ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/ТС 25238— 2009

Информатизация здоровья

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОТ МЕДИЦИНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ISO/TS 25238:2007
Health informatics — Classification of safety risks from health software (IDT)

Издание официальное

БЗ 10—2009/748

Москва
Стандартинформ
2010

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН 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 аутентичного перевода на русский язык стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 сентября 2009 г. № 404-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/ТС 25238:2007 «Информатизация здоровья. Классификация угроз безопасности от медицинского программного обеспечения» (ISO/TS 25238:2007 «Health informatics — Classification of safety risks from health software»)

5 ВВЕДЕН ВПЕРВЫЕ

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

© Стандартинформ, 2010

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

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 1
3 Принципы анализа опасностей и рисков . . . 2
4 Определение класса риска программного продукта для сферы здравоохранения . . . 4
4.1 Введение . . . 4
4.2 Определение категорий последствий . . . 4
4.3 Определение правдоподобия последствий . . . 5
4.4 Классы риска . . . 6
4.5 Определение класса риска программного продукта для сферы здравоохранения . . . 7
4.6 Итерационный процесс . . . 7
5 Аналитический процесс . . . 7
5.1 Введение . . . 7
5.2 Привлечение заинтересованных сторон . . . 7
5.3 Понимание среды системы и пользователя . . . 7
5.4 Анализ последствий . . . 8
5.5 Анализ правдоподобия последствий . . . 8
5.6 Итерации . . . 9
5.7 Пересмотры . . . 9
5.8 Документация . . . 9
5.9 Библиотека инцидентов . . . 9
6 Примеры определения классов риска для программных продуктов . . . 9
7 Взаимосвязь классов риска с проектированием и контролем производства программных продуктов . . . 10
Приложение А (справочное) Программные продукты для сферы здравоохранения и медицинские приборы . . . 11
Приложение В (справочное) Примеры определения классов риска . . . 14
Приложение С (справочное) Иллюстрация сути взаимосвязи между классами риска и потенциальными средствами контроля для управления рисками . . . 18
Библиография . . . 20

Введение

В прошлом программное обеспечение, связанное со здравоохранением, в основном использовалось для реализации некритичных административных функций, представляющих незначительную потенциальную угрозу для пациентов по сравнению с влиянием на работу организации. Медицинские системы в основном были несложными и часто содержали большой объем административных (а не медицинских) данных, предоставляющих слабую поддержку для принятия решений. Даже медицинские системы поддержки принятия решений были относительно простыми, с понятной логикой и использовались в качестве не основного, а, скорее, вспомогательного средства для принятия решений. Но в этой области произошли и продолжают постоянно происходить серьезные изменения, повышающие степень потенциального риска для пациентов.

В связи с применением медицинского программного обеспечения были зарегистрированы серьезные несчастные случаи, например в сфере скрининга и вызовов врачей, когда в результате отказа программного обеспечения врачи не были вызваны к пациентам, находящимся под угрозой. Подобные случаи не только причиняли страдания пациентам, но и приводили к летальному исходу. Существенно было подорвано доверие общественности. Сфера скрининга заболеваний расширяется, вовлекается большое число людей, что требует высокой степени доверия (как с административной, так и с медицинской точки зрения) к программному обеспечению в том, что оно способно выявлять нормальные и ненормальные ситуации, «формировать вызовы» или «осуществлять обработку» в ситуациях, кажущихся потенциально опасными. Такое программное обеспечение должно быть безопасным.

Во всем мире отмечается растущее беспокойство по поводу большого числа предотвратимых клинических несчастных случаев, оказывающих негативное воздействие на пациентов, из которых значительная часть приводит к летальному исходу или недееспособности [1]—[6]. К таким предотвратимым клиническим несчастным случаям относятся, например, неправильный или неполный диагноз или другие неправильно принятые решения. Способствующим этому фактором часто является отсутствие или неполнота информации, а иногда просто незнание, например, медицинских возможностей в сложных случаях или взаимного влияния применяемых лечебных средств.

Все чаще утверждается, что информационные системы, такие как поддержка принятия решений, протоколирование, выдача рекомендаций и руководств, могут существенно снизить негативный эффект. Более частое применение систем поддержки принятия решений и контроля заболеваемости неизбежно способствовало бы их развитию и совершенствованию. Также можно предположить, что под воздействием времени и медико-юридических факторов врачи будут все больше полагаться на такие системы, меньше обращая внимание на их производительность. Действительно, по мере интеграции подобных систем в сферу медицинского обслуживания любая неспособность использовать стандартные средства поддержки может быть осуждена на юридическом основании.

Усиление поддержки принятия решений может ожидаться не только непосредственно при лечении, но и в областях, также важных для обеспечения безопасности пациента, например при принятии решения о направлении к специалисту, когда ошибка в выдаче «правильного» направления или «своевременной» выдаче направления может иметь серьезные последствия.

Экономические факторы также могут привести к росту числа систем поддержки принятия решений, например для общего и/или экономичного назначения лекарств или экономии на количестве и стоимости клинических испытаний.

Системы, подобные системам поддержки принятия решений, имеют значительный потенциал для снижения числа медицинских ошибок и улучшения клинической практики. Например, значительное число опубликованных свидетельств подтверждает снижение ошибок и негативных инцидентов при применении электронных назначений лекарств. Однако все подобные системы потенциально могут также нанести и вред. Причиной вреда может стать слепое и/или непрофессиональное их использование, несмотря на то, что разработчики могут снижать вероятность подобных обстоятельств, например, посредством инструкций (руководств) по применению, обучающих курсов и экранных презентаций. Потенциальный вред может быть скрыт также в конструкции системы в следующих случаях:

- плохая доказательная база для разработки;
- ошибки в проектной логике, не позволяющие правильно реализовывать поставленные цели;
- ошибки в логике при представлении успешного опыта или доказательств на стадии проектирования;
- плохое или запутывающее представление информации или плохие средства поиска информации;

- невозможность обновления информации в соответствии с текущим уровнем знаний.

Некоторые недостатки таких систем проявляются не сразу и могут быть не замечены пользователем.

Следует отметить существенное увеличение финансирования на информационные технологии и управление информацией во многих национальных системах здравоохранения. Связанные с этим графики проведения работ весьма напряженные, а поставленные цели - амбициозные. Можно ожидать, что подобное увеличение финансирования привлечет новых производителей, некоторые из которых могут не знать медицинской специфики. Данные обстоятельства могут привести к образованию среды повышенных рисков для здоровья пациентов.

Бурное развитие информационных и коммуникационных технологий ожидается в телемедицине. Многие программные продукты для сферы здравоохранения, поддерживающие приложения телемедицины, будут инновационными и непроверенными, а отдаление врачей от пациентов увеличит число возможных ошибок, сделав их при этом менее очевидными. Возрастающее применение мобильных инновационных информационных устройств, особенно в новых областях, также, вероятно, будет связано с рисками.

Хотя нам еще далеко до внедрения полностью безбумажных технологий в больницах, врачи общей практики возглавляют движение в этом направлении. Невозможность использования бумаги и пленки повышает степень использования компьютеров и баз данных. Искажение и потеря данных не только приводят к административному хаосу, но могут также существенно повлиять на лечение пациентов.

Угроза потенциального вреда для пациентов при использовании информационных и коммуникационных технологий (ИКТ) в медицине увеличивается по мере роста числа их внедрений, усложнения приложений и повышения доверия к ИКТ. В среде специалистов и общественности растет беспокойство по поводу инцидентов, вызванных сбоями программного обеспечения и приведших к негативным последствиям для здоровья пациентов.

Следовательно, ряд организаций здравоохранения все чаще опирается на стандарты по «обеспечению средств контроля», включая стандарты по «руководству» и «управлению рисками». Важным свойством средств контроля является управление рисками в контексте вреда для пациентов и недостаточном качестве лечения. Средства контроля зачастую охватывают покупку и применение программных продуктов для сферы здравоохранения.

Сбои или недостатки программных продуктов для сферы здравоохранения могут, разумеется, оказывать негативное воздействие не только непосредственным причинением вреда пациентам. Например, они могут создавать административные неудобства или даже административный хаос, влияющие на работу медицинского учреждения, включая возможные финансовые потери. Вред, нанесенный пациенту, также может иметь последствия для медицинского учреждения, например финансовые потери из-за судебного разбирательства. Подобные негативные организационные воздействия могут иметь значение для медицинского учреждения, однако в настоящем стандарте они не учитываются, если только они не приводят к причинению вреда пациенту. Например, сбой в центральной системе учета пациентов больницы, несомненно, вызовет существенные административные неудобства, но такое негативное воздействие лежит вне области применения настоящего стандарта, если оно не может потенциально нанести вред пациенту (что в принципе возможно). Областью применения настоящего стандарта является потенциальный вред для пациента.

Безопасность лекарственных препаратов и медицинских приборов во многих странах обеспечивается множеством юридических и административных мер. Например, в Европейском союзе безопасность является предметом ряда директив ЕС [7]—[9]. Подобные меры зачастую подкрепляются стандартами, связанными с обеспечением безопасности, как национальными, так и международными, включая стандарты Международной организации по стандартизации (ИСО), Международного электротехнического комитета (МЭК) и Европейского комитета по стандартизации (CEN). Программное обеспечение, необходимое для правильного применения или функционирования медицинских приборов, зачастую охватывается данными нормативными документами. Однако другие виды программного обеспечения, используемого в здравоохранении, обычно не регламентируются подобным образом. Настоящий стандарт относится к программному обеспечению, применяемому в медицине, за исключением программного обеспечения, необходимого для правильного применения или функционирования медицинских приборов.

Необходимой предпосылкой для определения и реализации надлежащих средств контроля проектирования и производства в целях минимизации рисков для пациента при сбоях или неправильном

функционировании программного обеспечения является четкое понимание опасности, которую программный продукт может представлять для пациентов в случае сбоя или непредусмотренного события и вероятности данного сбоя или события, наносящего вред пациенту. Кроме того, если производителям программных продуктов для сферы здравоохранения должно быть выдано руководство по контролю проектирования и производства (и по применению разработанных стандартов), то следует учитывать, что средства контроля для программных продуктов, представляющих небольшие риски, будут отличаться от средств контроля для программных продуктов, представляющих большие риски. Средства контроля должны соответствовать уровню риска, который программный продукт может представлять для пациента. С этой целью во многих стандартах, нормативных актах и спецификациях, связанных с контролем рисков при проектировании и производстве, программные продукты группируются в ограниченное число классов или типов в зависимости от степени риска, который они могут представлять.

В настоящем стандарте представлен подход к классификации программных продуктов для сферы здравоохранения. Определены пять классов риска, облегчающих сортировку обобщенных типов и отдельных программных продуктов в зависимости от применяемых средств контроля проектирования и производства в соответствии с уровнем риска. Таким образом, предложенная классификация может стать предпосылкой для разработки стандартов по контролю проектирования и производства. В этих целях может потребоваться более подробный, глубокий и строгий анализ рисков для конкретного программного продукта, нежели тот, который потребовался для процесса общей классификации в настоящем стандарте. Приведены примеры применения процесса назначения класса риска для нескольких разных типов программных продуктов для сферы здравоохранения.

Термин «программные продукты для сферы здравоохранения» относится к любому программному продукту, предназначенному для медицинских целей, независимо от того, представлен ли он на рынке, является ли он коммерческим или свободно распространяемым. Поэтому требования настоящего стандарта распространяются как на коммерческие программные продукты, так и, например, на медицинское программное обеспечение с открытым исходным кодом, а также на программное обеспечение, разработанное только для одного медицинского учреждения или применяемое только в одном медицинском учреждении, например в больнице. Существует широкий диапазон разнообразных программных продуктов для сферы здравоохранения, начиная от простых научно-исследовательских баз данных и до систем обработки вызовов и повторных вызовов, медицинских систем поддержки принятия решений, систем электронного учета здоровья, диспетчерских систем скорой помощи, больничных систем клинических лабораторий и систем для врачей общей практики. В приложении В приведены четыре примера применения настоящего стандарта к разным программным продуктам для сферы здравоохранения. Однако программное обеспечение, необходимое для правильного применения или функционирования медицинских приборов, не относится к области применения настоящего стандарта.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ОТ МЕДИЦИНСКОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Health informatics. Classification of safety risks from health software

Дата введения — 2010—07—01

1 Область применения

Настоящий стандарт относится к сфере обеспечения безопасности пациентов и содержит руководство по анализу и классификации угроз и рисков для пациентов при применении программных продуктов для сферы здравоохранения, обеспечивающее отнесение любого программного продукта к одному из пяти классов риска. Требования настоящего стандарта распространяются на угрозы и риски, которые могут причинить вред пациенту. Другие виды рисков, например финансовые или организационные риски, не относятся к области применения настоящего стандарта, если только они не несут потенциальной угрозы для пациента.

Требования настоящего стандарта распространяются на любой программный продукт для сферы здравоохранения независимо от того, присутствует ли он на рынке программного обеспечения и продается ли он или распространяется бесплатно. Приведены примеры применения классификационной схемы.

Требования настоящего стандарта не распространяются на любое программное обеспечение, необходимое для правильного применения или функционирования медицинских приборов.

Примечание — Настоящий стандарт предназначен для классификации медицинского программного обеспечения в соответствии с общими классами риска в целях принятия решений (например, какие средства контроля следует применить для обеспечения безопасности). Настоящий стандарт не предназначен для применения анализа рисков и управления рисками к проектированию программных продуктов для сферы здравоохранения или для снижения каких-либо идентифицированных рисков до приемлемого уровня (см. приложение А).

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 [10].

2.3 **программный продукт для сферы здравоохранения** (health software product): Программное обеспечение, предназначенное для использования в сфере здравоохранения в целях охраны здоровья, за исключением программного обеспечения, которое необходимо для правильного применения медицинского прибора.

2.4 **производитель** (manufacturer): Физическое или юридическое лицо, отвечающее за разработку, производство, 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.

Издание официальное

Примечание — Заимствовано из [11].

2.5 **пациент** (patient): Любое лицо, к которому применяется или которое использует 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).

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

2.7 **риск** (risk): Комбинация правдоподобия нанесения вреда и серьезности этого вреда (см. раздел 4).

Примечание — Заимствовано из [10].

2.8 **анализ рисков** (risk analysis): Систематическое использование доступной информации для идентификации опасностей и оценки рисков.

2.9 **класс риска** (risk class): Классификация программного продукта для сферы здравоохранения в соответствии с риском, который он может представлять для безопасности пациентов.

2.10 **безопасность** (safety): Независимость от недопустимого риска нанесения вреда [10].

2.11 **допустимый риск** (tolerable risk): Риск, приемлемый в данном контексте с учетом существующей системы ценностей в обществе [12].

3 Принципы анализа опасностей и рисков

Производители программных продуктов для сферы здравоохранения должны точно знать опасности, которые их продукт может представлять для пациента в случае неправильной работы или возникновения непредусмотренного события, а также вероятность конкретной опасности при использовании программного продукта в приемлемых условиях. Подобное знание необходимо для определения требуемых контрольных мероприятий, а также жесткости их применения, чтобы снизить риск для пациентов до допустимого уровня. Такими мероприятиями могут быть, например, встроенные средства самодиагностики, инструкции по применению и предварительное обучение. Степень допустимости риска зависит от обстоятельств и существующих понятий в обществе и регулятивных органах.

Необходимой предпосылкой данного процесса является выполнение анализа опасностей и рисков.

Существуют разнообразные подходы к анализу опасностей и рисков. Все они используют ряд базовых понятий. Существующие стандарты, руководства и публикации имеют тенденцию к концентрации на конкретных областях деятельности (например, электронные системы безопасности, аэронавтика) или на предметных областях (например, финансовые риски, риски относительно собственности, риски безопасности личных данных). В этой связи их следует интерпретировать в контексте программных продуктов для сферы здравоохранения. Настоящий стандарт основан на ряде источников, что обеспечивает его соответствие общепринятым положениям. В разделе «Библиография» приведен список полезных источников информации по данной теме. При рассмотрении данного подхода применительно к программным продуктам для сферы здравоохранения учитывались классификация и контроль медицинских приборов с точки зрения безопасности (см. приложение А).

Ниже приведены основные понятия для целей настоящего стандарта. Данный раздел не предназначен для рассмотрения всех аспектов анализа опасностей и рисков.

Риск для безопасности пациента при использовании программного продукта для сферы здравоохранения зависит от возможных последствий, которые могут иметь место в результате неправильной работы программного продукта или привести к неблагоприятному событию, а также от правдоподобия возникновения таких последствий. Таким образом, понятие риска включает в себя две составляющие — последствие и правдоподобие.

Примечания

1 В [10] риск определен как «комбинация вероятности события и его последствий», тогда как в настоящем стандарте риск определен как «комбинация правдоподобия нанесения вреда и серьезности этого вреда» (см. 2.7). Вероятность возникновения опасности может быть выражена в некоторых областях количественно как вероятность, основанная на ретроспективном или экспериментальном анализе сбоев и статистике инцидентов. Весьма маловероятно, что такой подход может быть применен к безопасности программных продуктов для сферы здраво-

охранения, где статистика и данные отсутствуют и потому требуется качественная оценка. Поскольку вероятность, несомненно, может быть выражена количественно, предпочтительнее использовать термин «правдоподобие», который точнее отражает смысл и поэтому использован в настоящем стандарте.

2 В [14] риск определен как «комбинация вероятности события и его последствия». Данное определение имеет тот же недостаток, отмеченный в примечании 1, в отношении использования термина «вероятность» вместо «правдоподобие». Более того, настоящий стандарт относится только к событиям, которые, возможно, могут нанести вред пациентам, позволяет оценить серьезность этого вреда, и не касается иных событий. Поэтому термин «событие» не используется.

Последствие, т. е. вред, нанесенный пациенту, может принимать разные формы, начиная от незначительного беспокойства и до летального исхода. Последствия могут быть классифицированы по категориям. Такие категории подлежат интерпретации в соответствии с областью применения, в данном случае — применения ИКТ в здравоохранении. Настоящий стандарт определяет 5 категорий «последствий» и области их применения (см. 4.2).

Возможность того, что опасность возникнет при достаточно предсказуемых обстоятельствах, может быть выражена количественно как вероятность, основанная на ретроспективном или экспериментальном анализе сбоев и статистике инцидентов. Весьма маловероятно, что такой подход может быть применен к безопасности программных продуктов для сферы здравоохранения, где статистика и данные отсутствуют и потому требуется качественная оценка. Настоящий стандарт определяет 5 категорий «правдоподобия» и области их применения (см. 4.3).

Как уже отмечалось, риск для безопасности пациента при использовании программного продукта для сферы здравоохранения зависит от последствий, к которым может привести неправильная работа программного продукта, а также от правдоподобия возникновения таких последствий. Уровень рисков может быть представлен матрицей рисков, у которой правдоподобие и последствие являются двумя ее размерностями (в соответствии с таблицей 1).

Таблица 1

Правдоподобие	Последствие				
	наихудшее				наименьшее
Наивысшее	1	2			
	3				
					4
Наименьшее				5	6

Каждая ячейка матрицы представляет уровень риска. Таким образом, в матрице рисков 25 ячеек представляют 25 уровней риска, серьезность которых уменьшается при движении по диагонали от левой верхней ячейки к правой нижней.

Данные уровни риска могут быть сгруппированы в классы следующим образом:

- класс наивысшего риска образует группа ячеек, расположенная в левой верхней части матрицы, такие как 1, 2 и 3;

- класс наименьшего риска образует группа ячеек, расположенная в правой нижней части таблицы, такие как 4, 5 и 6.

Итак, ячейки матрицы рисков могут быть соотнесены с классами риска. При группировании ячеек в класс необходимо учитывать обстоятельства в рамках области применения и значения, определенные для каждой категории последствия и правдоподобия. Целью является снижение сложности посредством идентификации ячеек, соответствующих одинаковой степени риска для пациента, и группирование их в класс на этом основании. Таким образом, незначительное последствие с высоким правдоподобием может быть приравнено к наихудшему последствию, но с меньшим правдоподобием.

В настоящем стандарте определены пять классов риска (см. 4.4).

4 Определение класса риска программного продукта для сферы здравоохранения

4.1 Введение

В данном разделе определены категории последствий, являющихся результатом опасностей, и категории правдоподобия реализации данных последствий в контексте программных продуктов для сферы здравоохранения. В нем также определены классы риска для программных продуктов для сферы здравоохранения и связь данных классов с предложенными категориями последствий и их правдоподобия посредством матрицы рисков. В приложении В показано применение данных определений к разным типам программных продуктов для сферы здравоохранения.

4.2 Определение категорий последствий

Опасности (потенциальные возможности нанесения вреда), которые программный продукт для сферы здравоохранения может представлять для пациента в случае неправильной работы или вызванного им неблагоприятного события, должны быть определены. Кроме того, должны быть идентифицированы потенциальные последствия данных опасностей. Каждое последствие должно быть отнесено к одной из следующих категорий:

- катастрофические;
- серьезные;
- значительные;
- существенные;
- незначительные.

Примечание — Нет необходимости идентифицировать и классифицировать все возможные последствия. Анализ в целях идентификации реалистичных последствий и возможностей их возникновения должен быть выполнен только в той степени, которая требуется для уверенного отнесения продукта к классу риска посредством итерационного процесса, описанного в 4.6.

Категории последствий должны интерпретироваться в соответствии с таблицей 2. Описания категорий последствий были разработаны для целей настоящего стандарта, но согласованными с принятыми в других областях и дополнительных дисциплинах и подходах (см. [15]—[17]).

В случае, когда имеется сомнение, к которой из двух категорий следует отнести последствие, оно должно быть отнесено к категории, соответствующей более тяжелым последствиям.

При определении опасностей, которые программный продукт или тип продуктов для сферы здравоохранения может представлять для пациента, не следует отвергать опасность только из-за уверенности, что сам программный продукт или заложенные в нем свойства таковы, что не существует обстоятельств, при которых опасность может возникнуть. Потенциальная возможность нанесения вреда (опасности) пациенту при использовании программного продукта должна быть определена, как если бы таких свойств у продукта не было или они реализовывались бы неправильно.

Таблица 2

Категории последствий	Интерпретация	
	Последствие	Количество случаев
Катастрофические	Летальный исход	Множество
	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
Серьезные	Летальный исход	Единичные
	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	Единичные

Категории последствий	Интерпретация	
	Последствие	Количество случаев
	Серьезная травма или недееспособность, восстановление после которой ожидается в ближайшее время	Множество
	Серьезная психологическая травма	Множество
Значительные	Серьезная травма или недееспособность, восстановление после которой ожидается в ближайшее время	Единичные
	Серьезная психологическая травма	Единичные
	Незначительная травма или травмы, восстановление после которых не ожидается в ближайшее время	Множество
	Существенная психологическая травма	Множество
Существенные	Незначительная травма или травмы, восстановление после которых не ожидается в ближайшее время	Единичные
	Существенная психологическая травма	Единичные
	Незначительная травма, восстановление после которой ожидается в ближайшее время	Множество
	Незначительное психологическое расстройство; беспокойство	Множество
Незначительные	Незначительная травма, восстановление после которой ожидается в ближайшее время; незначительное психологическое расстройство; беспокойство; любые несущественные последствия	Единичные

При определении опасностей, которые программный продукт для сферы здравоохранения может представлять для пациента в случае, если он неправильно функционировал или вызвал непредвиденное событие, не следует отвергать опасность только потому, что даже в случае ее возникновения пациент бы не пострадал, например благодаря бдительности пользователя или других событий, внешних по отношению к программному продукту. Данный фактор соответствует определению возможности возникновения опасности, представленному в 4.3 и 5.5.

4.3 Определение правдоподобия последствий

Для каждого из идентифицированных последствий должно быть определено правдоподобие возникновения последствия в достаточно предсказуемых обстоятельствах.

Примечание — Как указано в 4.2, нет необходимости идентифицировать все возможные последствия. Анализ возможных последствий и определение правдоподобия их возникновения следует выполнять только в той степени, которая необходима для уверенного отнесения программного продукта к классу риска посредством итерационного процесса, описанного в 4.6.

Правдоподобие последствия должно быть отнесено к одной из следующих категорий:

- очень высокое;
- высокое;
- среднее;
- низкое;
- очень низкое.

Категории правдоподобия должны интерпретироваться в соответствии с таблицей 3. Описания категорий правдоподобия были разработаны для целей настоящего стандарта, однако они соответствуют категориям в других областях, например в области корпоративного управления в здравоохранении (см. [18]).

В случае, когда имеется сомнение, к которой из двух категорий следует отнести правдоподобие последствия, оно должно быть отнесено к категории, соответствующей более высокому правдоподобию (см. таблицу 3).

При оценке правдоподобие последствия не должно преуменьшаться из-за каких-либо характеристик самого продукта, включая относящиеся к нему инструкции по применению (см. определение продукта в 2.6). В контексте данного подраздела термин «правдоподобие» не имеет отношения к вероятности неправильного функционирования программного продукта или к неблагоприятному событию. Именно правдоподобие последствий в результате неправильного функционирования или неблагоприятного негативного события обычно оценивается на практике.

Таблица 3

Категории правдоподобия	Описание
Очень высокое	Обязательно или почти обязательно; очень вероятно, что событие произойдет
Высокое	Не обязательно, но весьма возможно; ожидается, что событие произойдет в большинстве случаев
Среднее	Возможно; есть вероятность, что событие произойдет
Низкое	Событие может произойти, но в большинстве случаев не произойдет
Очень низкое	Незначительная или практически незначительная вероятность события

Однако допустимо учитывать достаточно предсказуемые обстоятельства, внешние по отношению к программному продукту. Например, если идентифицированным последствием опасного события является травма, то при оценке правдоподобия данного события, приведшего к реальной травме пациента, могут учитываться, например, следующие факторы:

- возможность того, что опасное событие будет замечено пользователем с соответствующим уровнем квалификации до того, как последствие произойдет;
- возможность того, что последствия удастся избежать, поскольку число опасных событий в течение некоторого периода времени до возникновения последствия может увеличить возможность выявления опасности;
- возможность того, что пациента осмотрит врач до того, как ему будет нанесен какой-либо вред, причем времени будет достаточно для проведения эффективного лечения или терапии.

Обстоятельства, которые могут быть учтены при определении правдоподобия, должны соответствовать серьезности рассматриваемого последствия, а строгость критериев напрямую зависит от серьезности последствия.

Не допускается предполагать наличие наилучших обстоятельств во всех случаях. Например, не допускается предполагать, что оператор всегда имеет достаточную квалификацию и/или опыт, поскольку логично предположить, что возможны обстоятельства, при которых программный продукт используется оператором впервые, и что операторы, даже прошедшие обучение, могут иметь недостаточную квалификацию. Учет таких обстоятельств как возможных, очевидно, важен, когда возможное последствие весьма серьезно, например летальный исход.

4.4 Классы риска

Настоящий стандарт базируется на концепции классов риска, каждый из которых представляет комбинацию категорий последствий и категорий правдоподобия. Предложены пять классов риска, обозначенные от A до E.

Каждый класс представляет группировку комбинаций последствий и их правдоподобия, которые в общем случае представляют одинаковый уровень риска для безопасности пациентов. Класс A представляет наибольший потенциальный риск, а класс E — наименьший.

Комбинации, соответствующие классам риска, приведены в таблице 4.

Примечание — Решение о том, какие ячейки таблицы группируются вместе, образуя класс, принимается на основании рассмотрения определений каждой категории последствий и правдоподобия. Поэтому достоверность таблицы 4 зависит от опыта ее применения в разных областях, относящихся к информатизации здоровья, и от использования классов при определении средств контроля, применимых к продуктам из разных классов для обеспечения их безопасности. Данный опыт важен при возможных последующих корректировках настоящего стандарта.

Таблица 4

Правдоподобие	Последствия				
	катастрофические	серьезные	значительные	существенные	незначительные
Очень высокое	A	A	B	B	C
Высокое	A	B	B	C	C
Среднее	B	B	C	D	D
Низкое	B	C	D	D	E
Очень низкое	C	C	D	E	E

4.5 Определение класса риска программного продукта для сферы здравоохранения

Комбинации последствий и их правдоподобия должны быть размещены в матрице рисков, описанной в 4.4 (см. таблицу 4), с использованием итерационного процесса, описанного в 4.6. Программному продукту для сферы здравоохранения присваивается наивысший из идентифицированных для него классов риска, при этом класс A соответствует наибольшему риску, а класс E — наименьшему.

4.6 Итерационный процесс

Класс риска, к которому относится продукт, зависит от комбинации категории последствий и категории правдоподобия. Таким образом, высокая категория последствий в сочетании с низким правдоподобием может быть отнесена к более низкому классу риска, чем более низкая категория последствий, но в сочетании с более высоким правдоподобием. Хотя любой анализ наиболее вероятно будет изначально сфокусирован на реальных наихудших последствиях, также будет необходимо рассмотреть и менее серьезные последствия до тех пор, пока в ходе итераций не будет обеспечена уверенность, что продукту в конце концов присвоен наивысший из выявленных классов риска.

5 Аналитический процесс

5.1 Введение

В данном разделе представлены некоторые из процессов, которые должны быть рассмотрены при анализе в целях определения класса риска.

5.2 Привлечение заинтересованных сторон

Любой анализ должен быть основан на четком и уместном глубинном понимании системы, среды, в которой система будет использоваться, и пользователей, для которых система предназначена. Следует заручиться согласием и решениями со стороны представителей заинтересованных в программном продукте для сферы здравоохранения сторон. Наилучшим способом добиться этого является создание группы, по крайней мере, из следующих участников:

- специалисты, участвующие в проектировании, разработке и эксплуатации систем;
- пользователи;
- лица, вовлеченные в деловую или технологическую среду, в которой система будет использоваться.

Также может быть полезным включение в данную группу представителей юристов и экспертов по управлению.

Что касается продуктов, которые должны распространяться на коммерческой основе, необходимо исключить влияние коммерческих интересов на результаты анализа.

5.3 Понимание среды системы и пользователя

Первым шагом в работе сформированной группы является достижение общего понимания по следующим вопросам:

- назначение системы;
- среда, в которой предполагается использовать систему (к факторам окружающей среды, подлежащим рассмотрению, относятся не только физические факторы, но и, например, степень привлечения медицинских экспертных знаний);

- характеристики и режимы работы системы;
- человеко-машинный интерфейс;
- динамика процессов, с которыми система будет взаимодействовать и на которые она будет влиять.

Достигнутое общее понимание должно быть документально оформлено, включая любые рассмотренные и признанные нереальными сценарии.

5.4 Анализ последствий

При определении последствий, если система будет неправильно работать или приведет к неблагоприятному событию, группа должна выполнить следующее:

- обеспечить, чтобы данный процесс направлялся деловыми, профессиональными или пользовательскими интересами в противоположность, например, коммерческим интересам;
- игнорировать встроенные средства контроля и характеристики безопасности системы;
- выявить неблагоприятные события, которые могут произойти в случае, если система неправильно функционировала, вызвала непредусмотренное событие или использовалась ненадлежащим образом, включая:
  - человеческий фактор (случайные или умышленные действия или бездействия);
  - физические сбои;
  - логические сбои;
  - коммуникационные сбои;
  - сбои аппаратных средств;
  - сбои программного обеспечения;
- обратить особое внимание на сценарии, считающиеся «допустимыми наихудшими случаями»;
- собирать информацию о реальных инцидентах, связанных с системой, и делать из этого выводы;
- собирать информацию о реальных инцидентах, связанных с аналогичными программными продуктами, и делать выводы на основе чужого опыта, включая случаи, описанные в соответствующих публикациях;
- обеспечивать привлечение всех заинтересованных сторон;
- поощрять инновационное мышление;
- выявлять любое скрытое или возможное воздействие, не только приводящее к немедленным последствиям;
- быть творческой, оставаясь реалистичной;
- полностью учитывать точки зрения пользователей и лиц, представляющих медицинскую среду, для использования в которой предназначена система.

5.5 Анализ правдоподобия последствий

При оценке правдоподобия последствия, происходящего в достаточно предсказуемых обстоятельствах, группа должна выполнить следующее:

- изучить перечень неблагоприятных событий, которые могут произойти при неправильном функционировании программного продукта и т. п., использованный при определении категорий последствий;
- сфокусироваться в первую очередь на наихудших неблагоприятных событиях и последствиях;
- проанализировать процессы, которые могут привести к нанесению вреда пациенту в результате неблагоприятных событий, и ограничения, сопутствующие данным процессам;
- рассмотреть прошлые инциденты, которые привели к нанесению вреда, включая случаи, описанные в литературе;
- рассмотреть все возможные изменения и тенденции в достаточно предсказуемой перспективе в области применения продукта;
- принимать во внимание при рассмотрении человеческого фактора следующие обстоятельства:
  - мотивацию;
  - рабочие нагрузки и возможности;
  - компетентность;

- стимулы и препятствия;
- рабочую среду;
- выявить обстоятельства, которые могут повысить правдоподобие последствия;
- избегать необоснованной уверенности в квалификации медицинского работника или пользователя, достаточной, чтобы избежать последствий;
- принимать во внимание сложность решений или процессов;
- принимать во внимание обоснованные предположения о доступности человеческих и иных ресурсов, и особенно влияние их нехватки;
- принимать во внимание взаимозависимость событий в цепочке;
- принимать во внимание временную задержку между неблагоприятным событием, вызванным системой, и любым последствием, которое может произойти;
- принимать во внимание объем предпринимаемых действий и степень удаленности любых последствий от операторов. Например, система «вызовов и повторных вызовов» для скрининга груди может обрабатывать многие тысячи пациентов, выдвигая на первый план статистическое правдоподобие последствия в случае, если неправильная работа системы повлияла на большое число пациентов, расположенных на удаленном расстоянии от лиц, работающих с системой и имеющих мало средств или не имеющих их вообще для того, чтобы распознать, что неблагоприятное событие имело место.

5.6 Итерации

Как было отмечено в 4.6, класс риска, к которому относится продукт, зависит от комбинации категории последствий и категории правдоподобия. Высокая категория последствий в комбинации с низким правдоподобием будет отнесена к более низкому классу риска, чем более низкая категория последствий, но с большим правдоподобием. Таким образом, хотя любой анализ наиболее вероятно будет изначально сфокусирован на наихудших последствиях, также будет необходимо рассмотреть менее серьезные последствия и их правдоподобие. Однако не все последствия и их правдоподобие следует рассматривать в ходе процесса итераций. Итерационный процесс должен продолжаться только до тех пор, пока не будет достигнута уверенность в правильном определении класса риска, т. е. когда не останется других комбинаций последствия и его правдоподобия, соответствующих более высокому классу риска.

5.7 Пересмотры

Изменения в программном продукте или в области его применения будут происходить время от времени, например в следующих случаях:

- при введении новых или изменении существующих функций;
- при продвижении в новую среду (например, выведение исследовательской системы на широкий рынок, выход на рынок сбыта в новой стране, переориентация на другую медицинскую специализацию, среду здравоохранения или тип медицинского учреждения);
- при введении новых или изменении существующих интерфейсов с другими системами.

Изменения в программном продукте или в области его применения могут привести к изменению класса риска, к которому должен быть отнесен продукт. Поэтому должны проводиться соответствующие пересмотры как периодически, так и при внесении или планировании любых изменений, которые могут повлиять на класс риска программного продукта.

5.8 Документация

Аналитический процесс должен быть полностью документирован, включая:

- рассмотренные ситуации неправильной работы и неблагоприятных событий, а также их последствия, включая и те, которые были отклонены как нереальные;
- анализ правдоподобия последствий, включая сценарии, отклоненные как нереальные;
- итерационный процесс и логика, которые привели к уверенному определению класса риска.

Данная документация должна рассматриваться как основная документация по системе, постоянная доступность и актуальность которой должны быть обеспечены.

5.9 Библиотека инцидентов

Решения по обоснованным последствиям и возможностям их возникновения должны быть в значительной степени подкреплены ссылками на библиотеку инцидентов. Поэтому должны быть предусмотрены средства для сбора и хранения информации об инцидентах.

6 Примеры определения классов риска для программных продуктов

Примеры определения класса риска для разных типов программных продуктов для сферы здравоохранения приведены в приложении В.

7 Взаимосвязь классов риска с проектированием и контролем производства программных продуктов

Важным применением настоящего стандарта является определение классов риска для разных типов программных продуктов для сферы здравоохранения, для того чтобы сгруппировать их в целях создания руководства (стандарта) по проектированию и производству данных продуктов. Сущность таких средств контроля и строгость, с которой надлежит применять их, будут зависеть от класса риска, к которому относится продукт. Хотя целью настоящего стандарта не является определение того, какие средства контроля следует использовать для определенных классов риска, в приложении С приведена иллюстрация сущности взаимосвязи между классами риска и возможными средствами контроля для управления рисками.

Приложение А
(справочное)

Программные продукты для сферы здравоохранения и медицинские приборы

А.1 Общие сведения

Во многих странах безопасность медицинских приборов обеспечивается законодательными мерами. Контроль различных видов программного обеспечения отличается в деталях, но в целом применяется в целях определения правильности применения медицинского прибора.

На практике, по крайней мере в настоящее время, программные продукты для сферы здравоохранения (см. 2.3) не охватываются данными средствами контроля. Примерами являются системы врачей общей практики, вызова и повторного вызова, исследовательские базы данных, программное обеспечение для электронных предписаний, диспетчерские системы скорой помощи и т. д.

При рассмотрении классификации программных продуктов для сферы здравоохранения имеет смысл оценить подход, принятый для медицинских приборов, и в рамках данного подхода взаимосвязь между классификациями и средствами контроля для обеспечения безопасности, чтобы, насколько это возможно, подходы были сходными. Данный вопрос рассмотрен в настоящем приложении. В целях краткости не приведен углубленный анализ, а ряд сложных проблем и вопросов, связанных с определениями, были упрощены.

Подход, относящийся к медицинским приборам, основан на следующем:

- во-первых, позволяет классифицировать приборы по классам на основе осознанного потенциального риска для пациентов (обычно по четырем классам с подклассами);

- во-вторых, позволяет применять средства контроля в отношении проектирования, производства, систем качества, маркировки и т. д., причем охват средствами контроля и строгость их применения зависят от класса: чем выше класс риска, тем более жесткие средства контроля.

В данном сценарии вопрос риска поднимается в двух очень разных контекстах — в контексте классификации и в контексте средств контроля систем качества.

Система классификации основана на осознанном потенциальном риске для пациентов. Однако для медицинских приборов определение класса риска не требует анализа риска как такового. Классификация существенно зависит от применений прибора, например является ли он инвазивным, неинвазивным, активным, контактирует ли с кожей или нет, передает ли энергию телу и т. д. Классификация основывается на предположении, что, с некоторыми исключениями, инвазивные приборы представляют больший потенциальный риск, чем неинвазивные приборы. Программные продукты для сферы здравоохранения не могут быть охарактеризованы такими терминами, как «инвазивный» или «активный», или что они контактируют с кожей. Таким образом, системы классификации, используемые для медицинских приборов, не могут быть применены к программным продуктам для сферы здравоохранения.

Напротив, обычным контрольным мероприятием является требование наличия у производителя удовлетворяющей техническим требованиям системы качества. Частью данного требования может быть требование управления рисками и проведения полной и углубленной оценки рисков при использовании прибора, а также снижения рисков до приемлемого уровня.

Настоящий стандарт касается рисков только в контексте системы классификации программных продуктов для сферы здравоохранения и, являясь таковым, рассматривает потенциальный риск для пациентов при использовании программных продуктов в общем смысле. В настоящем стандарте не рассматриваются контрольные мероприятия по обеспечению безопасности программных продуктов для сферы здравоохранения. Однако в нем учитывается, что, если контрольные мероприятия должны быть внедрены, то предварительно следует классифицировать программные продукты для сферы здравоохранения, чтобы обеспечить для безопасности пациентов соответствие средств контроля риску. Средства контроля могут, разумеется, включать требование к системе управления качеством, а в его рамках — требование применения процесса полной оценки рисков для программного продукта и снижения рисков до приемлемого уровня. Однако анализ рисков в данном контексте не является предметом настоящего стандарта.

Имеет смысл исследовать, могут ли системы классификации, применяемые в контексте медицинских приборов, применяться к программным продуктам для сферы здравоохранения. По причинам, указанным в данном приложении, можно сделать вывод о том, что их применить нельзя. Отсюда вытекает актуальность настоящего стандарта.

А.2 Руководство FDA по программному обеспечению

В США Управление по контролю за продуктами питания и лекарствами (FDA) разработало руководство по программному обеспечению, охватываемому средствами контроля для медицинских приборов. Оно содержит материалы, имеющие значение для настоящего стандарта.

В [20] представлена классификация такого программного обеспечения исходя из уровня его значимости для безопасности пациентов или операторов. Суть и объем документации, необходимой для предпродажного представления, затем сопоставляются с уровнем значимости. Уровень значимости определяется оценкой серьезности травмы, которую прибор может нанести или причинить, напрямую или косвенно, пациенту или оператору в результате сбоев в работе прибора, конструктивных недоработок или просто при применении прибора не по назначению. В данном руководстве определены три следующих 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», т. е. прибор, содержащий программное обеспечение, должен оцениваться без учета принятых мер по снижению опасности. В настоящем стандарте установлено аналогичное требование (см. 4.2 и 4.3).

Руководство Центра по приборам и радиологической безопасности (CDRH) FDA по использованию присутствующего на рынке программного обеспечения в медицинских приборах [21] содержит следующее положение.

«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 [22]. Основываясь на определениях анализа рисков из [11] и [23], 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».

В данном руководстве [21] также предложена классификация, основанная на «уровне значимости», по существу, с аналогичными определениями.

Необходимо отметить, что в руководстве по программному обеспечению для медицинских целей четко заявлено, что руководство по «уровню значимости» применимо только к предпродажным оценкам и «не относится к классификации приборов (по классам I, II или III) или непосредственно к анализу опасностей или рисков». Тем не менее возникает вопрос о том, может ли данная классификация быть применима к программным продуктам для сферы здравоохранения, т. е. использована в настоящем стандарте.

Подобно руководству FDA [20], настоящий стандарт признает, что проблемой для программного обеспечения является систематическая ошибка и что риск не может определяться на основе частоты сбоев программного обеспечения. По существу, если ошибка заложена в программу, то она обязательно проявится, то есть вероятность сбоя программы составляет 100 %. Таким образом, для программного обеспечения анализ рисков сводится к анализу опасностей, т. е. к идентификации сути и серьезности потенциального вреда при проявлении систематической ошибки. Настоящий стандарт классифицирует суть и серьезность потенциального вреда по пяти категориям последствий (в отличие от трех категорий, установленных FDA) в целях более детального разграничения, которое не затрагивает операторов. Кроме того, в настоящем стандарте дано более полное определение последствий, например проводится различие между вредом для одного пациента и вредом для многочисленных пациентов, осо-

бо выделено нанесение психологической травмы. Последнее обстоятельство, например, может быть достаточно существенным при неправильной работе системы обеспечения безопасности базы данных по исследованиям ВИЧ-инфицированных пациентов с их идентификацией. Тем не менее, термины, используемые в настоящем стандарте, аналогичны тем, которые использованы в руководстве FDA [20].

Однако в руководстве FDA не рассмотрен вопрос о том, будет ли вред действительно нанесен в достаточно предсказуемых обстоятельствах, если произойдет неблагоприятное событие, которое потенциально может нанести данный вред. Например, в случае неправильной работы системы программного обеспечения, предназначенной для отправки пациентам напоминаний о посещениях врача, назначенных им в поликлинике, можно сказать, что вред пациенту может быть нанесен в результате пропущенного посещения врача. Тем не менее, вероятность реализации такого вреда на практике имеет отдаленную причинную связь, поскольку пациент, знающий о назначенном посещении, предпримет необходимое действие, когда поймет, что посещение врача было пропущено или пропущенное посещение будет замечено в поликлинике и будет предпринято действие по назначению следующего посещения врача. С другой стороны, если неправильная работа системы вызовов и повторных вызовов приведет к тому, что пациент не получит уведомление о неблагоприятных результатах анализа, то пациенту не только может быть нанесен вред, но и вероятность реально нанесенного вреда может быть высокой, то есть пациент не будет знать о необходимости повторного анализа, а система не распознает, что пациент не был вызван. Целесообразно различать подобные случаи при определении класса риска.

Таким образом, настоящий стандарт устанавливает возможность реального нанесения вреда в предсказуемых обстоятельствах, если произошло неблагоприятное событие, которое потенциально могло нанести данный вред.

Важно понимать, что хотя матрица 5 × 5, определяющая пять классов риска (см. 4.4 и таблицу 4), и выглядит, как классическая матрица рисков, которая может быть получена, например, в результате анализа рисков для медицинского прибора в системе управления качеством (например, как в [11]), ее ось «правдоподобие» имеет фундаментальное отличие. Ось «правдоподобие» в настоящем стандарте не определяет качественную вероятность возникновения неблагоприятного события в программном продукте для сферы здравоохранения. Она определяет правдоподобие того, что последствия данного неблагоприятного события будут действительно иметь место, если данное неблагоприятное событие произошло. Оценка данного фактора особенно важна при возможных последующих пересмотрах настоящего стандарта.

Приложение В
(справочное)

Примеры определения классов риска

В.1 Введение

Данное приложение только иллюстрирует процесс определения классов риска для разных программных продуктов для сферы здравоохранения. В нем содержатся лишь примеры, поэтому его не следует использовать в качестве безусловного руководства по определению классов риска для таких продуктов.

В.2 Больничная система электронных предписаний с поддержкой принятия решений

При определении класса риска для больничных систем электронных предписаний с поддержкой принятия решений в первую очередь следует рассмотреть, какие последствия могут произойти в случае сбоя или неправильной работы системы или какие причины могут привести к непредусмотренному событию.

Непредусмотренным событием может быть назначение лекарства не тому человеку, не того лекарства, не той дозировки, а также, если указаны неверные периодичность, способ, время приема или применения, не предусмотрены взаимодействие лекарств, аллергическая реакция на лекарство.

Приведенные непредусмотренные события могли быть вызваны ошибкой в размещении десятичной запятой в выписанной дозе лекарства или назначением лекарства, вид или количество которого не годится для конкретного типа пациента, например для ребенка. Хотя многие из таких событий могут быть результатом неправильной работы системы, но более вероятно, что они произойдут из-за непреднамеренного ввода пользователем неверной информации по незнанию или при потере концентрации внимания. Подобные неблагоприятные события, однако, не могут быть просто списаны на ошибки пользователя, поскольку проектные решения подобных систем должны предусматривать выдачу соответствующих предупреждений при данных обстоятельствах. Возможность выдачи подобных потенциально опасных предписаний может, таким образом, быть вызвана как ошибкой или неадекватной реакцией системы поддержки принятия решений, так и просто ошибкой пользователя.

Разработчику недопустимо пренебрегать возможностью возникновения неблагоприятных событий, опираясь на убеждение, что его продукт так хорошо разработан, что подобные события не могут произойти. В недавнем исследовании [19] использовались 18 потенциально опасных сценариев для тестирования четырех хорошо обоснованных систем для врачей общей практики, применяемых 75 % врачей общей практики в Великобритании. Системы были разработаны для выдачи предупреждений о взаимодействии лекарств. Однако ни одна из программ не выдала предупреждения для всех 18 сценариев: лучшая из них выдала семь предупреждений, а худшая — четыре. В случае назначения лекарств со сходными названиями ни одна из систем не выдала предупреждения для всех десяти тестовых пар лекарств. Производители всех систем, возможно, были уверены в том, что в их системах учтены все опасные обстоятельства, но оказалось, что это не так.

Следующим шагом является определение правдоподобия последствий неблагоприятных событий. В данном примере легко представить обстоятельства, при которых, в случае выдачи ошибочного назначения, последствия будут иметь форму летального исхода или недееспособности в течение длительного времени. Данные последствия относятся к категории «серьезных».

Следующим шагом является оценка правдоподобия возникновения последствий в форме летального исхода или недееспособности в «достаточно предсказуемых обстоятельствах». Подобные «достаточно предсказуемые обстоятельства» подразумевают рассмотрение цепочки событий, включающей передачу потенциально опасного предписания от дежурного врача к фармацевту, затем к ответственному за отпуск лекарств и, наконец, прием лекарства пациентом, после чего возникает реальное последствие. Поэтому оценка правдоподобия возникновения летального исхода или недееспособности включает разумную оценку того, будет ли ошибка в предписании замечена и скорректирована на какой-либо из стадий рассмотренной цепочки событий, а также того, можно ли, даже в случае приема пациентом выписанного лекарства, избежать летального исхода или недееспособности. Не допускается предполагать наличие наилучших или совершенных условий где-либо в данной цепочке событий. Например, нельзя предполагать, что все участники цепочки событий являются опытными высококвалифицированными врачами. С другой стороны, правдоподобие того, что в цепочке будут задействованы только полностью некомпетентные лица, может быть нереальным предположением. Однако именно требование того, что фактор, который при определении возможности может быть принят приемлемым, должен согласовываться с серьезностью рассматриваемого последствия, определяет, что критерий будет тем строже, чем серьезнее последствие. В данном примере возможное последствие является исключительно серьезным.

Из опыта известно, что при выдаче потенциально опасного предписания оно может привести и приводит к приему выписанного, результатом чего является летальный исход или недееспособность. Присвоенная категория правдоподобия, таким образом, определяется как «очень высокое» или «высокое». В соответствии с матрицей рисков комбинация «серьезной» категории последствия и «очень высокой» категории правдоподобия определяет принадлежность системы электронных предписаний с поддержкой принятия решений к классу А. Однако комбинация

«серьезной» категории последствий и «высокой» категории правдоподобия определяет принадлежность к классу В. Решение об определении принадлежности к классу принимается в соответствии с требованием, что, «если имеется сомнение, к которой из двух категорий следует отнести правдоподобие последствия, оно должно быть отнесено к категории, соответствующей более высокому правдоподобию». Следовательно, данная система должна быть отнесена к классу А.

Проведения дальнейшего анализа (итераций) не требуется, поскольку анализ необходимо проводить «только до тех пор, пока в ходе итераций не будет обеспечена уверенность, что продукту присвоен наивысший из выявленных классов риска», а класса риска «выше», чем класс А, не существует.

Присвоение класса А системам электронных предписаний с поддержкой принятия решений оправданно, поскольку легко понять, что в случае плохой проработки подобных систем они могут нанести серьезный вред пациентам. Любые руководства, стандарты или нормативные документы, относящиеся к средствам контроля, применяемые при проектировании и производстве программных продуктов для сферы здравоохранения, должны быть наиболее строгими в отношении программных продуктов данного типа (относящихся к классу А) из-за их потенциальной возможности нанести серьезный вред, если на них не будет обращено особое внимание.

В.3 Система отслеживания истории болезни по штрих-коду

В данном примере рассмотрена система, производящая наклейку со штрих-кодом, который однозначно идентифицирует папку с историей болезни пациента, с тем чтобы при передаче истории болезни между отделениями больницы ее можно было отслеживать на входе и выходе из отделения посредством устройства считывания штрих-кода, чтобы идентифицировать ее текущее местоположение.

В первую очередь следует рассмотреть, какие последствия могут иметь место в случае, если система будет неправильно работать или вызовет непредвиденное событие.

Одним из случаев неправильной работы системы может быть невозможность прослеживать некоторое множество историй болезни, что приведет к невозможности определения их местоположения и недоступности для врача, когда они понадобятся. Последствие данного обстоятельства будет зависеть от клинической ситуации, имеющей место в тот момент, когда история болезни не может быть найдена.

Даже с учетом того, что врач средней квалификации может проявить осторожность и не предпримет действий до получения достаточной информации, подтвержденной каким-либо образом, последствия серьезной или значительной категории все равно могут иметь место, но правдоподобие их возникновения будет «очень низким». Это указывает на класс С.

Кому-то такое решение может показаться излишне строгим, поскольку на практике подобные последствия скорее будут относиться к категории существенных или незначительных последствий со средним или низким правдоподобием. Это бы указало на класс D или Е.

Потребуется дальнейший анализ, включая, возможно, исследование опубликованных источников, чтобы окончательно определиться с классом (С, D или Е), что представляется вполне обоснованным. Любые руководства, стандарты или нормативные документы, относящиеся к средствам контроля, применяемым при проектировании и производстве программных продуктов для сферы здравоохранения, относящихся к классам С, D или Е, вряд ли будут предъявлять к ним такие же серьезные требования, как к системе электронных предписаний с поддержкой принятия решений (относящейся к классу А).

В.4 Исследовательская система для болезней, передаваемых половым путем

В данном примере представлена система собственной разработки, предназначенная для хранения и анализа данных по заболеваниям, передаваемым половым путем. В системе хранятся личные данные пациентов.

В первую очередь следует рассмотреть, что может произойти в случае сбоя или неправильной работы системы.

Данная система не используется для непосредственного лечения пациентов, и потому для нее не рассматриваются события, вызывающие такие последствия, как смерть, серьезные или незначительные травмы. Однако проблемы с должной защитой конфиденциальных данных о пациенте могут иметь место, например, при недостаточном или отсутствующем контроле доступа либо недостаточно строгих требованиях к паролю. Таким образом, отождествление пациента с болезнью, передаваемой половым путем, например ВИЧ, может быть осуществлено неавторизованным лицом или лицами. Из-за психологической травмы, нанесенной в связи с этим пациенту, данное последствие будет относиться к категории «существенных».

Следующим шагом является рассмотрение правдоподобия реально возникающих последствий. Психологическая травма у пациента не возникнет, если пациент не узнает о том, что конфиденциальность информации о нем была нарушена. Это зависит от обстоятельств несанкционированного доступа. Если несанкционированный доступ был осуществлен врачом, который непреднамеренно просмотрел конфиденциальную информацию, то такой врач вряд ли будет передавать кому-либо данную информацию в силу своего долга сохранять врачебную тайну. Однако случайный или несанкционированный доступ к информации со стороны лица, не связанного врачебными обязательствами, может привести к бездумному или умышленному разглашению информации, особенно если данный пациент известен в местном сообществе. Тем не менее до момента, когда пациент узнает о данном инциденте, пройдет длинная цепочка событий, поэтому правдоподобие может быть оценено от среднего до низкого. В любом случае данная система относится к классу D.

Дополнительное рассмотрение следует произвести, если в системе ведется журнал регистрации событий, в котором был отмечен факт несанкционированного доступа. «Владелец» системы в подобных обстоятельствах может быть обязан уведомить пациента о том, что утечка информации имела место. Это означает, что правдоподобие последствия становится «очень высоким». Однако здраво предположить, что психологическая травма, наносимая пациенту, может быть уменьшена, если его информирует и консультирует опытный врач. Психологическая травма, таким образом, может быть оценена как «незначительная» вместо «существенная». В результате система может быть отнесена к классу С.

В соответствии с приведенными аргументами система может быть отнесена к классу С или D. Если имеются существенные сомнения, к какому классу отнести систему, то система должна быть отнесена к более высокому классу, т. е. к классу С.

Примечание — В отношении исследовательской системы, содержащей менее деликатные данные о здоровье, наихудшим последствием, которого можно ожидать, является незначительное психологическое расстройство (если таковое вообще будет иметь место) с низким или очень низким правдоподобием, т. е. такая система относится к классу Е.

Неудивительно, что система, хранящая персональные данные о здоровье весьма деликатного характера, например данные о болезнях, передаваемых половым путем, должна быть отнесена к относительно «высокому» классу. Следует ожидать, что любые руководства, стандарты и нормативные документы по средствам контроля, применяемым при разработке и производстве программных продуктов для сферы здравоохранения данного класса (класса С), будут достаточно строгими, сфокусированными (как в рассмотренном примере) на защите данных, безопасности и контроле доступа.

В.5 Диспетчерская система службы скорой помощи

Сфера оказания неотложной помощи неизбежно решает проблему «жизни и смерти», однако в реальности ситуация может складываться иначе. В то время как разработка передовых решений для диспетчерской службы скорой помощи (например, Лондонская служба скорой помощи середины 1990-х годов [24]) и в самом деле решает данную проблему, системы более раннего поколения (которые, например, не позволяют направлять бригады в зависимости от их специализации и/или машины, оборудованные специальной аппаратурой) являются скорее «поддерживающими», чем «исправляющими». Такая система и рассматривается в данном примере.

При рассмотрении реального наихудшего случая следует определить возможные ситуации, при которых после звонка в службу скорой помощи бригада не отправляется на вызов или отправляется не по тому адресу.

В случае летального исхода следует предположить, что состояние пациента было критическим и рядом с ним не было человека, который мог бы сделать вызов и отследить его выполнение. В ситуации, когда человек находится в одиночестве и испытывает обширный сердечный приступ, маловероятно, что он сможет вызвать врача. Если в результате исход будет летальным, то это не будет связано с диспетчерской системой. В случае крупной автомобильной аварии, ранения в бою, обрушения здания или другого значительного инцидента обычно присутствуют представители одной или нескольких служб экстренной медицинской помощи. Можно ожидать, что данные представители смогут точно определить характер травмы и отследить восприимчивость организма. В таких случаях также, если летальный исход произошел до прибытия скорой помощи на место происшествия или сразу после ее прибытия, это не относится к диспетчерской системе службы скорой помощи.

Поэтому для данного сценария последствие, вероятно, будет связано с отдельной личностью, получившей травму, или с группой травмированных людей, когда машина скорой помощи задерживается или не была направлена, что привело к ухудшению состояния и/или увеличению длительности восстановления по сравнению с обычно ожидаемой. Это может привести к длительной недееспособности и/или серьезной психологической травме пациента, что соответствует определению «существенного» последствия.

Рассмотрение правдоподобия наихудшего последствия должно быть комплексным. Неспособность направить машину скорой помощи, задержка отправки машины и отправка ее по неверному адресу (т. е. задержка отправки машины по правильному адресу) могут быть вызваны следующими причинами:

a) задержка вызова скорой помощи (не входит в сферу ответственности службы скорой помощи);

b) задержка ответа диспетчера на звонок (много различных причин, например, недостаточная емкость входящих линий);

c) ошибка или неточность диспетчера при вводе адреса и/или почтового индекса (из-за плохой слышимости или ошибки при печати);

d) направление на вызов недоступной бригады скорой помощи (бригада находится на вызове, отдыхает или по другой причине);

e) сообщение диспетчера не дошло до бригады скорой помощи (по причине, не связанной с самой диспетчерской системой).

Правдоподобие ситуации по перечислению b) оценивается как «очень низкое». Обычно телефонные компании предоставляют для служб экстренной медицинской помощи каналы с высокой пропускной способностью, что считается неотъемлемой составляющей обеспечения нормальной работы.

Если предположить, что система не опирается на знания в данной области или имеет дефекты, то правдоподобие ситуации по перечислению d) может быть оценено как «низкое», поскольку можно предположить, что бригада будет быстро сообщать, что она недоступна для направления на вызов.

Интерес представляет ситуация по перечислению c). Система может не иметь возможности проверки почтовых индексов и/или проверки соответствия адресов и почтовых индексов либо функционирование системы может быть нарушено или дать сбой. Почтовые индексы, несомненно, очень похожи один на другой, не имеют четкой логики и их слишком много, чтобы диспетчер мог запоминать их и соотносить с конкретным адресом. В данном случае правдоподобие данной ситуации оценивается как «высокое», но также может быть оценено и как «очень высокое».

Комбинация «существенного» последствия с «очень низким», «низким» и «высоким» правдоподобием позволяет отнести систему к классам риска D, C и B соответственно. Даже при «очень высоком» правдоподобии последствия система относится к классу риска B, соответствующему реальному наихудшему случаю.

Поэтому практически риски отказа, объединенные в ситуации по перечислению c), должны быть разделены и рассмотрены по отдельности, даже если ни один из них не может повысить степень риска выше класса B. В свете оценки правдоподобия как «высокого» и «очень высокого» следует сконцентрироваться на оценке последствия, чтобы убедиться, что не существует «серьезных» или «катастрофических» сценариев. Если же такие сценарии существуют, то систему следует отнести к классу риска A.

Приложение С
(справочное)

Иллюстрация сути взаимосвязи между классами риска и потенциальными средствами контроля для управления рисками

С.1 Использование классов риска

Целью отнесения программных продуктов к классам риска в соответствии с настоящим стандартом является, в основном, обеспечение четкого различия между:

- программными продуктами, которые могут представлять серьезный риск для пациентов в случае неправильного функционирования;

- программными продуктами, не представляющими серьезного риска для пациентов в случае неправильного функционирования;

- программными продуктами, находящимися между этими двумя крайностями.

Программные продукты, отнесенные к высокому классу риска (например, к классу А), очевидно, требуют особого внимания для обеспечения того, чтобы представляемые ими риски для пациентов не материализовались.

Минимизация вероятности материализации рисков может быть достигнута несколькими неисключительными путями, например следующими:

- контроль при проектировании, производстве, сопровождении и обновлении программного продукта (включая инструкции по применению) для обеспечения, насколько целесообразно, того, что неблагоприятные события, которые могут привести к вредным последствиям, не возникнут на практике;

- обучение и переобучение пользователей для обеспечения их знания о возможных рисках и неблагоприятных событиях в целях предотвращения последствий, к которым могут привести данные события;

- активные административные средства контроля и проверки в рамках окружающей среды, в которой функционирует или с которой взаимодействует система, в целях выявления неблагоприятных событий и предотвращения или уменьшения их последствий.

Лица, ответственные за анализ и снижение рисков в сфере здравоохранения, заинтересованы в идентификации тех программных продуктов, на которые им следует обратить внимание при принятии решения о покупке, внедрении и использовании, а также при анализе способов эксплуатации. Они не обязаны проявлять такое же внимание или применять столь же строгие средства контроля к программным продуктам, относящимся к классам D или Е, как и к продуктам классов А и В.

Лица, ответственные за разработку руководств, стандартов или нормативных документов по средствам контроля, необходимым при проектировании и производстве программных продуктов для сферы здравоохранения, заинтересованы в проведении различия между типами продуктов, которые без адекватных средств контроля могут представлять наибольшие риски, и типами продуктов, которые представляют меньшие риски. Для продуктов класса А требуются наиболее жесткие средства контроля, применяемые с наибольшей строгостью, а для продуктов класса Е — наименее строгие (может быть, и не требуются вовсе).

Инспекторы и разработчики стандартов могут посчитать, что деление программных продуктов на пять классов является излишней градацией, и могут объединить некоторые из них в целях применения укрупненных требований к контролю. Таким образом, для целей определения необходимых средств контроля инспекторы могут принять решение не делать различия между классами А и В или между классами С и D.

Целью настоящего стандарта не является определение средств контроля, необходимых для предотвращения или снижения последствий для пациентов, в соответствии с классом риска программного продукта. Однако очевидно, что для продуктов, относящихся к более высокому классу риска, необходим намного более подробный и строгий анализ при определении мероприятий для снижения риска, чем анализ, проводимый при их «сортировке» в целях отнесения к одному из классов риска в соответствии с настоящим стандартом.

С.2 Основные положения

Классификация рисков, основанная на процессе оценки (сформированная из оценки возможного воздействия на пациента или нанесения вреда пациенту и вероятности его реализации), обеспечит обоснование для средств контроля, рекомендованных для обеспечения безопасности продукта. Данное обоснование будет относиться как к объему, так и к строгости контроля, поэтому потребуется иерархическая многоуровневая библиотека средств контроля.

Процесс классификации рисков не затрагивает такие вопросы, как техническая архитектура, или такие факторы, как зависимость. Поэтому классификация рисков не обеспечивает обоснования применимости. Поскольку данный вопрос должен быть рассмотрен в дальнейшем в руководствах или стандартах по средствам контроля, то отсюда следует, что потребители процесса классификации рисков должны будут сделать такие оценки вручную эмпирическим путем.

Варьируемый объем средств контроля, полученный в результате процесса классификации рисков, может не содержать рекомендаций по их применению для некоторых областей контроля, относящихся к низкому классу риска. Наоборот, для продуктов, отнесенных к высокому классу риска, требования должны быть достаточно жесткими и должны предусматривать выполнение таких работ, как независимая экспертиза, формальное проектирование, всестороннее тестирование и т. д.

Процесс классификации рисков не предназначен для замены построенной на более широкой основе и более детальной оценки рисков. Действительно, оценка рисков является основой обеспечения того, что инфраструктура и среда, в которой размещается программный продукт для сферы здравоохранения, соответствуют рискам. Например, в контексте информационной безопасности данный процесс будет устанавливать требования к таким средствам контроля, как защита от вирусов, безопасность передачи сообщений, сетевая безопасность, конфиденциальность данных в сетях и т. д. Более того, итоговые комбинированные требования, вероятно, будут охватывать взаимодействия, интерфейсы и функциональную совместимость программного продукта для сферы здравоохранения, чтобы задействовать их в интересах безопасности.

С.3 Примеры контролируемых факторов

В процессе ведения и интерпретации установленной «классификации рисков» может потребоваться рассмотрение следующих факторов, контролируемых соответствующими средствами:

- действия по дополнительной классификации рисков;
- действия по оценке рисков, связанных с безопасностью;
- программное управление;
- программное управление рисками;
- средства проектирования;
- управление проектированием системы;
- квалификация и опыт проектировщиков системы;
- правила отображения и представления информации;
- целостность проекта;
- гарантия правильности/аттестация проекта;
- средства разработки системы;
- управление разработкой системы;
- квалификация и опыт разработчиков системы;
- средства контроля целостности;
- тестирование/техническая гарантия защиты системы от проникновения;
- средства разработки базы знаний;
- управление проектированием базы знаний;
- управление разработкой базы знаний;
- гарантия правильности/аттестация базы знаний;
- разработка политики безопасности;
- требования к устойчивости и резервированию;
- идентификация и аутентификация;
- контроль доступа пользователей;
- повторное использование объектов;
- требования к хранению/планирование объема памяти;
- требования к резервному копированию;
- бухгалтерский учет и аудит;
- защита от сбоев оборудования;
- контроль происшествий;
- контроль непрерывности бизнес-процессов;
- разработка тестирования систем;
- формальная оценка разработанных систем;
- разработка процедур эксплуатации;
- разработка процедур сопровождения;
- разработка процедур пользователя;
- обучение персонала;
- руководство администрированием.

Данный перечень не является окончательным и потребует дальнейшего анализа и проработки, прежде чем он сможет быть принят в каком-либо из руководств или стандартов. Степень востребованности перечисленных контролируемых факторов и строгость, с которой они должны контролироваться, будут зависеть от класса риска.

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 Organization 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, pp. 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] 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

[8] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices

[9] Council Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in-vitro diagnostic medical devices

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

[11] ISO 14971, Medical devices — Application of risk management to medical devices

[12] IEC 61508-4:1998, Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

[13] IEC 61508 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

[14] ISO/IEC Guide 73:2002, Risk management — Vocabulary — Guidelines for use in standards

[15] UK Government Information Security, Risk Analysis and Management Method (CRAMM) User Manual, CCTA, (now part of the Office of Government on Commerce) Publisher Central Computer Telecommunications Agency

[16] ISO/IEC 17799:2005, Information technology — Security techniques — Code of practice for information security management

[17] AS/NZS 4360:1999, Risk Management

[18] Corporate governance in health care Qualitative Measures of Likelihood of Risk, Department of Health, England

[19] Fernando, B., Savelych, B., Avery, A., Bainbridge, M., Horsfield, P and Teasdale, S., Prescribing safety features of general practice computer systems: evaluation using simulated test cases, BMJ, May 2004, 328, pp. 1171—1172

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

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

[22] IEC 60601-1-4, Medical electrical equipment — Part 1-4: General requirements for safety — Collateral Standard: Programmable electrical medical systems

[23] EN 1441, Medical devices — Risk analysis

[24] LASCAD Case Study available at: http://

gost.e-ecolog.ru

УДК 61:004:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, безопасность пациентов, риски, классификация угроз безопасности, программное обеспечение для сферы здравоохранения

Редактор *М.Р. Холодкова*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 05.10.2010. Подписано в печать 13.10.2010. Формат 60x84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 3,26. Уч.-изд. л. 3,00. Тираж 79 экз. Зак. 812.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6

gost.e-ecolog.ru