медицинский прибор представляет собой или содержит программное обеспечение, то программное обеспечение должно быть спроектировано так, чтобы реализовывать замысел изготовителя, и должно быть аттестовано».

Медицинские приборы и приборы для лабораторной диагностики классифицируются посредством правил, разработанных так, чтобы быть «гармонизированными» с правилами классификации приборов ЕС и классификациями приборов США [49], [50]. Классификация медицинских приборов практически совпадает с классификациями, принятыми в Австралии и ЕС. Программное обеспечение не упоминается прямо, за исключением программного обеспечения, предназначенного для конкретных приборов, например активных терапевтических или диагностических приборов, приборов, излучающих радиацию, систем доставки лекарственных средств и анестезирующего оборудования. Программное обеспечение также упоминается как предназначенное для использования в приборах для лабораторной диагностики.

Программа «Канадские терапевтические изделия» содержит указатель по ключевым словам, чтобы помочь изготовителям определять класс медицинских приборов [51].

Хотя в указателе имеется категория «компьютер», все описания систем привязаны к медицинским приборам конкретных видов. Поэтому программное обеспечение, относящееся к программным продуктам для сферы здравоохранения в контексте настоящего стандарта, не охватывается средствами контроля.

А.2 США

В США медицинские приборы контролирует Управление по контролю за продуктами питания и лекарствами (FDA) и его Центр по приборам и радиологической безопасности (CDRH).

В соответствии с определением Федерального акта о пищевых продуктах, лекарственных и косметических средствах медицинский прибор представляет собой «инструмент, аппарат, приспособление, машину, механическое приспособление, имплантат, лабораторный реактив или иной подобный объект, включая составные части, или аксессуар, который:

- присутствует в официальном Национальном справочнике, Фармакопее Соединенных Штатов или в какомлибо из приложений к ним, предназначен для диагностики заболевания или других состояний либо для исцеления, облегчения, лечения или профилактики заболевания у человека или животных, или предназначен для воздействия на строение или какую-либо функцию тела человека или животных, и достижение какой-либо из его основных целей не осуществляется посредством химического воздействия в или на теле человека или животного и не зависит от его метаболизации».

Программное обеспечение, «содержащееся» в медицинском приборе, включая имеющееся на рынке программное обеспечение, используемое в медицинских приборах, охватывается данными средствами контроля [52], [53]. «Руководство по общим принципам аттестации программного обеспечения» [54] относится к:

- программному обеспечению, используемому в качестве компонента, части или аксессуара медицинского прибора;
- программному обеспечению, которое само по себе является медицинским прибором (например, программное обеспечение для определения группы крови);
- программному обеспечению, используемому при производстве прибора (например, контроллеры с программируемой логикой в производственном оборудовании);
- программному обеспечению, используемому при реализации системы качества у изготовителя прибора (например, программное обеспечение, регистрирующее и поддерживающее ведение истории прибора).

Таким образом, можно считать, что средства контроля медицинских приборов применяются к программному обеспечению в соответствии с приведенным выше определением.

Неясным остается вопрос, какое программное обеспечение само по себе является медицинским прибором. Понятно, что программное обеспечение, подпадающее под определение медицинского прибора, таковым является. Однако программные продукты для сферы здравоохранения в контексте настоящего стандарта по существу не могут быть описаны как «инструмент, аппарат, приспособление, машина, механическое приспособление, имплантат, лабораторный реактив или иной подобный объект, включая составные части, или аксессуар». С другой стороны, программное обеспечение может обладать одной из функций, указанных в определении медицинского прибора, например «предназначается для использования при диагностике заболевания или других состояний». Изучение «Кодов изделий» FDA/CHRA и области применения «Классификации приборов» не дает ответа на данный вопрос. Независимо от того, может или нет программное обеспечение, относящееся к категории программных продуктов для сферы здравоохранения, быть описано как медицинский прибор, практически очень небольшая

часть программных продуктов для сферы здравоохранения в контексте настоящего стандарта может регулироваться как медицинский прибор.

Однако целью изучения правил для медицинских приборов является определение того, существует ли какое-либо программное обеспечение, относящееся к медицинским приборам, на которое распространяются соответствующие руководства и средства контроля, которые можно было бы применить в отношении неконтролируемого программного обеспечения, то есть программных продуктов для сферы здравоохранения. В США существуют такие руководство и средства контроля, которые могут быть рассмотрены с этой точки зрения (например, см. В.3).

Система классификации медицинских приборов США, несмотря на некоторые различия, в основном соответствует системе, применяемой в ЕС, Австралии, Канаде и GHTF, по крайней мере, в контексте настоящего стандарта. Однако рекомендации FDA, относящиеся к программному обеспечению, содержащемуся в медицинских приборах (см. [52]), предусматривают систему классификации такого программного обеспечения в соответствии с риском или «уровнем беспокойства». Данная классификация рассмотрена в разделе В.3 (приложение В) в отношении программных продуктов для сферы здравоохранения.

А.3 Рабочая группа по глобальной гармонизации (GHTF)

В GHTF входят представители национальных регулирующих органов по медицинским приборам и промышленности. Назначением GHTF является поддержка сближения в области регулирования, обеспечивающего безопасность, эффективность, производительность и качество медицинских приборов. Через свои пять рабочих групп GHTF публикует руководящие материалы, часть которых имеют отношение к настоящему стандарту.

GHTF «гармонизировала» определение медицинского прибора следующим образом [8].

«Под медицинским прибором подразумевается любой инструмент, аппарат, приспособление, машина, имплантат, лабораторный реагент или калибратор, программное обеспечение, материал или другой подобный или родственный объект:

a) предназначенный изготовителем для использования автономно или в комбинации с другими объектами на людях для одной или нескольких из следующих конкретных целей:

- диагностика, профилактика, мониторинг, лечение или облегчение заболевания;
- диагностика, мониторинг, лечение, облегчение или компенсация травмы;
- исследование, замена, модификация или поддержка анатомии или физиологического процесса;
- помощь или поддержание жизни;
- контроль оплодотворения;
- дезинфекция медицинских приборов;
- предоставление информации в медицинских или диагностических целях посредством лабораторного исследования;
- исследование проб, взятых из тела человека;

b) не реализующий своего основного назначения в или на теле человека посредством фармакологических, иммунологических или метаболических средств, но которому подобные средства могут помогать реализовывать его функцию».

Данное определение существенно отличается от определений, принятых в ЕС, Австралии, Канаде и США в том, что «программное обеспечение» в нем определено как медицинский прибор, а не как необходимое для применения медицинского прибора или являющееся его дополнением. Однако данное определение охватывает программное обеспечение, реализующее только указанные функции. Понятно, что многие программные продукты для сферы здравоохранения выходят за рамки реализации данных функций и поэтому не будут охвачены данным определением. Тем не менее некоторые из них будут ему соответствовать, например «программное обеспечение для диагностики заболеваний».

GHTF разработала документ «Принципы классификации медицинских приборов» [55], в котором предложено разделение медицинских приборов на четыре класса. Единственной явной ссылкой на программное обеспечение в нем является следующий абзац:

«Хотя большая часть программного обеспечения встроена непосредственно в медицинские приборы, существует и автономное программное обеспечение. При условии что такое автономное программное обеспечение относится к области применения определения «медицинского прибора», его следует классифицировать следующим образом:

- если программное обеспечение обеспечивает или влияет на использование отдельного медицинского прибора, то оно относится к тому же классу, что и сам прибор;
- если программное обеспечение является независимым от какого-либо медицинского прибора, то оно классифицируется само по себе в соответствии с правилами, изложенными в разделе 8».

Однако в 16 правилах, изложенных в разделе 8 указанного документа, программное обеспечение не упоминается ни в самих правилах, ни в примерах. Хотя данные правила основаны на риске, который медицинский прибор может представлять для пациента, риск не определяется в терминах последствий; так, при исследовании повреждения серьезность последствий определяется, например, тем, является ли прибор проникающим или нет. В этом смысле данная классификация совпадает с системами классификации, принятыми в ЕС, Австралии, Канаде и США.

Приложение В
(справочное)

Анализ процедур классификации

Примечание — Настоящий обзор предназначен только для целей настоящего стандарта, затрагивая и резюмируя только вопросы, имеющие к нему отношение. Он не должен использоваться в качестве полного руководства в каком-либо отношении и для какой-либо цели (в случае необходимости следует обратиться к исходным документам и компетентным национальным органам).

В.1 Классификации медицинских приборов в ЕС, Австралии, Канаде и GHTF

Несмотря на некоторые различия, системы классификации медицинских приборов в ЕС, Австралии и Канаде в основном схожи. В качестве иллюстрации ниже изложена сущность классификации медицинских приборов в ЕС, заимствованная из [56].

Правила ЕС представлены в приложении IX директивы по медицинским средствам 93/42/EEC [19]. Данная директива охватывает широкий спектр изделий, начиная от бандажей первой помощи и «ходунков» до сканеров компьютерной томографии и неактивных имплантатов. Медицинские приборы, охватываемые данной директивой, разделены на 4 класса следующим образом:

- класс I: в общем смысле представленный как класс низкого уровня риска;
- класс IIa: в общем смысле представленный как класс среднего уровня риска;
- класс IIb: в общем смысле представленный как класс среднего уровня риска;
- класс III: в общем смысле представленный как класс высокого уровня риска.

Различие между классами основывается на выборе доступных процедур оценки соответствия.

Указанное приложение начинается с ряда определений (инвазивный, активный, долгосрочный и т. п.), чтобы минимизировать любую возможную неоднозначность. Далее приведен ряд исполнительных правил, основанных на базовых принципах, например: «Если к прибору можно применить более одного правила, то он классифицируется по наиболее строгому из них».

Правила представляют собой набор общих формулировок, связанных с ситуациями, функциями, обрабатываемыми частями тела, свойствами и т. п., но не с перечнем изделий, который бы требовал постоянного обновления.

Существуют 4 группы правил:

- правила 1—4: неинвазивные приборы;
- правила 5—8: инвазивные приборы;
- правила 9—12: дополнительные правила для активных приборов;
- правила 13—18: различные правила для изделий, которые заслуживают отнесения к более высокой классификации, чем та, к которой они могут быть приписаны.

Хотя целью настоящего стандарта не является подробное рассмотрение всех этих правил, они явно не предназначены для программных продуктов для сферы здравоохранения и не могут быть применены к ним. Если же они были применены, то все программные продукты для сферы здравоохранения были бы отнесены к классу I, «низкого уровня риска». Понятно, что такой подход не годится.

Процедуры классификации в Австралии [57] и Канаде [49] являются неподходящими по тем же причинам. То же можно сказать и о GHTF [55].

В.2 Классификация медицинских приборов в США

Процедура классификации в США основана на более широком определении риска, нежели «низкий», «средний» и «высокий». Например, к классу III отнесены приборы, которые «поддерживают или защищают жизнь и имеют существенное значение для предотвращения ухудшения здоровья человека или представляют высокий потенциальный риск заболевания или травмы». Тем не менее процедура классификации, включая документ «Классификация приборов в США», не представляется подходящей для программных продуктов для сферы здравоохранения по тем же причинам, что и системы, используемые в Австралии, Канаде и ЕС.

В.3 Руководство Управления по контролю за продуктами питания и лекарствами США по классификации программного обеспечения

Управление по контролю за продуктами питания и лекарствами США (далее — FDA) выпустило руководство по программному обеспечению, охватываемому средствами контроля медицинских приборов. Оно содержит материалы, существенные для настоящего стандарта.

«Руководство по содержанию предпродажных документов для программного обеспечения, содержащегося в медицинских приборах» [9] определяет классификацию такого программного обеспечения на основе «уровня значимости», который оно представляет для пациентов или операторов. Сущность и детальность предпродажной документации также соотнесены с уровнем значимости. Уровень значимости «основывается на оценке серьезности вреда, который прибор может причинить, непосредственно или косвенно, пациенту или оператору в результате

сбоев в работе прибора, ошибок проектирования или просто применения прибора по его прямому назначению». В Руководстве выделены три уровня значимости:

- **высокий:** если сбой или скрытые ошибки проектирования могут привести непосредственно к летальному исходу или нанесению серьезного вреда для пациента или оператора; уровень значимости также определяется как высокий, если сбой или скрытые ошибки могут косвенно привести к летальному исходу или нанесению серьезного вреда для пациента или оператора вследствие искажения или задержки информации либо действий медицинского работника;
- **средний:** если сбой или скрытые ошибки проектирования могут привести непосредственно к нанесению незначительного вреда для пациента или оператора; уровень значимости также определяется как средний, если сбой или скрытые ошибки могут косвенно привести к нанесению незначительного вреда для пациента или оператора вследствие искажения или задержки информации либо действий медицинского работника;
- **низкий:** если сбой или скрытые ошибки проектирования не могут привести к нанесению какого-либо вреда для пациента или оператора.

Серьезный вред определен как травма или заболевание, которое:

- угрожает жизни;
- приводит к устойчивому ухудшению функций организма или к устойчивому повреждению структуры организма;
- требует медицинского или хирургического вмешательства для предотвращения устойчивого ухудшения функций организма или устойчивого повреждения структуры организма.

Термин «устойчивый» определен как «необратимое ухудшение или повреждение структуры или функций организма, за исключением незначительных ухудшений или повреждений».

Незначительный вред определен как вред, который не подпадает под определение серьезного вреда.

Особое значение имеет рекомендация, в соответствии с которой уровень значимости оценивается «до снижения опасности», то есть прибор, содержащий программное обеспечение, должен оцениваться без учета принятых мер по снижению опасности.

Данная рекомендация нашла свое отражение в руководстве FDA по использованию присутствующего на рынке программного обеспечения в медицинских приборах [10], в котором приведена следующая точка зрения Центра по приборам и радиологической безопасности (далее — CDRH) FDA.

«Поскольку оценить риски для опасностей, связанных с программным обеспечением, на основании частоты сбоев программного обеспечения достаточно трудно, CDRH пришел к выводу, что управление техническими рисками для программного обеспечения медицинских приборов должно фокусироваться на серьезности вреда, который может быть нанесен в результате сбоя программного обеспечения. Анализ опасностей определяется как идентификация опасностей и вызывающих их причин [67]. Основываясь на определениях анализа рисков из [36] и [68], можно сказать, что анализ опасностей, по сути, является подмножеством анализа рисков; поскольку анализ рисков для программного обеспечения не может основываться на вероятности инцидента, то реальная функция анализа рисков для программного обеспечения может быть сведена к функции анализа опасностей. С технической точки зрения, использование любого из терминов — «анализ рисков» или «анализ опасностей» является уместным. Однако CDRH принял решение применять термин «анализ опасностей», чтобы подчеркнуть положение, что расчет риска на основании частоты сбоев программного обеспечения, как правило, неправомерен, и поэтому более уместно управлять рисками со стороны программного обеспечения на основании серьезности вреда, а не на основании частоты сбоев программного обеспечения».

Руководство по присутствующему на рынке программному обеспечению также предлагает классификацию, основанную на «уровне значимости», по существу, с аналогичными определениями.

Данные руководящие документы FDA определяют возможные подходы к программным продуктам для сферы здравоохранения. Однако следует отметить, что в руководстве по программному обеспечению для медицинских приборов отмечено, что руководство по «уровню значимости» применимо только к предпродажным документам, и «не относится к классификации приборов (классам I, II, или III) или непосредственно к анализу опасностей или рисков».

В.4 Классификация ИСО/СЕН программных продуктов для сферы здравоохранения

ИСО и СЕН через свои Технические комитеты по информатизации здоровья ИСО/ТК 215 и СЕН/ТК 251 опубликовали идентичные технические спецификации по классификации рисков для безопасности от медицинского программного обеспечения [11], [12]. Данные технические спецификации обеспечивают средства для широкого скрининга программных продуктов для сферы здравоохранения, с тем чтобы классифицировать их в соответствии с риском, который они могут представлять для пациентов. Одним из предполагаемых применений данной классификации является ее использование в качестве основы для определения средств контроля на стадиях проектирования и производства, соответствующих риску.

В технических спецификациях определены пять классов риска, основанных на последствиях для пациента, если в программном продукте для сферы здравоохранения произошел сбой или он стал причиной неблагоприятного события и вероятности того, что последствие может иметь место в «достаточно предсказуемых обстоятельствах».

Последствия разделяют на пять категорий:
- катастрофические;
- серьезные;
- значительные;
- умеренные;
- незначительные.

Описание этих категорий приведено в таблице В.1.

Таблица В.1

Категория	Интерпретация	
	Последствие	Число случаев
Катастрофические	Летальный исход. Устойчивая недееспособность и любое состояние, при котором прогнозируется летальный исход или устойчивая недееспособность; серьезная травма или недееспособность, последствия которой не будут преодолены в ближайшее время	Множество Множество
Серьезные	Летальный исход. Устойчивая недееспособность и любое состояние, при котором прогнозируется летальный исход или устойчивая недееспособность; серьезная травма или недееспособность, последствия которой не будут преодолены в ближайшее время. Серьезная травма или недееспособность, восстановление после которой ожидается в ближайшее время. Серьезная психологическая травма	Единичные Единичные Множество Множество
Значительные	Серьезная травма или недееспособность, восстановление после которой ожидается в ближайшее время. Серьезная психологическая травма. Незначительная травма или травмы, восстановление после которых не ожидается в ближайшее время. Умеренная психологическая травма	Единичные Единичные Множество Множество
Умеренные	Незначительная травма или травмы, восстановление после которых не ожидается в ближайшее время. Умеренная психологическая травма. Незначительная травма, восстановление после которой ожидается в ближайшее время. Незначительное психологическое расстройство; беспокойство	Единичные Единичные Множество Множество
Незначительные	Незначительная травма, восстановление после которой ожидается в ближайшее время; незначительное психологическое расстройство; беспокойство; любые несущественные последствия	Единичные

Выделяют пять категорий вероятности возникновения последствий:
- очень высокая;
- высокая;
- средняя;
- низкая;
- очень низкая.

Описание этих категорий приведено в таблице В.2.

Таблица В.2

Вероятность	Описание
Очень высокая	Обязательно или почти обязательно; большая вероятность, что событие произойдет
Высокая	Не обязательно, но весьма возможно; ожидается, что событие произойдет в большинстве случаев
Средняя	Возможно; есть вероятность, что событие произойдет
Низкая	Событие может произойти, но в большинстве случаев не произойдет
Очень низкая	Незначительная или практически незначительная вероятность события

Наконец, «классы риска», на которые подразделяют продукты, представлены в таблице В.3.

Таблица В.3

Вероятность	Последствия				
	Катастрофические	Серьезные	Значительные	Умеренные	Незначительные
Очень высокая	A	A	B	B	C
Высокая	A	B	B	C	C
Средняя	B	B	C	D	D
Низкая	B	C	D	D	E
Очень низкая	C	C	D	E	E

Класс А соответствует наивысшему потенциальному риску, а класс Е — самому низкому.

Важными являются приведенные ниже требования.

«При идентификации опасностей, которые программный продукт или тип программных продуктов для сферы здравоохранения может представлять для пациента, опасность не должна отбрасываться просто из-за предположения, что продукт разработан таким образом, что не существует обстоятельств, при которых возможно возникновение опасности вследствие свойств конкретного программного продукта или проекта, по которому он создавался. Возможность вреда (опасности), который может нанести программный продукт, должна быть определена, как если бы соответствующих свойств проекта или средств контроля не существовало или они работали бы неправильно.

При идентификации опасностей, которые программный продукт для сферы здравоохранения может представлять для пациента, независимо от того, связаны ли они с неправильным функционированием или являются результатом непредусмотренного события, также не следует отбрасывать опасности, которые могли возникнуть просто из-за отсутствия неблагоприятных последствий для пациента благодаря, например, бдительности пользователя или другим событиям, внешним по отношению к программному продукту. Данный аспект учитывается посредством назначения вероятности возникновения последствий».

«При оценке вероятности вероятность последствия не должна отбрасываться в связи с каким-либо свойством самого продукта (включая сопутствующие инструкции по применению). Вероятность в контексте настоящего раздела не является вероятностью неправильного функционирования продукта или неблагоприятного события. Здесь имеется в виду вероятность последствий такого неправильного функционирования или неблагоприятного события, действительно имевшего место.

Однако допустимо принять во внимание реально прогнозируемые обстоятельства, являющиеся внешними по отношению к программному продукту. Таким образом, если, например, идентифицированное последствие опасного события может привести к травме, то вероятность данного последствия, выразившегося в нанесении реального вреда пациенту, может учитывать следующие аспекты:

- возможность того, что опасное событие будет замечено пользователем, обладающим соответствующей квалификацией, до того как произойдет его последствие;
- возможность того, что последствия удастся избежать вследствие ряда событий в течение некоторого интервала времени, произошедших до возникновения последствия, которые повысили бы вероятность выявления опасности;
- возможность того, что пациент будет осмотрен врачом до того, как ему будет нанесен реальный вред, и будет достаточно времени для проведения лечения или терапии».

Технические спецификации содержат рекомендации в отношении того, как следует применять данные требования к программным продуктам для сферы здравоохранения.

Подход к классификации программных продуктов для сферы здравоохранения, изложенный в технических спецификациях, согласуется с подходом FDA к классификации «программного обеспечения для медицинских приборов» [9] и «присутствующего на рынке программного обеспечения» [10] (см. В.3).

Три «уровня значимости», определенные в классификации FDA, могут быть сопоставлены с пятью категориями последствий, определенными в технических спецификациях. Однако «уровень значимости» FDA не совсем соответствует вероятности последствия, например летальный исход или травма, имевшие место в действительности. Это же относится и к безопасности оператора и пациентов, в отличие от самого пациента.

В.5 Выводы

Системы классификации ЕС, Австралии, Канады, США и GHTF для медицинских приборов не подходят для программных продуктов для сферы здравоохранения.

Классификация FDA CDRH «программного обеспечения в медицинских приборах» и «присутствующего на рынке» программного обеспечения может быть применена к программным продуктам для сферы здравоохранения.

Однако в [11] представлена наиболее подходящая система классификации, основанная на классах рисков. Они соответствуют подходу FDA CDRH к «программному обеспечению в медицинских приборах» и «присутствующему на рынке» программному обеспечению.

Приложение С
(справочное)

Управление рисками

С.1 Общие сведения

Если управление рисками должно использоваться в качестве контрольного мероприятия, то потребуются подкрепляющие его стандарты. В настоящем приложении рассмотрена приемлемость для этой цели уже существующих стандартов.

Примечание — Настоящий обзор предназначен только для целей настоящего стандарта, затрагивая и резюмируя только вопросы, имеющие к нему отношение. Он не должен использоваться в качестве полного руководства в каком-либо отношении и для какой-либо цели (в случае необходимости следует обратиться к исходным документам и компетентным национальным органам).

С.2 Атрибуты, необходимые для успешного внедрения процессов управления рисками

Для успешного применения управления рисками к программным продуктам для сферы здравоохранения в стандартах, руководствах и инструментах должны присутствовать ключевые атрибуты, а именно:

- доступный для понимания базовый процесс, включающий логику вычисляемых результатов и не привлекающий внешний персонал и других специалистов;
- совокупность всех основных составляющих риска;
- возможность измерения и взвешивания элементов на языке здравоохранения и в контексте незавершенного исторического события и данных об инциденте, позволяющая реализацию количественного подхода;
- гибкость в терминах детализации анализа и рекомендаций по средствам контроля, соответствующих сложности программного продукта для сферы здравоохранения, вычисленным уровням риска и стадии разработки продукта;
- способность итерационного повторения и расширения возможностей по оценке и управлению рисками в ходе разработки программного продукта для сферы здравоохранения;
- поддержка составных процессов и сложной природы программных продуктов для сферы здравоохранения в форме баз знаний, чтобы помочь их использованию «неспециалистами».

Данные атрибуты были использованы для оценки разных кандидатов в стандарты.

С.3 Минимум компонентов, необходимых для эффективного управления рисками

Во многих областях, смежных с разработкой программных продуктов для сферы здравоохранения, таких как информационная безопасность, с определенным успехом внедрены процессы управления рисками (см. С.6). Однако существуют установленные на практике общие компоненты управления рисками, являющиеся полезными индикаторами приемлемого процесса при разработке программных продуктов для сферы здравоохранения:

- идентификация свойств компонентов программного продукта для сферы здравоохранения, а также факторов риска и уязвимости этих свойств;
- оценка влияния (на изготовителя, пользователя и пациента со стороны программного продукта для сферы здравоохранения);
- вероятность угроз и оценка степени защищенности;
- определение уровней рисков (как составного результата уровней влияния, угроз и степени защищенности);
- идентификация рекомендуемых средств контроля (то есть обоснованных и соответствующих);
- сравнение с существующими средствами контроля для определения областей корректируемого риска;
- дополнительные возможности для обработки риска, включая прямое управление, признание, предотвращение, управляемый перевод риска и т. п.;
- планирование обработки риска (то есть реализация контроля).

С.4 Процессы управление рисками на предприятии

С.4.1 Общие сведения

«Управление рисками на предприятии» — это новый термин, используемый для большего акцентирования комплексной природы процесса и, следовательно, применимости процесса к организации и осуществляемым ей действиям.

Можно ожидать, что стандарты по управлению рисками на предприятии являются высокоуровневыми документами, определяющими общую структуру, а не подробную модель процессов с сопутствующими базами знаний или экспертных знаний для поддержки анализа рисков и управления рисками от программных продуктов для сферы здравоохранения.

С.4.2 PD 6668:2000 «Управления рисками при корпоративном управлении»

Опубликованный документ PD 6668:2000 [58] в основном содержит информацию по основам управления рисками и охватывает:

- корни движущих механизмов управления рисками;
- план более широкого рассмотрения корпоративного управления;
- описание структуры управления рисками;
- практическое руководство по формулировке бизнес-требований к управлению стратегическими рисками;
- вопросник для сравнения эффективности структур управления рисками на предприятиях.

Структура включает в себя:

- классический подход к системам управления — планировать, исполнить, проверить и действовать (известный как PDCA);
- деятельность по управлению рисками на трех уровнях (стратегическом, управленческом, операционном);
- идентификацию угроз;
- оценку рисков;
- принятие решений о способах управления рисками;
- идентификацию ресурсов;
- планирование управления отдельными рисками;
- коммуникации;
- мониторинг и измерение.

Однако модель процесса дает только общее представление, несмотря на то что концепция «правдоподобия» широко признана. Возникает путаница между угрозами и контрмерами, например «неудачная попытка установить эффективные мероприятия в случае аварийной ситуации» приводится скорее в качестве примера угрозы, а не контрмеры.

Более того, применяемые матрицы основаны на оценках типа «Низкая», «Средняя» и «Высокая», что не позволяет классифицировать риски более чем по трем классам, что в свою очередь приведет к недостаточно специализированным структурам контроля.

Чрезвычайно важным для настоящего стандарта является тот факт, что руководство практически не содержит указаний по контрмерам. Также оно не описывает такие разделы, как списки угроз (они присутствуют только в виде примеров). Будучи документом высокого уровня, оно недостаточно всестороннее и специализированное для применения в секторе здравоохранения и не предоставляет механизмов по обеспечению безопасности пациентов при использовании программного обеспечения в сфере здравоохранения.

С.4.3 Стандарт Австралии и Новой Зеландии AS/NZS 4360:2004

Стандарт Австралии и Новой Зеландии AS/NZS 4360:2004 [59] был принят на национальном уровне организациями здравоохранения для целей корпоративного управления, включая Национальную службу здравоохранения Соединенного Королевства. Содержащиеся в нем понятия, такие как «обработка рисков», были взяты из других стандартов, основанных на рисках, таких как BS 7799-2:2002 (см. С.6.1). Он является еще одним высокоуровневым описанием необходимого процесса, хотя и с сопутствующим документом, содержащим руководства по управлению рисками. Данный документ является скорее справочником по возможным процессам, а не рекомендуемым подходом.

Данный стандарт определяет классический/типовой «процесс» управления рисками, независимый от конкретной отрасли промышленности или сектора экономики, но предполагающий необходимость гибкости при реализации.

В нем отмечается, что установление вероятности события и возможных последствий должно и может быть выполнено качественным, наполовину качественным или количественным образом, в зависимости от наличия статистики инцидентов. Однако данный стандарт содержит перечень уместных источников информации и технологий, которые могут быть применены. В стандарте содержатся руководства по следующим аспектам:

- выбор метода анализа (в зависимости от ситуации);
- реальные последствия и соответствующие градации вероятностей;
- типы шкал для измерения рисков, которые могут быть использованы;
- различные технологии для определения уровней рисков.

В области обработки рисков стандарт AS/NZS 4360 предоставляет подробную информацию по дополнительным возможностям обработки рисков с негативными последствиями (например, рисков для безопасности пациентов), относящуюся к следующим факторам:

- предотвращение риска посредством принятия решения не начинать или не продолжать некоторые действия;
- принятие мер по изменению вероятности отрицательных последствий;
- принятие мер, изменяющих последствия с целью уменьшения величины потерь, таких как страхование или планирование непредвиденных затрат;
- разделение рисков посредством контрактов и т. п., чтобы передать ответственность;
- фиксация/признание риска.

Более того, данный стандарт также содержит руководство по разработке планов обработки рисков, сопоставляющее стоимость обработки с приобретаемыми выгодами, чтобы обеспечить объективное признание риска. Однако противореча таким планам и даже конфликтуя с ними, данный стандарт в то же время в основном направлен на снижение риска до практически разумного уровня (так называемый принцип ALARP). На практике очень часто получается, что данный принцип подменяется неприемлемой и неуместной точкой зрения «избегания рисков».

В качестве общего руководства данный стандарт можно считать достаточно хорошо проработанным. Однако его неполнота с точки зрения экспертных знаний и недостаточное отражение специфики программных продуктов для сферы здравоохранения делают его неподходящим, если взять его «как есть» для целей настоящего стандарта.

С.4.4 Рабочая группа ИСО/МЭК по управлению рисками

Совместная рабочая группа ИСО/МЭК (Технической дирекции) по управлению рисками [35] была сформирована в середине 2005 г. Задачей рабочей группы была разработка международного стандарта на основе существующих национальных стандартов с внесением изменений при необходимости. Рабочий проект стандарта был опубликован для обсуждения. Предполагается, что данный проект должен стать «высокоуровневым, обобщенным, руководящим документом», который «обеспечивает поддержку существующих стандартов по конкретным приложениям, связанным с рисками», и «предоставляет определения и структуры, независимые от законодательных и регулятивных ограничений», но которые «применимы с минимальными изменениями» в качестве «основы для деловой повседневной практики».

Данный документ был структурирован следующим образом:

- комплекс принципов успешной практики по управлению рисками;
- организационный контекст управления рисками;
- структура управления рисками, состоящая из:
- общения и консультаций;
- установления (делового) контекста;
- идентификации риска;
- оценки риска;
- обработки риска;
- мониторинга и анализа.

В отличие от аналогичных стандартов данная структура включает в себя оценку существующих средств контроля как части анализа рисков, не определяя тем самым «базовый риск» и фокусируясь на «сетевом риске». Причины, по которым было принято такое решение, неясны. Проект изложен в основном с использованием терминов рисков, относящихся к организации, а не к применению анализа рисков и управления рисками для безопасности программного продукта. Следовательно, он представляется неуместным в контексте обеспечения безопасности программных продуктов для сферы здравоохранения.

Что касается других стандартов высшего уровня, то данный рабочий проект содержит перечни примеров, но не предлагает окончательно установленного процесса с экспертной поддержкой.

С.4.5 Выводы в отношении стандартов по управлению рисками предприятия

Поскольку данные стандарты не ориентированы на здравоохранение, ни один из рассмотренных в данном разделе стандартов не обеспечивает достаточно четкой или определенной модели процесса, которую можно было бы применить для целей настоящего стандарта. Однако имеет место некоторый общий уровень унификации между предложенными в них процессами. Отдельные компоненты каждого из данных документов, особенно AS/NZS 4360, могут претендовать на их применение для программных продуктов для сферы здравоохранения.

С.5 Стандарты по управлению рисками, относящиеся к здравоохранению

С.5.1 ИСО 14971:2007 «Применение управления рисками к медицинским приборам»

ИСО 14971:2007 [36] является признанным международным стандартом по управлению рисками применительно к медицинским приборам. Стандарт по системам качества для медицинских приборов ИСО 13485:2003 [27], в частности, ссылается на ИСО 14971 по управлению рисками. FDA в 2001 г. также признало ИСО 14971 в качестве основного стандарта по управлению рисками для медицинских приборов.

В рекомендации 4 заключительного отчета Рабочей группы по технологиям здравоохранения (HTTF) при Объединении по мировым стандартам (WSC), опубликованного в 2006 г. [60], говорится:

«Следует отметить недавние усилия рабочей группы Технической дирекции ИСО по разработке более глобального стандарта по управлению рисками. WSC должно обеспечить, чтобы разработка более общего стандарта по управлению рисками не заменяла, не изменяла или не пересекалась с существующим международным стандартом ИСО 14971, широко применяемым в отношении медицинских приборов».

ИСО 14971 представляет обзор процесса управления рисками, предназначенного для использования как неотъемлемого элемента системы качества. Соответствие международному стандарту требует выполнения следующих действий:

- установить процесс управления рисками;
- установить политику по отношению к приемлемым рискам;

- нанять и подготовить квалифицированный персонал;
- провести анализ рисков;
- провести оценку рисков;
- осуществить контроль рисков;
- провести заключительный анализ управления рисками и предоставить информацию по остаточному риску;
- предоставить постпроизводственную информацию.

В ИСО 14971:2007 включены следующие технологии анализа риска:

- анализ видов и последствий отказов (FMEA-анализ);
- анализ дерева неисправностей (FTA-анализ);
- исследование опасности и работоспособности (HAZOP).

Не предусмотрено никаких средств или технологий оценки воздействия, и данный международный стандарт не обеспечивает четкого разделения понятий оценки воздействия, оценки угрозы и степени защищенности и средств контроля. Более того, в нем предполагается, что процесс принятия решений о приемлемости идентифицированных рисков с учетом уменьшения их влияния, реализованного в процессе проектирования, должен представлять собой действие по оценке рисков. Это противоречит содержанию других стандартов, рассмотренных в настоящем приложении. Тем не менее в данный стандарт включена полезная таблица по средствам контроля рисков.

С.5.2 Документ GHTF/SG3/NI5R8 «Принципы управления рисками и системы управления качеством»

В документе GHTF/SG3/NI5R8 [39] рассмотрена реализация принципов управления рисками и действий в рамках системы управления качеством. Утверждается, что изготовители медицинских приборов обычно должны (в соответствии, например, с регулятивными или законодательными требованиями) иметь на производстве систему управления качеством, а также установленные процессы, соответствующие рискам, связанным с приборами.

Поскольку процессы управления риском могут развиться до автономной системы управления, изготовителям медицинских приборов рекомендуется их интегрировать для снижения затрат, устранения избыточности и создания более эффективной системы управления. Данный документ предназначен для поддержки изготовителей медицинских приборов в части интеграции системы управления рисками или принципов и действий, установленных для управления рисками, в существующую у них систему управления качеством. Варианты интеграции иллюстрируются примерами с решениями.

В ИСО 15941:2007, приложение А, представлена матрица, связывающая серьезность наносимого вреда с вероятностью инцидента (точнее, с правдоподобием инцидента). Однако серьезность представлена в матрице просто как «низкая, средняя и высокая», а ячейки на пересечении столбцов и строк окрашены красным, желтым и зеленым цветами. Кроме того, приведено полезное, хотя и высокоуровневое, изображение технологического процесса управления рисками при проектировании и разработке. Отмечена также важность рассмотрения и согласования уровня допустимого риска на ранних стадиях данного процесса.

Однако принципы управления рисками, упомянутые в названии данного документа, не рассмотрены подробно, и маловероятно, что данный документ будет непосредственно использоваться кем-либо кроме экспертов.

С.5.3 ИСО/МЭК 62304 «Процессы жизненного цикла программного обеспечения медицинских приборов»

ИСО/МЭК 62304 [61] был разработан совместной рабочей группой ИСО/МЭК, состоявшей из членов подкомитета 62А «Общие вопросы электрооборудования, применяемого в медицинской практике», технического комитета 62 МЭК «Электрооборудование в медицинской практике» и Технического комитета 210 ИСО «Управление качеством и соответствующие общие вопросы по медицинским приборам».

Данный стандарт объединяет требования к модели жизненного цикла программного обеспечения, установленные в ИСО 12207:1995 [30] и поправке к нему [31], с риском, основанным на подходе, установленном в ИСО 14971 [36]. ИСО 12207 относится к разработке и сопровождению программного обеспечения медицинских приборов, когда программное обеспечение само по себе является медицинским прибором или когда программное обеспечение является встроенным или неотъемлемой частью медицинского прибора. Данный международный стандарт не охватывает аттестацию и выпуск на рынок медицинского прибора, даже если медицинский прибор состоит исключительно из программного обеспечения.

В данном стандарте представлена структура процессов, действий и задач, необходимых для проектирования и сопровождения безопасных медицинских приборов. В данном международном стандарте средства контроля представлены только в общем виде.

С.5.4 Документ FDA «Руководство по контролю проектирования для производителей медицинских приборов»

Документ FDA «Руководство по контролю проектирования для производителей медицинских приборов» [34] разработан для поддержки изготовителей медицинских приборов в понимании требований системы качества к контролю проектирования и применим как к проектированию медицинских приборов, так и к проектированию соответствующих технологических процессов. В данном руководстве вопросы рассматриваются в том же порядке, что и в директиве FDA по системам качества, которая вряд ли подойдет (напрямую) всем остальным пользователями. В документе представлено определение средств контроля проектирования и объяснено их значение. Отмечено, что управление рисками является процессом, который должен сопровождать весь процесс проектирования, однако данное положение практически не раскрыто.

С.5.5 Австралия и Канада

Австралийский документ «Руководство по медицинским приборам. Процедуры оценки соответствия» [62] и Канадская директива по соответствию медицинских приборов и его обеспечению [63] связаны с процедурами оценки соответствия, однако ни в одном из них в явном виде не приведено структурированное рассмотрение управления рисками.

С.5.6 Выводы по стандартам по управлению рисками, относящимся к здравоохранению

В рассмотренных стандартах, относящихся к здравоохранению, используются такие фразы и термины, как «анализ рисков», «оценка рисков» и «управление рисками». В большинстве стандартов данные термины используются для ссылки на классификацию медицинских приборов. Однако, как было показано, классы приборов (хотя они и могут явиться результатом формальной оценки) в значительной степени связаны с возможным влиянием на безопасность, а уровни угрозы и степени защищенности (объединяемые понятием «правдоподобие») не рассмотрены должным образом. Действительно, в большинстве рассмотренных стандартов и руководств часто встречаются такие фразы, как «например» и «включая», то есть в них не определяется процесс, который можно было бы использовать. Поэтому для эффективного использования данных документов требуются значительные усилия.

С другой стороны, в рассмотренных документах содержится достаточно данных, для того чтобы четко сформулировать, что понятия «медицинские приборы» и «программные продукты для сферы здравоохранения» не являются синонимами.

Более того, несмотря на то что многие из предложенных средств контроля медицинских приборов могут быть применены и к программным продуктам для сферы здравоохранения, сама сущность программных продуктов может потребовать применения иных средств контроля. Использование некоторых средств контроля, представленных в рассмотренных документах, предписано скорее законодательными требованиями, нежели определенным или идентифицированным риском. В настоящем стандарте законодательные мероприятия не рассматриваются.

При разработке стандарта по обеспечению безопасности пациентов при использовании программных продуктов для сферы здравоохранения наиболее полезными будут ИСО 14971 и GHTF/SG3/NI5R8, хотя отдельные положения могут быть заимствованы из большинства рассмотренных документов.

В совокупности рассмотренные документы дают полезное напоминание о необходимости анализа и управления рисками как в ходе проектирования, так и разработки, а также при контроле и поддержании соответствия в процессе всего жизненного цикла. Это особенно важно, поскольку программные продукты для сферы здравоохранения обычно чаще обновляются в форме выпуска новых модифицированных версий, чем медицинские приборы, которые обычно заменяются новыми изделиями.

С.6 Стандарты, связанные с управлением рисками

С.6.1 BS 7799-2:2002, ИСО/МЭК 17799:2005, ИСО/МЭК 27001:2005

В BS 7799-2:2002, ИСО/МЭК 17799:2005 [65] и ИСО/МЭК 27001:2005 [64] отражен передовой опыт в области управления информационной безопасностью, то есть в области, к которой относятся программные продукты для сферы здравоохранения. Первоначально BS 7799 был разработан в 1995 г. и с тех пор регулярно обновлялся и становился все более признанным в международном масштабе. Поскольку приведенное в нем определение информационной безопасности включает в себя конфиденциальность, целостность и доступность, можно сказать, что в данном стандарте учтены многие аспекты критичности безопасности, особенно когда безопасность пациента определяется качественной оценкой воздействия на него.

Данный британский стандарт состоит из двух частей:

- часть 1 содержит совокупность общепримени мых целей контроля, скомпонованных в подгруппы, и главные задачи;
- часть 2 определяет концепцию системы управления информационной безопасностью (на протяжении жизненного цикла), согласованную с критичностью безопасности, качеством, информационными процедурами и защитой окружающей среды. Система управления информационной безопасностью также базируется на модели PDCA (планирование, исполнение, проверка и реализация).

Цели контроля тесно связаны с вопросами оценки рисков для безопасности пациентов. К ним относят:

- политику безопасности;
- организацию и управление безопасностью;
- классификацию и контроль ресурсов;
- безопасность персонала;
- физическую и экологическую безопасность;
- управление коммуникациями и действиями;
- контроль доступа;
- разработку и сопровождение систем;
- управление непрерывностью бизнеса;
- соответствие;
- управление инцидентами.

BS 7799-2 был принят в качестве международного стандарта ИСО/МЭК 27001, содержание которого было скорректировано с учетом предыдущего стандарта ИСО/МЭК 17799:2005. BS 7799-1 еще ранее был принят в ка-

честве международного стандарта ИСО/МЭК 17799:2005, однако ожидается, что он будет включен в ИСО 27002. Кроме того, ожидается, что в ближайшем будущем в этой же серии появятся новые стандарты.

Важным для настоящего стандарта является центральная зависимость стандарта от сильно структурированной и всесторонней (и подробной) оценки риска бизнес-процессов, информационных сервисов и инфраструктур (аппаратное и программное обеспечение, носители данных, документация и т. д.), используемых в рамках системы управления информационной безопасностью.

Кроме юридических и регулятивных требований в ИСО/МЭК 27001:2005, подраздел 4.2, перечисление 1b, также дополнительно сделан акцент на рассмотрении контрактных обязательств на всех стадиях системы управления информационной безопасностью, особенно в отношении оценки рисков, обработки рисков, выбора средств контроля, контроля записей и ресурсов, мониторинга и анализа системы управления информационной безопасностью и требований к документации.

Более того, в будущем еще один документ, BS 7799-3:2006 [69], по управлению рисками в системе управления информационной безопасностью будет принят в качестве международного стандарта ИСО/МЭК 27005 [66]. В нем представлена информация, подобная приведенной в опубликованном документе Британского института стандартов PD 3002:2000. Этот документ содержит подробное описание проблем эффективной реализации управления рисками информационной безопасности, очень похожее по форме на перечень ключевых компонентов, представленный в С.3.

Комплекс стандартов ИСО 2700Х направлен на то же, что и стандарты МЭК 61508-3 и МЭК 61508-5 (см. С.6.2). Однако в нем снова отсутствуют всесторонние спецификации охватываемых процессов или вопросов, подлежащих рассмотрению. С другой стороны, область применения ИСО 27001 может быть в значительной мере использована в отношении оценок рисков для безопасности пациентов при использовании программных продуктов для сферы здравоохранения.

С.6.2 МЭК 61508 «Оценка критического риска для безопасности»

МЭК 61508 состоит из восьми частей. В части 0 представлен обзор. Основное содержание представлено в частях 1—4. Их проект был разработан в 1998 г., а проект части 2, содержащей требования к системам, связанным с безопасностью, был пересмотрен в 2000 г. Версии всех четырех частей, выпущенные в декабре 2005 г., в настоящее время являются предметом голосования в комитете. Части 5, 6 и 7 будут рассмотрены позже.

Стандарт применим к электрическим, электронным и программируемым электронным системам. Ранее возникал вопрос, должна ли область применения МЭК 61508 ограничиваться контроллерами с программируемой логикой. Однако последние разработки, например охватывающие информационные сетевые системы, связанные с безопасностью, подключенные к Интернету, подчеркнули применимость стандарта ко всем программируемым системам, независимо от их конкретного применения.

МЭК 61508 предназначен для совместного применения с ИСО 9000 и основывается на следующих положениях:

- безопасность не может быть абсолютной (с нулевым риском);
- риски, создаваемые системами, должны быть выявлены;
- недопустимые риски должны быть снижены или исключены;
- уверенность в безопасности должна быть определена заранее, а не ретроспективным анализом проекта;
- безопасность должна быть демонстрируемой;
- разрушение веры в то, что «все, сделанное (то есть построенное) хорошо, автоматически будет безопасным», имеет критическое значение;
- правильное функционирование не обязательно адекватно безопасности.

К настоящему стандарту имеют отношение следующие части МЭК 61508:

- Часть 1. Общие требования;
- Часть 3. Требования к программному обеспечению (то есть к программным компонентам);
- Часть 5. Примеры методов для дифференцирования уровней целостности безопасности.

Эффективное использование стандарта, несомненно, требует понимания управления рисками, и текущая версия частей 1—4 частично отражает мнение, что некоторые процессы слишком сложны и неоднозначны.

В основе данного стандарта лежит концепция «уровней целостности безопасности», которые в чем-то аналогичны уровням рисков. Хотя конкретные процессы по установлению уровней целостности безопасности не представлены, в части 5 показан спектр альтернативных методов. Главной среди них является классификация рисков, основанная на отображении частоты и последствиях, на основании которых выбирается один из четырех классов риска. Поскольку в данном случае «частота» понимается как синоним «правдоподобия», то мы имеем дело с процессом, основанным на рисках, в чистом виде, и данный стандарт приходит к тем же выводам, что и GHTF/SG3/N15R8 [39].

Однако примеры, приведенные в части 5, остаются высокоуровневыми и не опускаются до подробных перечней критериев, подлежащих рассмотрению, или средств контроля, подходящих для применения. Также следует учесть относительное предпочтение стандарта к количественным мерам оценки рисков, хотя потенциальная роль качественной оценки в нем также признается. Разумеется, качественную оценку будет практически невозможно применить при отсутствии надежного или обширного банка статистики, на основании которого она могла бы быть сформирована.

Поскольку МЭК 61508 представляет совокупность понятий и принципов, которые могут быть учтены при оценке рисков для безопасности пациентов со стороны программных продуктов для сферы здравоохранения, механизмы, представленные в стандарте в настоящем виде, обычно рассматриваются в комплексе и едва ли могут быть реализованы подходящим образом. Поэтому если какой-либо процесс оценки будущих рисков со стороны программных продуктов для сферы здравоохранения и мог бы использовать основные принципы, то это считается непригодным. Кроме того, особенно важно будет достичь общей согласованности со сферой медицинских приборов, где уже используется ИСО 14971 (см. С.5.1), и в которой используются разные, как правило, более практичные механизмы.

С.6.3 Метод оценки риска информационной безопасности Правительства Великобритании CRAMM

CRAMM [40] является методом, распространяемым на коммерческой основе. В виде исключения он рассмотрен в настоящем стандарте с признанием того, что он является интеллектуальной собственностью правительства Великобритании, что он широко и успешно применяется многими организациями здравоохранения, а также внедрен в Национальную службу здравоохранения Великобритании.

Данный метод был разработан примерно 17 лет назад и регулярно развивался и пересматривался. В течение почти всего времени он поддерживался полуавтоматической сервисной программой, и известно, что более 600 копий данной сервисной программы были внедрены более чем в 25 странах.

Данный метод и его сервисная программа поддерживают:

- процесс управления информационной безопасностью по BS 7799/ИСО 27001;
- моделирование ресурсов и зависимостей;
- анализ и управление рисками информационной безопасности, включая обработку рисков;
- спецификацию требований к непрерывности и возвращению к норме;
- создание библиотеки многократно используемых моделей рисков и соответствия;
- итеративные оценки с использованием взаимодействующих уровней функциональности «экспресс» и «эксперт»;
- формирование отчетов по рискам и соответствию;
- средства повышения безопасности и планирование реализации.

Информационная безопасность трактуется в CRAMM в соответствии с ИСО 27001. CRAMM содержит базы знаний/экспертные системы, включая:

- около 400 типов ресурсов (в том числе обработку информации, информационные сервисы, аппаратное и программное обеспечение, коммуникационные протоколы, носители данных и места размещения);
- 26 разных типов воздействия (в том числе проблемы с конфиденциальностью, целостностью и доступностью);
- оценку воздействия по 10-балльной количественной или качественной шкале;
- около 40 типов угроз и степеней защищенности (включая случайные, преднамеренные, технические, человеческие и т. п. факторы), а также вопросы, на которые необходимо ответить, чтобы оценить их;
- семь уровней риска;
- восемь зон информационной безопасности (программное и аппаратное обеспечение, коммуникации, персонал, документация, процедуры, физические аспекты и излучения);
- около 3500 контрмер (организованных в иерархические группы по мере возрастания конкретности и охвата программных принципов, задач, функций и действующих образцов), индексированных в соответствии с угрозами и ресурсами, адекватным ответом на которые они являются.

Из изложенного выше следует, что подход, близкий к CRAMM или основанный на нем, может достаточно эффективно использовать оценку безопасности пациентов при использовании программных продуктов для сферы здравоохранения посредством систематизации существующих экспертных знаний, делающей информацию и процессы общедоступными, и упрощения их использования не экспертами.

С.6.4 Выводы по стандартам, связанным с управлением рисками

Все стандарты, рассмотренные в настоящем разделе, имеют прямое отношение к обеспечению безопасности пациентов при использовании программных продуктов для сферы здравоохранения, хотя ни один из них не может быть использован в его настоящем виде.

Совместное использование ИСО 27001 и CRAMM дает почти действующий образец того, что могло бы быть достигнуто при использовании метода и инструментальных средств, соответствующих концепциям, изложенным в МЭК 61508.

С.7 Общие выводы по стандартам по управлению рисками

Приведенный обзор показывает, что существует множество документов, стандартов и инструментальных средств по управлению рисками, многие из которых относятся к законодательным и регулятивным требованиям (которые не являются предметом рассмотрения в настоящем стандарте) или медицинским приборам (которые по своей сути отличаются от программных продуктов). Что касается стандартов по медицинским приборам, то в область применения некоторых из них включены программные продукты, хотя и как эффективные добавки к самим медицинским приборам.

Данный обзор стандартов показал, что они носят либо очень общий характер, либо слишком сложны для непосредственного применения для целей настоящего стандарта, то есть для решения конкретных проблем безопасности пациентов при применении программных продуктов для сферы здравоохранения неспециалистами (с определенной степенью уверенности в точности результата).

Учитывая, что четкие нормативные материалы появятся только после завершения разработки стандарта совместной рабочей группой ИСО/МЭК [35], следует понимать, что уже достигнуты существенная унифицированность и консенсус по ключевым компонентам эффективного управления рисками.

Многие компоненты рассмотренных стандартов, особенно примеры реализации, могут оказаться очень полезными, если их объединить. Однако подобное объединение все равно не обеспечит всестороннего освещения проблем, то есть потребуется их дальнейшая проработка.

Тем не менее при разработке любого стандарта по обеспечению безопасности пациентов при использовании программных продуктов для сферы здравоохранения все рассмотренные нормативные документы могут оказаться полезными.

Основываясь на рассмотренных нормативных документах и их практическом применении для высокоуровневых определений и конкретных реализаций, сложно предположить, что один нормативный документ сможет охватить все понятия и экспертные знания, необходимые для обеспечения безопасности пациентов при использовании программных продуктов для сферы здравоохранения. Даже если это могло бы быть достигнуто, то весьма маловероятно, что такой документ может быть также эффективно использован в реальных условиях без привлечения дополнительных средств поддержки.

Объединение ИСО 27001 и CRAMM создает почти рабочий образец того, что могло бы быть достигнуто.

Общий вывод заключается в том, что если управление рисками должно войти в перечень требований по обеспечению безопасности при использовании программных продуктов для сферы здравоохранения, то:

- требуется новый стандарт, согласованный на высоком уровне с результатами совместной рабочей группы ИСО/МЭК, ИСО 14971 и ИСО 61508, разработанный специально для программных продуктов для сферы здравоохранения. Такой стандарт должен воплощать концепции, изложенные в GHTF/SG3/NI5R8, и основываться на опыте использования CRAMM и ИСО/МЭК 17799;
- новый стандарт должен быть подкреплен руководством по реализации, предназначенным специально для программных продуктов для сферы здравоохранения.

Библиография

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

[2] An Organisation with a Memory, HMSO, June, 2000

[3] Quality in Australian Healthcare, Study, 1994

[4] Brennan T.A., Leape I.I., Laird N.M., Herbert I., Localio A.R. and Lawthers A.G. Incidents of adverse events and negligence in hospitalised patients, results of the Harvard Medical Practice Study, New England J Med., 324, 1991, p. 370—376

[5] Quality of care: patient safety, Report of the WHO Secretariat, EB 109/9, 5 December, 2001

[6] Building a safer NHS for Patients, UK Department of Health, April, 2001

[7] ISO/IEC Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards

[8] Information document concerning the definition of the term «Medical Device», Final document GHTF/SG1/N29R16:2005, GHTF Study Group 1, the Global Harmonization Task Force, 29 June, 1999

[9] Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Services, 11 May, 2005

[10] Off-the-Shelf Software Use in Medical Devices, Guidance, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Services, 9 September, 1999

[11] ISO/TS 25238, Health informatics — Classification of safety risks from health software

[12] CEN/TS 15260:2006, Health informatics — Classification of safety risks from health informatics products

[13] EN 1041:1998, Information supplied by the manufacturer with medical devices

[14] ISO 14155 (both parts), Clinical investigation of medical devices for human subjects

[15] ISO/TS 19218:2005, Medical devices — Coding structure for adverse event type and cause

[16] Adverse Event Reporting Guidance for the Medical Device Manufacturer or its Authorized Representative, Final Document GHTF/FD:99-7, GHTF Study Group 2, the Global Harmonization Task Force, 29 June, 1999

[17] UK National Patient Safety Agency, http://www.npsa.nhs.uk

[18] ISO/TS 22224, Health informatics — Electronic Reporting of adverse drug reactions

[19] Council Directive 93/42/EEC of 14 June, 1993, Concerning medical devices

[20] Guide to the implementation of directives based on the New Approach and the Global Approach, European Commission, Luxembourg, Office for Official Publications of the European Communities, 2000, ISBN 92-828-7500-8

[21] http://europa.eu.int/comm/enterprise/medical_devices/meddev/index.htm

[22] Guidance on Quality Systems for the Design and Manufacture of Medical Devices, GHTF.SG3.N99-8, Global Harmonization Task Force, 29 June, 1999

[23] ISO 9001:1994, Quality systems — Model for quality assurance in design, development, production, installation and servicing

[24] ISO/TR 14969:2004, Medical devices — Quality management systems — Guidance on the application of ISO 13485:2003

[25] Quality System Regulations, 21 CFR Part 820 [Federal Register, October 7, 1996, Part VII 21 CFR Parts 808, 812 and 820 Medical Devices; Current Good Manufacturing Practice (CGMP); Final Rule]

[26] Medical Device Quality Systems Manual: A Small Entity Compliance Guide, Center for Devices and Radiological Health, FDA, December, 1996

[27] ISO 13485:2003, Medical devices — Quality management systems — Requirements for regulatory purposes

[28] ISO 9001:2000, Quality management systems — Requirements

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

[30] ISO/IEC 12207:1995, Information technology — Software life cycle processes

[31] ISO/IEC 12207:1995/Amd.1:2002, Information technology — Software life cycle processes Amendment 1

[32] ISO/IEC TR 15271:1998, Information technology — Guide for ISO/IEC 12207 (Software Life Cycle Processes)

[33] Design Control Guidance for Medical Device Manufacturers, GHTF.SG3.N99-9, Global Harmonization Task Force, 29 June, 1999

[34] Design Control Guidance for Medical Device Manufacturers, Center for Devices and Radiological Health, FDA, 11 March, 1997

[35] ISO 31000, General guidelines for principles and implementation of risk management

[36] ISO 14971:2007, Medical devices — Application of risk management to medical devices

[37] IEC 61508-3:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software Requirements

[38] IEC 61508-5:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 5: Examples of methods for the determination of safety integrity levels

[39] GHTF/SG3/NI5R8, Global Harmonization Task Force Study Group 3, Risk Management Principles and Quality Management Systems, May, 2005
[40] CRAMM, UK Government's Preferred Risk Analysis and Management Method for Information Security Management, January, 2003
[41] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices
[42] Council Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in-vitro diagnostic medical devices
[43] Therapeutic Goods Act 1989 as amended by the Therapeutic Goods Amendment (Medical Devices) Bill 2002 and the Therapeutic Goods (Medical Devices) Regulations 2002 [known as Therapeutic Goods Amendment (Medical Devices) Act 2002]
[44] Australian Medical Devices Guidelines: An Overview of the New Medical Devices Regulatory System, Guidance Document Number 1, Version 1.6, Therapeutic Goods Administration, Department of Health and Ageing, 23 May, 2003
[45] Differences between the Australian and European Union regulatory systems (1), Fundamental differences and classification, Fact Sheet, Draft for comment, Therapeutic Goods Administration, Australian Department of Health and Ageing, December, 2004
[46] Differences between the Australian and European Union regulatory systems (2), Essential principles, Fact Sheet, Draft for comment, Therapeutic Goods Administration, Australian Department of Health and Ageing, April, 2005
[47] Medical Devices Regulations, 1998 of the Food and Drugs Act
[48] Medical Device Compliance and Enforcement Directive, Health Products and Food Branch Inspectorate, Health Canada, 11 February, 2004
[49] Guidance for the Risk-based Classification System, Draft, GD006, Therapeutic Products Directorate, Medical Devices Bureau, Health Canada, 4 May, 1998
[50] Guidance for the Risk-based Classification System of In Vitro Diagnostic Devices, Draft, GD007, Therapeutic Products Directorate, Medical Devices Bureau, Health Canada, 17 March, 1998
[51] Keyword Index To Assist Manufactures In Verifying The Class of Medical Devices, Therapeutic Products Programme, Licensing Services Division, Medical Devices Bureau, Health Canada
[52] Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Human Sciences, 11 May, 2005
[53] Off-The-Shelf Software Use in Medical Devices, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Human Sciences, 9 September, 1999
[54] General Principles of Software Validation; Final Guidance for Industry and FDA staff, Center for Devices and Radiological Health, Food and Drug Administration, US Department of Health and Human Sciences, 11 January, 2002
[55] Principles of Medical Devices Classification, Proposed Document SG1/N015R22, GHTF Study Group 1, the Global Harmonization Task Force, 17 November, 2003
[56] The Classification Rules, Bulletin Number 10, UK Medical Devices Agency (now UK Medicines and Healthcare products Regulatory Agency), February, 1995
[57] Classification of Medical Devices, Guidance Document Number 25, Therapeutic Goods Administration, Australian Department of Health and Ageing, January, 2005
[58] PD 6668, Managing Risk for Corporate Governance, British Standards Institution, November, 2000
[59] AS/NZS 4360:2004, Risk Management, Standards Australia Institute
[60] World Standards Cooperation Healthcare Technology Task Force (HTTF), Final Report, January, 2006
[61] IEC 62304:2004, Medical device software — Software life cycle processes
[62] Australian Medical Devices Guidelines — Conformity Assessment Procedures, Guidance Document Number 3, Version 1.5, Therapeutic Goods Administration, Australia, 23rd May, 2003
[63] Medical Device Compliance and Enforcement Directive, Health Canada, 11th February, 2004
[64] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements
[65] ISO/IEC 17799, Information technology — Security techniques — Code of practice for information security management
[66] ISO/IEC 27005, Information technology — Security techniques — Information security risk management
[67] IEC 60601-1-4, Medical electrical equipment — Part 1—4: General requirements for safety — Collateral Standard: Programmable electrical medical systems
[68] EN 1441, Medical devices — Risk analysis
[69] BS 7799-3, Information security management systems — Guidelines for information security risk management

УДК 61:004:006.354 ОКС 35.240.80 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, безопасность программного обеспечения, безопасность пациентов, вред здоровью

Редактор *Е.А. Моисеева*
Технический редактор *В.Н. Прусакова*
Корректор *Е.И. Рычкова*
Компьютерная верстка *Л.В. Софейчук*

Сдано в набор 23.01.2019. Подписано в печать 30.01.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,19. Уч.-изд. л. 4,65.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

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