ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56841— 2015/IEC/TR 80001-2-4: 2012

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-4

Руководство по применению. Общее руководство для медицинских организаций

(IEC/TR 80001-2-4:2012,
Application of risk management for IT-networks incorporating medical devices — Part 2-4: Application guidance — General implementation guidance for healthcare delivery organizations,
IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 28 декабря 2015 г. № 2229-ст

4 Настоящий стандарт идентичен международному документу IEC/TR 80001-2-4:2012 «Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2-4. Руководство по применению. Общее руководство для медицинских организаций» (IEC/TR 80001-2-4:2012 «Application of risk management for IT-networks incorporating medical devices — Part 2-4: Application guidance — General implementation guidance for healthcare delivery organizations», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Ноябрь 2018 г.

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

© Стандартинформ, оформление, 2018

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
1.1 Цель 1
1.2 Медицинская организация 1
1.3 Сфера применения 1
1.4 Необходимые предварительные условия 2
2 Нормативные ссылки 2
3 Термины и определения 2
4 ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ 5
4.1 Ответственности ВЫСШЕГО РУКОВОДСТВА 5
4.2 Учитываемые факторы небольших ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ 6
4.3 Учитываемые факторы больших ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ 6
5 Шаги реализации МЕНЕДЖМЕНТА РИСКА 7
5.1 Обзор 7
5.2 Определение клинического контекста предоставления медицинских услуг 7
5.3 Утверждение основного подхода для выполнения МЕНЕДЖМЕНТА РИСКА 7
5.4 Определение и описание МЕДИЦИНСКОЙ ИТ СЕТИ 8
6 СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ 11
Приложение А (справочное) Примеры конфигураций МЕДИЦИНСКИХ ИТ СЕТЕЙ 12
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 16
Библиография 17

Введение

Настоящий стандарт является руководством, предназначенным помочь МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ (см. 1.2) выполнить свои обязательства ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ по применению стандарта МЭК 80001-1 совместно с другими стандартами в данной серии. В частности, настоящий стандарт позволяет МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ оценить его влияние на организацию и установить последовательности деловых процессов в виде обычных ПРОЦЕССОВ для управления РИСКОМ на стадиях создания, сопровождения и поддержания в рабочем состоянии МЕДИЦИНСКИХ ИТ СЕТЕЙ. И хотя настоящий стандарт нацелен исключительно на МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ, понятие ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ используется в настоящем стандарте для обеспечения целостности терминологии МЭК 80001-1. В этом смысле эти два понятия являются синонимами.

Настоящий стандарт будет полезен лицам, ответственным за установление в рамках ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, планирующей создание одной и нескольких МЕДИЦИНСКИХ ИТ сетей общего подхода к МЕНЕДЖМЕНТУ РИСКА, соответствующему МЭК 80001-1. В особенности общий подход к МЕНЕДЖМЕНТУ РИСКА должен обеспечивать ОСНОВНЫЕ СВОЙСТВА — БЕЗОПАСНОСТЬ, ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМЫ и ЭФФЕКТИВНОСТЬ, как они определены в МЭК 80001-1. Целью общего подхода является предотвращение возможных проблем, идентифицированных в МЭК 80001-1, которые связаны с подключением МЕДИЦИНСКИХ ПРИБОРОВ к ИТ сетям.

Установление и реализация общего подхода к МЕНЕДЖМЕНТУ РИСКА и изменения в деловых процессах, которые он может за собой повлечь, потребует от ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ использования всего набора навыков, которыми располагает организация, связанных как с управлением, так и с технической и клинической деятельностью. В случаях, когда подобными навыками в ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ никто не обладает, следует рассмотреть вариант сотрудничества с аналогичными организациями или с экспертами в данной области. Важно, чтобы ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ могла опираться на экспертные знания, относящиеся к подходящим стандартам и соответствующим им техническим отчетам.

При формировании инфраструктуры МЕНЕДЖМЕНТА РИСКА ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна учитывать:

- размер и возможности организации;
- масштаб ИТ операций организации и сложность текущей инфраструктуры и систем организации, а также
- стоимость реализации МЭК 80001-1.

Предполагается, что некоторые из вышеперечисленных факторов, например размер ИТ операции и сложность сетей, будут пропорциональны размеру организации. Важно, чтобы сам общий подход не создавал РИСК для пациентов, предъявляя излишние требования к медицинскому персоналу, в то же время эта рабочая нагрузка не должна привнести новые устранимые РИСКИ при реализации новой технологии.

При рассмотрении ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ основных решений и шагов, требующихся для успешного формирования структуры МЕНЕДЖМЕНТА РИСКА для МЕДИЦИНСКИХ ИТ сетей, необходимо учитывать, что данный документ ссылается как на малые, так и на большие организации. Данные понятия являются субъективными, и никаких точных мер измерения размеров организаций не дается, тем не менее:

- маленькой организацией может являться медицинский центр:
- с небольшим числом практикующих врачей, или
- с большим числом практикующих врачей, с консолидированной ИТ функцией и с высоко централизованной структурой управления;
- большой организацией может быть:
- объединение, состоящий из множества больниц, или
- организация с распределенными клиниками и комбинацией внутреннего и стороннего руководства клинической и ИТ деятельностью.

Небольшие организации могут также подчиняться более крупной соответствующей организации.

Общий подход к МЕНЕДЖМЕНТУ РИСКА, разработанный ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ, если следовать указаниям настоящего стандарта, должен сочетаться с формализованными системами

менеджмента, которые повсеместно используются в обычных деловых процессах. Подобный деловой процесс в виде обычных ПРОЦЕССОВ, необходимых для обеспечения выполнения МЕНЕДЖМЕНТА РИСКА, является частью постоянного требования при изменении систем или развертывании новых систем, посредством:

- включения ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА в существующие ПРОЦЕССЫ менеджмента, например, в систему менеджмента качества организации;
- обеспечения включения ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА в график внутреннего аудита;
- предоставления обучения МЕНЕДЖМЕНТУ РИСКА, как части введения в курс обязанностей нового персонала, и предоставления подобного обучения уже задействованному персоналу; а также
- обеспечения выполнения МЕНЕДЖМЕНТА РИСКА как для новой работы, так и для изменений в существующих МЕДИЦИНСКИХ СЕТЯХ.

Утвердив структуру МЕНЕДЖМЕНТА РИСКА, ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ становится готовой к выполнению подробной ОЦЕНКИ РИСКА (см. IEC/TR 80001-2-1 [1]).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-4

Руководство по применению.
Общее руководство для медицинских организаций

Health informatics. Risk management for IT-networks incorporating medical devices. Part 2-4. Application guidance. General guidance for healthcare delivery organizations

Дата введения — 2016—11—01

1 Область применения

1.1 Цель

Настоящий стандарт предназначен помочь ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ при принятии основных решений и выполнении шагов, требующихся для установления общего подхода к МЕНЕДЖМЕНТУ РИСКА, перед тем, как организация предпримет детальную ОЦЕНКУ РИСКА для каждой из своих МЕДИЦИНСКИХ ИТ СЕТЕЙ. Данные шаги сопровождаются точками принятия решений, предназначенными направлять ОТВЕТСТВЕННУЮ ОРГАНИЗАЦИЮ в ПРОЦЕССЕ понимания контекста МЕДИЦИНСКОЙ ИТ СЕТИ и идентификации любых организационных изменений, которые требуются при реализации ответственных решений ВЫСШИМ РУКОВОДСТВОМ, как это определено на рисунке 1 МЭК 80001-1.

1.2 Медицинская организация

Данный технический отчет направлен на все МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ. МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ включают больницы, офисы врачей, дома коммунальной медико-социальной помощи и клиники.

В обеспечении МЕДИЦИНСКОЙ ИТ СЕТИ, содержащей МЕДИЦИНСКИЙ ПРИБОР, в рамках МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ может участвовать несколько ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ. В настоящем стандарте основное внимание уделяется МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ и ее обязательствам согласно МЭК 80001-1.

Для МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ важно идентифицировать ОТВЕТСТВЕННУЮ(ЫЕ) ОРГАНИЗАЦИЮ(ИИ), несущую(ие) ответственность за любые аспекты сети, которые регулируются МЭК 80001-1. Это позволяет четко распределить роли и ответственности настоящего стандарта.

1.3 Сфера применения

В настоящем стандарте подробно рассмотрены шаги, которые необходимо выполнить ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ для реализации требований пунктов 3.1—3.3 и 4.1—4.6 МЭК 80001-1:2010.

Примечание — Предполагается, что ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ будет использовать IEC/TR 80001-2-1 [1] для получения подробных советов по выполнению требований подраздела 4.4 МЭК 80001-1:2010.

Издание официальное

1.4 Необходимые предварительные условия

МЭК 80001-1:2010 является необходимым предварительным условием для настоящего стандарта. Руководящие указания, представленные в настоящем стандарте, предназначены помочь ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ установить общий подход к МЕНЕДЖМЕНТУ РИСКА для удовлетворения базовых требований МЭК 80001-1, обеспечивая:

- наличие политики и ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА;
- установление масштабов вероятности, тяжести и допустимость РИСКА;
- строгое определение МЕДИЦИНСКИХ ИТ сетей.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы или их части, обязательные для применения данного документа. В случае датированных ссылок действует только цитируемое издание. Для недатированных ссылок действует самое позднее издание документа, на который производится ссылка (включая любые внесенные в него поправки).

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

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **СОПРОВОДИТЕЛЬНЫЙ ДОКУМЕНТ** (ACCOMPANYING DOCUMENT): Документ, сопровождающий МЕДИЦИНСКИЙ ПРИБОР или вспомогательное оборудование и содержащий информацию, предназначенную для ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ или ОПЕРАТОРА, в частности, касающуюся БЕЗОПАСНОСТИ.

Примечание — Адаптировано из МЭК 60601-1:2005, статья 3.4.

[МЭК 80001-1:2010, статья 2.1]

3.2 **УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ** (CHANGE-RELEASE MANAGEMENT): Процесс, гарантирующий, что все изменения в ИТ СЕТИ оценены, приняты, выполнены и проанализированы контролируемым способом, а также, что изменения проведены, распространены и отслежены, что приводит к смене версии контролируемым способом с соответствующими входными и выходными данными для УПРАВЛЕНИЯ КОНФИНУРАЦИЕЙ.

Примечание — Адаптировано из ИСО/МЭК 20000-1:2005, подразделы 9.2 и 10.1.

[МЭК 80001-1:2010, статья 2.2]

3.3 **УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ** (CONFIGURATION MANAGEMENT): ПРОЦЕСС, гарантирующий, что информация о конфигурации компонентов и ИТ СЕТИ определена и поддерживается с надлежащей точностью и контролем, а также обеспечивает механизм для идентификации, управления и отслеживания версий ИТ СЕТИ.

Примечание — Адаптировано из ИСО/МЭК 20000-1:2005, подраздел 9.1.

[МЭК 80001-1:2010, статья 2.4]

3.4 **ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ** (DATA AND SYSTEM SECUIRTY): Рабочее состояние МЕДИЦИНСКОЙ ИТ сети, в котором информационные ресурсы (данные и системы) обоснованно защищены от нарушения конфиденциальности, полноты и доступа.

Примечания

1 В настоящем стандарте в понятие защиты включена ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ.

2 ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ обеспечивается совокупностью политики, руководящих принципов, инфраструктуры и служб, спроектированных для защиты информационных ресурсов и систем, которые передают, хранят и используют информацию для осуществления миссии организации.

[МЭК 80001-1:2010, статья 2.5]

3.5 **ЭФФЕКТИВНОСТЬ** (EFFECTIVENESS): Способность достигать намеченных результатов по отношению к пациенту и ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

[МЭК 80001-1:2010, статья 2.6]

3.6 **УПРАВЛЕНИЕ СОБЫТИЕМ** (EVENT MANAGEMENT): ПРОЦЕСС, который гарантирует, что все события, негативно влияющие или способные негативно повлиять на работу ИТ СЕТИ, фиксируются, оцениваются и обрабатываются контролируемым способом.

Примечание — Адаптировано из ИСО/МЭК 20000-1:2005, подразделы 8.2 и 8.3.

[МЭК 80001-1:2010, статья 2.7]

3.7 **ВРЕД** (HARM): Физическая травма, или ущерб здоровью людей, или имуществу, или окружающей среде, а также снижение ЭФФЕКТИВНОСТИ или нарушение ЗАЩИЩЕННОСТИ СИСТЕМЫ И ДАННЫХ.

Примечание — Адаптировано из ИСО 14971:2007, подраздел 2.2.

[МЭК 80001-1:2010, статья 2.8]

3.8 **ОПАСНОСТЬ** (HAZARD): Потенциальный источник ВРЕДА.

[МЭК 80001-1:2010, статья 2.9]

3.9 **ОПАСНАЯ СИТУАЦИЯ** (HAZARDOUS SITUATION): Обстоятельства, при которых люди, имущество или окружающая среда подвержены одной или нескольким ОПАСНОСТЯМ.

[МЭК 14971:2007, статья 2.4]

3.10 **МЕДИЦИНСКАЯ ОРГАНИЗАЦИЯ, МО** (HEALTHCARE DELIVERY ORGANIZATION): Одна или несколько **ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ**.

Примечание — В настоящем стандарте МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ полагаются профессиональными организациями здравоохранения, включая больницы, офисы врачей, дома коммунальной медико-социальной помощи и клиники.

3.11 **ИТ СЕТЬ** (INFORMATION TECHNOLOGY NETWORK, IT-NETWORK): Система или системы, состоящие из взаимодействующих узлов и каналов передачи данных, предназначенные для обеспечения проводной или беспроводной передачи данных между двумя или более установленными узлами коммуникации.

Примечания

1 Адаптировано из МЭК 61907:2009, статья 3.1.1.

2 В настоящем стандарте область применения МЕДИЦИНСКОЙ ИТ СЕТИ определяется ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ в зависимости от того, где в МЕДИЦИНСКОЙ ИТ СЕТИ располагаются МЕДИЦИНСКИЕ ПРИБОРЫ, а также от заданного применения сети. В область применения могут входить ИТ инфраструктура, медицинское обслуживание на дому и неклинические применения.

[МЭК 80001-1:2010, статья 2.12]

3.12 **ОСНОВНЫЕ СВОЙСТВА** (KEY PROPERTIES): Три управляемые характеристики риска (БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ) МЕДИЦИНСКИХ ИТ СЕТЕЙ.

[МЭК 80001-1:2010, статья 2.13]

3.13 **МЕДИЦИНСКИЙ ПРИБОР** (MEDICAL DEVICE): Любой инструмент, устройство, приспособление, машина, прибор, имплантат, реагент или калибратор в пробирке, программное обеспечение, материал или другие подобные, связанные с ними изделия:

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

- диагностика, профилактика, контроль, лечение или облегчение течения заболеваний,
- диагностика, контроль, лечение, облегчение травмы или компенсация последствий травмы,
- исследования, замещения, изменения или поддержка анатомического строения или физиологических процессов,
- поддержание и сохранение жизни,
- предупреждение беременности,
- дезинфекция медицинских приборов,
- предоставление информации для медицинских и диагностических целей, посредством исследований проб в пробирке, полученных из тела человека; и

b) не реализующие свое основное предназначение в или на теле человека с помощью фармакологических, иммунологических или метаболических средств, но чья основная функция может поддерживаться подобными мерами.

Примечания

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

2 Изделия, которые в некоторых юрисдикциях могут быть приняты за медицинские приборы, но к которым еще не существует согласованного подхода, это:

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

3 Аксессуары, специально предназначенные производителями для использования совместно с медицинским прибором, для которого они разработаны, для реализации цели медицинского прибора, должны подчиняться тем же процедурам GHT (Целевая группа глобальной гармонизации), которые применяются к самому медицинскому прибору. Например, аксессуар классифицируется так, как будто он является медицинским прибором. Это может привести к различию в классификациях аксессуара и прибора, для которого он разработан.

4 Компоненты медицинских приборов в общих случаях контролируются через систему управления качеством производителя и процедуры оценки соответствия прибора. В некоторых юрисдикциях компоненты включаются в определение «медицинского прибора».

[МЭК 80001-1:2010, статья 2.14]

3.14 **МЕДИЦИНСКАЯ ИТ СЕТЬ** (MEDICAL IT-NETWORK): ИТ СЕТЬ, к который подключен хотя бы один МЕДИЦИНСКИЙ ПРИБОР.

[МЭК 80001-1:2010, статья 2.16]

3.15 **СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ СЕТИ** (MEDICAL IT-NETWORK RISK MANAGER): Лицо, ответственное за МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ СЕТИ.

[МЭК 80001-1:2010, статья 2.17]

3.16 **ОПЕРАТОР** (OPERATOR): Лицо, работающее с оборудованием.

[МЭК 80001-1:2010, статья 2.18]

3.17 **ПРОЦЕСС** (PROCESS): Совокупность взаимосвязанных и взаимодействующих действий, преобразующая входы в выходы.

Примечание — Термин «действия» охватывает и использование ресурсов.

[МЭК 80001-1:2010, 2.19]

3.18 **СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ** (RESPONSIBILITY AGREEMENT): Один или более документов, которые совместно определяют все ответственности для всех значимых заинтересованных сторон.

Примечание — Данное соглашение может быть юридическим документом, например контрактом.

[МЭК 80001-1:2010, статья 2.21]

3.19 **ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ** (RESPONSIBILE ORGANIZATION): Юридическое или физическое лицо, ответственное за использование и обслуживание МЕДИЦИНСКОЙ ИТ СЕТИ.

Примечания

1 Ответственным лицом может быть, например, больница, частный врач или организация телемедицины.

2 Адаптировано из МЭК 60601-1:2005, подраздел 3.101.

[МЭК 80001-1:2010, статья 2.22]

3.20 **РИСК** (RISK): Комбинация вероятности причинения ВРЕДА и его тяжести.

[МЭК 80001-1:2010, статья 2.23]

3.21 **АНАЛИЗ РИСКА** (RISK ANALYSIS): Систематическое использование доступной информации для выявления ОПАСНОСТЕЙ и количественной оценки РИСКА.

[МЭК 80001-1:2010, статья 2.24]

3.22 **ОЦЕНКА РИСКА** (RISK ASSESSMENT): Общий процесс, включающий в себя АНАЛИЗ РИСКА и ОЦЕНИВАНИЕ РИСКА.

[МЭК 80001-1:2010, статья 2.25]

3.23 **УПРАВЛЕНИЕ РИСКОМ** (RISK CONTROL): ПРОЦЕСС принятия решений и выполнения мер по уменьшению рисков до установленных уровней или поддержания рисков внутри установленного диапазона.

[МЭК 80001-1:2010, статья 2.26]

3.24 **ОЦЕНИВАНИЕ РИСКА** (RISK EVALUATION): ПРОЦЕСС сравнения количественно оцененного РИСКА с заданными критериями РИСКА для определения значимости РИСКА.

[МЭК 80001-1:2010, статья 2.27]

3.25 **МЕНЕДЖМЕНТ РИСКА** (RISK MANAGEMENT): Систематическое применение политик, процедур и практических методов менеджмента для решения задач анализа, оценивания, управления и контроля РИСКА.

[МЭК 80001-1:2010, статья 2.28]

3.26 **ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ** (RISK MANAGEMENT FILE): Совокупность записей и других документов, создаваемых в процессе МЕНЕДЖМЕНТА РИСКА.

[МЭК 80001-1:2010, статья 2.29]

3.27 **БЕЗОПАСНОСТЬ** (SAFETY): Отсутствие недопустимого РИСКА физической травмы, или ущерба здоровью людей, или ущерба имуществу, или окружающей среде.

Примечание — Адаптировано из ИСО 14971:2007, подраздел 2.24.

[МЭК 80001-1:2010, статья 2.30]

3.28 **ВЫСШЕЕ РУКОВОДСТВО** (TOP MANAGEMENT): Лицо или группа лиц, реализующих направление(я) деятельности и управление ОТВЕСТВЕННОЙ ОРГАНИЗАЦИЕЙ, отвечающих за МЕДИЦИНСКУЮ ИТ СЕТЬ на самом высоком уровне.

Примечание — Адаптировано из ИСО 9000:2005, пункт 3.2.7.

[МЭК 80001-1:2010, статья 2.31]

4 ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ

4.1 Ответственности ВЫСШЕГО РУКОВОДСТВА

Данный раздел затрагивает обязанности, которые МЭК 80001-1 возлагает на ВЫСШЕЕ РУКОВОДСТВО организации, а также охватывает потребность четко установленной политики для установления соответствия с МЭК 80001-1.

Как правило, ВЫСШЕЕ РУКОВОДСТВО формирует достаточно независимое функциональное подразделение, контролирующее эффективное выполнение работ по МЕНЕДЖМЕНТУ РИСКА в организации. Шаги, описанные в настоящем стандарте, обычно выполняются командой, состоящей из сотрудников ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Рекомендуется собирать такую команду из представителей различных отделов, включая отделы ИТ, биомедицинской инженерии, медицинский отдел и отдел МЕНЕДЖМЕНТА РИСКА. Состав команды должен соответствовать существующим внутри организации структурным подразделениям. Такая команда может рассматривать вопросы БЕЗОПАСНОСТИ пациентов и защищенности сети. Старшие медицинские работники должны принять участие в создании данного функционального подразделения и впоследствии консультировать по вопросам влияния на клинические процессы ОПАСНОСТЕЙ, связанных с ИТ СЕТЬЮ, что является частью процесса ОЦЕНКИ РИСКА. Должны также быть установлены соответствующие связи с подразделениями медицинской организации, ответственными за управление или контроль.

От ВЫСШЕГО РУКОВОДСТВА требуется обеспечение выполнения следующих функций:

- утверждение и документальное оформление политики МЕНЕДЖМЕНТА РИСКА в организации. Данная политика должна будет направлена на обеспечение ОСНОВНЫХ СВОЙСТВ;

- создание и распространение подходящих ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА. Данные ПРОЦЕССЫ могут быть соединены с клинической системой менеджмента БЕЗОПАСНОСТИ ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, ее системой менеджмента качества или же с ее корпоративной системой МЕНЕДЖМЕНТА РИСКА, если такие системы существуют;

- установление критериев допустимого РИСКА для определения того, какие из РИСКОВ приемлемы для организации. В данных критериях должны учитываться:

- регламент (например, Директивы ЕС),

- международные стандарты,

- национальные стандарты,

- региональные стандарты,
- профессиональные (например, клинические) руководства;
- уверенность в том, что для развертывания и использования МЕДИЦИНСКИХ ИТ СЕТЕЙ применяется пошаговый подход так, что ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКА могут быть разумно и эффективно применены в соответствии со сложностью развертываемой МЕДИЦИНСКОЙ ИТ СЕТИ. Данный подход требует от ВЫСШЕГО РУКОВОДСТВА утверждения каждого шага;
- проверка пригодности ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА в запланированные регулярные промежутки времени для обеспечения непрерывной ЭФФЕКТИВНОСТИ ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА и для документального оформления любых принятых решений и действий.

Как большим, так и малым организациям следует начинать свою реализацию МЭК 80001-1 с создания ФАЙЛА МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ СЕТИ, в котором должна быть зафиксирована информация о всей деятельности организации в данной области. ФАЙЛА МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ СЕТИ может использоваться как средство демонстрации соответствия организации требованиям МЭК 80001-1, что являющееся частью процесса аудита.

4.2 Учитываемые факторы небольших ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ

При оценивании функций ВЫСШЕГО РУКОВОДСТВА небольшой организации следует учитывать следующие факторы:

- Имеет ли организация какие-либо системы, которые создают помехи для МЕДИЦИНСКИХ ПРИБОРОВ? Применим ли в настоящий момент МЭК 80001-1 к деятельности организации? Есть ли у организации планы интегрирования МЕДИЦИНСКИХ ПРИБОРОВ в ИТ инфраструктуру организации?
- Может ли организация поэтапно и безопасно осуществить свои планы по достижению нормативов за более длительный промежуток времени, тем самым понизив непосредственную нагрузку на ресурсы?
- Есть ли поблизости похожие на организацию ОТВЕТСТВЕННЫЕ ОРГАНИЗАЦИИ, с которыми можно было бы разделить ресурсы и совместно добиться соответствия МЭК 80001-1? Известны ли руководству похожие ОТВЕТСТВЕННЫЕ ОРГАНИЗАЦИИ, уже добившиеся соответствия и готовые поделиться опытом?
- Каким образом организация может установить точную спецификацию средств для ИТ операций? Обладает ли она правильным проектом для своих ИТ СЕТЕЙ и любых существующих в организации МЕДИЦИНСКИХ ИТ СЕТЕЙ? Где находится граница между МЕДИЦИНСКОЙ ИТ СЕТЬЮ и стандартными ИТ системами организации?
- Утвержден ли в организации формальный ПРОЦЕСС для принятия подобных решений соответствия? Имеется ли у организации подходящее хранилище или, например, система менеджмента качества, в которую могут быть включены ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКА? Каким образом организация планирует подготовить подобные ПРОЦЕССЫ?
- Работает ли в организации сотрудник (менеджер или администратор), который может принять на себя дополнительные ответственности за МЕНЕДЖМЕНТ РИСКА МЕДИЦИНСКОЙ ИТ СЕТИ? Каким образом организация планирует проводить подходящее обучение персонала для выполнения МЕНЕДЖМЕНТА РИСКА?

4.3 Учитываемые факторы больших ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ

При оценивании функций ВЫСШЕГО РУКОВОДСТВА большой организации следует учитывать следующие нижеописанные факторы в дополнении к фактором, идентифицированным выше для небольшой организации:

- На ком в организации лежит ответственность за МЕНЕДЖМЕНТ РИСКА? Кто должен владеть политикой МЕНЕДЖМЕНТА РИСКА? Как с этим связано руководство клинической деятельностью?
- Как ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКА встраиваются в систему менеджмента качества организации? Какое место в организации будут занимать ПРОЦЕССЫ и политика МЕНЕДЖМЕНТА РИСКА?
- Каким образом ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА может быть разделен на управляемые подПРОЦЕССЫ и каким образом эти подПРОЦЕССЫ должны координироваться?
- Требуется ли организации специальный проект соответствия МЭК 80001-1? Необходимо ли назначение менеджера проекта и команды для его выполнения?
- Какие подготовительные работы по ИТ поддержке были сделаны? На каких поставщиках сказываются данные требования? Были ли ответственности поставщика грамотно ему сообщены?

5 Шаги реализации МЕНЕДЖМЕНТА РИСКА

5.1 Обзор

В настоящем разделе рассматриваются общий подход к МЕНЕДЖМЕНТУ РИСКА и необходимая предварительная работа, которую ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ необходимо выполнить перед тем, как она приступит к детальной ОЦЕНКЕ РИСКА новой или изменяющейся МЕДИЦИНСКОЙ ИТ СЕТИ.

Настоящий стандарт для реализации МЭК 80001-1 предлагает следующие три шага:

- установить клинический контекст, в рамках которого осуществляется предоставление медицинских услуг (см. 5.2);
- утвердить основной подход, лежащий в основе МЕНЕДЖМЕНТА РИСКА (см. 5.3),
- определить и понять существующие МЕДИЦИНСКИЕ ИТ СЕТИ (см. 5.4).

Эти три шага подробно рассматриваются в последующих подразделах.

5.2 Определение клинического контекста предоставления медицинских услуг

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна установить четкое понимание цели организации с медицинской точки зрения.

Для получения этого понимания ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ может рассмотреть следующее:

- клинические потребности пациентов, для которых организация предоставляет свои услуги;
- природу клинических услуг, предоставляемых организацией и ПРОЦЕССОВ, связанных с каждой из этих услуг;
- подбор медицинских кадров и их компетенцию.

5.3 Утверждение основного подхода для выполнения МЕНЕДЖМЕНТА РИСКА

Существует требование, согласно которому ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна определить основной подход к МЕНЕДЖМЕНТУ РИСКА и утвердить ПРОЦЕССЫ для данного менеджмента перед началом детальной ОЦЕНКИ РИСКА.

ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ следует рассмотреть, какие ПРОЦЕССЫ необходимы для поддержания деятельности МЕНЕДЖМЕНТА РИСКА. Например, это должны быть ПРОЦЕССЫ, соразмерные масштабу организации, клиническому контексту и уровню ИТ операций.

Определяя масштаб ПРОЦЕССОВ, которые необходимо разработать, или существующих ПРОЦЕССОВ, требующих обновления, организации следует обеспечить, как минимум, рассмотрение следующих определенных в МЭК 80001-1 процессов:

- МЕНЕДЖМЕНТ РИСКА (МЭК 80001-1:2010, пункт 4.2.2 и подразделы 4.4);
- УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ (МЭК 80001-1:2010, пункт 4.5.1);
- УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ (МЭК 80001-1:2010, пункт 4.5.1);
- запуск в эксплуатацию (МЭК 80001-1:2010, пункт 4.5.3);
- контроль (МЭК 80001-1:2010, пункт 4.6.1);
- УПРАВЛЕНИЕ СОБЫТИЯМИ (МЭК 80001-1:2010, пункт 4.6.2).

При формулировании ПРОЦЕССОВ, направляющих работу МЕНЕДЖМЕНТА РИСКА, существует несколько перечисленных далее принципов, которые помогут определить и сосредоточиться на потребностях ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ:

- **Не создавать дополнительный РИСК.** Работа сама по себе не должна привносить дополнительный РИСК, например, отвлекая практикующих врачей и перегружая дополнительной деятельностью в то время, как они заняты предоставлением медицинских услуг пациентам.

- **Легкость в работе.** Средства управления МЕНЕДЖМЕНТОМ РИСКА должны избегать чрезмерно бюрократические ПРОЦЕССЫ и быть соразмерными уровню РИСКА, идентифицированного в ходе ОЦЕНКИ РИСКА.

- **Ответственность.** Назначила ли ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ подходящий персонал для оценки РИСКОВ и несущий за них ответственность? Например, практикующие врачи несут ответственность за клинические ПРОЦЕССЫ и, таким образом, находятся в хорошем положении для оценки тяжести ВРЕДА. Следует регулярно консультироваться с ними для подтверждения решений и заключений в процессе ОЦЕНКИ РИСКА.

- **Согласованность.** Деятельность МЕНЕДЖМЕНТА РИСКА должна органично сосуществовать с мерами руководства клинической практикой в рамках ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ и соответствовать значимым национальным профессиональным клиническим стандартам и требованиям регламентов/законов.

- **Сетевой РИСК.** Введение новой МЕДИЦИНСКОЙ ИТ СЕТИ будет служить компромиссом между РИСКАМИ. Это позволит устранить или смягчить внутренние РИСКИ, которые приносит новая технология. При некоторых обстоятельствах, например в случае капиталовложения, на ОТВЕТСТВЕННУЮ ОРГАНИЗАЦИЮ может возлагаться обязанность продемонстрировать, что введение новой системы приведет к новым снижениям уровней РИСКА для пациента и организации. Для этой демонстрации от ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ потребуется провести оценку как старых, так и новых систем в соответствии с общим подходом к МЕНЕДЖМЕНТУ РИСКА.

5.4 Определение и описание МЕДИЦИНСКОЙ ИТ СЕТИ

5.4.1 Выполнение ОЦЕНКИ РИСКА

Выполнение ОЦЕНКИ РИСКА требует детального понимания того, каким образом МЕДИЦИНСКАЯ ИТ СЕТЬ предоставляет свои услуги. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна сформировать четкое понимание каждой МЕДИЦИНСКОЙ ИТ СЕТИ, ее границ, ее интерфейсов, типов данных, передающихся между ними и внутри каждой из них, а также того, каким образом используется информация.

В контексте настоящего стандарта МЕДИЦИНСКАЯ ИТ СЕТЬ может состоять:

- из индивидуального, дискретного МЕДИЦИНСКОГО ПРИБОРА, соединенного напрямую с ИТ СЕТЬЮ ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ;
- нескольких дискретных МЕДИЦИНСКИХ ПРИБОРОВ, соединенных напрямую с ИТ СЕТЬЮ ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ; или
- автономная МЕДИЦИНСКАЯ ИТ СЕТЬ, которая целиком подключена к ИТ СЕТИ ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

При анализе каждой МЕДИЦИНСКОЙ ИТ СЕТИ следует учитывать следующие аспекты:

- конфигурацию МЕДИЦИНСКОЙ ИТ СЕТИ, включая четкое определение оборудования, которое образует сеть, и функций, которые это оборудование предоставляет, а также интерфейсов «человек—машина» и данных, которыми обмениваются между этими интерфейсами (см. 5.4.2);
- статус разработки МЕДИЦИНСКОЙ ИТ СЕТИ (см. 5.4.3);
- доступный уровень поддержки (см. 5.4.5).

Выполняя вышеописанный анализ, большая ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна учесть следующие факторы:

- **Есть ли логический претендент на роль демонстрационного проекта?** Создание крупной и сложной МЕДИЦИНСКОЙ ИТ СЕТИ является достаточно сложной задачей для организации. Полезной методикой для осуществления этой задачи является использование пилотного (демонстрационного) проекта для обоснования необходимости новых ПРОЦЕССОВ.

- **Каким образом организация может идентифицировать квалифицированных людей для сбора информации?** На этот вопрос следует дать ответ перед сбором информации. Создавать многопрофильную команду для рассмотрения технических и клинических вопросов, которые возникнут, лучше всего с самого начала. Можно подготовить контактные сведения и оформить соглашения с руководителями подразделений, тем самым предотвращая возможную потерю темпа позже при выполнении ПРОЦЕССА.

5.4.2 Конфигурация МЕДИЦИНСКОЙ ИТ СЕТИ

5.4.2.1 Основные сведения о компонентах МЕДИЦИНСКОЙ ИТ СЕТИ

ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ потребуется сформировать отчетливое понимание компонентов МЕДИЦИНСКОЙ ИТ СЕТИ и того, как они взаимодействуют. Например, получить основные сведения об установленных МЕДИЦИНСКИХ ПРИБОРАХ, всех соединенных систем, характере связи и взаимоотношения компонентов и о более широких сетевых службах, таких как резервное копирование. Необходимо отметить, что пункт 4.3.2 МЭК 80001-1:2010 требует от организации установить список ресурсов для ИТ СЕТИ.

Усилия, которые требуются для сбора информации, пропорциональны сложности МЕДИЦИНСКОЙ ИТ СЕТИ и тому, насколько четко на данный момент она была документально оформлена. Тип сети может «потребовать» от ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ близкого взаимодействия с другими организациями.

В процессе описания конфигурации МЕДИЦИНСКОЙ ИТ СЕТИ могут быть сформированы следующие перечисленные далее представления (при необходимости можно также сформировать дополнительные представления):

- **Физическое представление.** Диаграмма, в которую включены МЕДИЦИНСКИЕ ПРИБОРЫ, другие системы и основные интерфейсы (как для человека, так и для машин). Это представление должно четко очерчивать границы МЕДИЦИНСКОЙ ИТ СЕТИ.

- **Представление уровня данных.** Диаграмма, демонстрирующая поток клинических данных, циркулирующих в МЕДИЦИНСКОЙ ИТ СЕТИ, например диаграмма потока данных.

- **Представление уровня ПРОЦЕССОВ.** Это представление может быть списком услуг, предоставляемых МЕДИЦИНСКОЙ ИТ СЕТЬЮ и связанными с ними МЕДИЦИНСКИМИ ПРИБОРАМИ. Услугой может быть результат диагностического лабораторного исследования. Важно иметь понимания ролей и задач, связанных с предоставляемыми услугами.

МЕДИЦИНСКАЯ ИТ СЕТЬ, рассматриваемая с точки зрения физического представления, попадет в одну из следующих категорий:

a) **Независимая** (Standalone). Классическая небольшая профильная МЕДИЦИНСКАЯ ИТ СЕТЬ с одной системой/небольшим количеством пользователей, которую, как правило, будет использовать небольшая ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ. В данную категорию также войдет тип небольшой специализированной МЕДИЦИНСКОЙ ИТ СЕТИ, которая может встречаться в узкоспециализированных отделениях крупных ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ. Такие сети изолированы от основной сети (например, размещены в лаборатории диагностических исследований).

b) **Совместная** (Collaborative). Сеть, в которой две или несколько ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ соединяют свои относительно простые и дискретные независимые системы в рамках более широкого интероперабельного контекста. Рекомендуется документально оформлять детали совмещения сетей в дополнение к деталям для простых независимых систем.

c) **Централизованная** (Centralised). Типичная централизованная МЕДИЦИНСКАЯ ИТ СЕТЬ может встречаться в больших больницах, в которых ИТ отдел занимается управлением сетью и службами, которые связаны с множеством клинических назначений. Сами назначения имеют ориентированные на них сетевые службы, предоставляемые центральной сетью, и обладают доступом к приложениям, которые предоставляют поддержку для административных и потенциально клинических областей предоставления услуг. Эти сети будут неизменно взаимодействовать с МЕДИЦИНСКИМИ ПРИБОРАМИ в той или иной степени. Уровень сложности такой МЕДИЦИНСКОЙ ИТ СЕТИ на порядок выше, чем уровень сети в небольшой ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Следует тщательно подходить к разделению клинических предметных областей сети, так как в случае централизованной сети, некоторые общие компоненты МЕДИЦИНСКОЙ ИТ СЕТИ будут совместно использоваться различными МЕДИЦИНСКИМИ ИТ СЕТЯМИ.

Примеры таких конфигураций представлены в приложении А.

Целью создания физического представления для вышеописанных конфигураций является обеспечение получения точной модели МЕДИЦИНСКОЙ ИТ СЕТИ на основе ОЦЕНКИ РИСКА, в особенности для соединенных систем и связанных с ними интерфейсов. И хотя характер конфигурации не изменяет базовый ПРОЦЕСС ОЦЕНКИ РИСКА, эта конфигурация будет полезной при установлении возможных ОПАСНОСТЕЙ и ОПАСНЫХ СИТУАЦИЙ.

5.4.2.2 Учитываемые факторы небольшой ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ

Для небольшой организации наихудшей угрозой является перегрузка количеством информации, которую необходимо упорядочивать. Поэтому на данном этапе важно избегать чрезмерного усложнения. Есть несколько простых вопросов, которые предназначены помочь небольшой организации получить представление о МЕДИЦИНСКОЙ ИТ СЕТИ:

- **Имеется ли у организации реестр основных средств? Насколько он точен?** Реестр основных средств является полезной исходной информацией для идентификации оборудования МЕДИЦИНСКОЙ ИТ СЕТИ. Но он должен содержать точную информацию. Если это не так, то велик шанс того, что большая часть МЕДИЦИНСКОЙ ИТ СЕТИ не будет охвачена ОЦЕНКОЙ РИСКА и тем самым подвергнет риску БЕЗОПАСНОСТЬ всей МЕДИЦИНСКОЙ ИТ СЕТИ.

- **Может ли организация добавить в реестр основных средств пометки, указывающие на МЕДИЦИНСКИЕ ПРИБОРЫ?** Если это возможно, следует отмечать те МЕДИЦИНСКИЕ ПРИБОРЫ в регистре средств, которые образуют часть МЕДИЦИНСКОЙ ИТ СЕТИ. Это упростит сопровождение и поддержку процесса оценки влияний изменений на МЕДИЦИНСКУЮ ИТ СЕТЬ.

- **Какие МЕДИЦИНСКИЕ ПРИБОРЫ используются в ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ?** МЕДИЦИНСКИЕ ПРИБОРЫ помечаются, как таковые, и должны предоставляться производителем вместе с сертификатом соответствия и СОПРОВОДИТЕЛЬНЫМ ДОКУМЕНТОМ. Имеет ли организация эти документы? Если у организации возникают проблемы, связанные с этой документацией, то ее можно обнаружить на сайтах поставщиков. В дополнение к этому, регулирующие органы располагают базами данных, содержащими информацию о подтверждении соответствия действующих систем.

- **Какие интерфейсы установлены между МЕДИЦИНСКИМ ПРИБОРОМ и более широкой(ими) системой(ами) организации?** Перед тем как перейти к ОЦЕНКЕ РИСКА, организации необходимо сформировать четкое представление об информации, которой обмениваются МЕДИЦИНСКИЕ ПРИБОРЫ. Очевидно, что основанием для данной части работы служит понимание того, что является и что не является МЕДИЦИНСКИМ ПРИБОРОМ.

5.4.2.3 Учитываемые факторы больших ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ

Перед тем как начать выполнение данной задачи в большой организации, важно установить различие между регулируемым автономным МЕДИЦИНСКИМ ПРИБОРОМ и регулируемым МЕДИЦИНСКИМ ПРИБОРОМ, который взаимодействует с другими системами через сеть. Важно помнить, что основное внимание в МЭК 80001-1 уделяется МЕДИЦИНСКОЙ ИТ СЕТИ, и, хотя хорошей практикой для ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ является наличие надежных ПРОЦЕССОВ и средств для управления автономными МЕДИЦИНСКИМИ ПРИБОРАМИ, предметом настоящего стандарта является проблема реализации МЭК 80001-1.

Формирование конфигурации сети в большой организации является сложной задачей, и поэтому кроме факторов, указанных выше для небольших организаций, необходимо учесть следующие факторы:

- **Каким предложением о клинической функции может помочь специалист для установления точной картины?** Хороший способ получения информации о МЕДИЦИНСКИХ ПРИБОРАХ в отделении рентгенологии задать этот вопрос рентгенологам и другому персоналу отделения, ежедневно использующим систему. Чтобы получить правильное представление о регламенте, приобрести знания о рабочих методах и оборудовании, используемом специалистами пользователями МЕДИЦИНСКИХ ПРИБОРОВ и систем, следует проконсультироваться с этими пользователями в рамках каждой предметной области, охваченной МЕДИЦИНСКОЙ ИТ СЕТЬЮ.

- **Какую помощь могут предложить технические функциональные отделы (ИТ и биомедицинской инженерии)?** Многие виды отказа МЕДИЦИНСКОЙ ИТ СЕТИ имеют технический характер и требуют экспертных знаний технических функций, как для идентификации видов отказа, так и для оценивания вероятности возникновения отказа.

- **Какую помощь может предложить функциональный отдел МЕНЕДЖМЕНТА РИСКА?** Хотя интерпретация понятия РИСКА немного отличается по отношению к количественному описанию ОПАСНОСТЕЙ и тому понятию, которое распространено среди менеджеров проекта, персонал, ознакомленный с подходом, основанном на РИСКЕ, может способствовать определению РИСКОВ, их документальному оформлению и управлению ими.

- **Какую помощь может предоставить команда, которая руководит клинической деятельностью ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ?** ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна располагать командой, обеспечивающей руководство и соответствие клинической практики и обладающей хорошим представлением о нормативно-правовой базе ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

- **Может ли организация разделить имеющиеся у нее МЕДИЦИНСКИЕ ПРИБОРЫ на соответствующие клинические предметные области?** Важно обеспечить получение организацией правильного представления о клиническом контексте, в котором действует МЕДИЦИНСКИЙ ПРИБОР. Конфигурация МЕДИЦИНСКОЙ ИТ СЕТИ за счет упрощения получит преимущество, если МЕДИЦИНСКАЯ ИТ СЕТЬ может быть разбита на соответствующие группы взаимосвязанных клинических предметных областей.

- **Присутствуют ли в организации обычные МЕДИЦИНСКИЕ ПРИБОРЫ, взаимодействующие между собой в ее рамках?** При сборе информации о конфигурации следует идентифицировать МЕДИЦИНСКИЕ ПРИБОРЫ, работающие в нескольких разных клинических условиях. Анализ МЕДИЦИНСКИХ ПРИБОРОВ в рамках ИТ СЕТИ может пригодиться в оценке других ИТ СЕТЕЙ, содержащих те же МЕДИЦИНСКИЕ ПРИБОРЫ.

5.4.3 Статус разработки МЕДИЦИНСКОЙ ИТ СЕТИ

Важно, чтобы при ОЦЕНКЕ РИСКА использовалась информация, корректно отражающая текущий статус МЕДИЦИНСКОЙ ИТ СЕТИ, так как это значительно влияет на метод, применяющийся для осла-

бления РИСКОВ. При определении статуса разработки МЕДИЦИНСКОЙ ИТ СЕТИ следует учитывать следующую классификацию:

- **Существующая сеть.** Стабильная и неизменяемая базовая МЕДИЦИНСКАЯ ИТ СЕТЬ. Целью ОЦЕНКИ РИСКА будет идентификация любых присущих ей РИСКОВ и оценка ЭФФЕКТИВНОСТИ любых широко распространенных средств управления или средств ослабления, связанных с развертыванием и функционированием МЕДИЦИНСКОЙ ИТ СЕТИ.

- **Модифицируемая сеть.** Стабильная базовая МЕДИЦИНСКАЯ ИТ СЕТЬ, в которую вносится одно или несколько изменений. Целью оценки является идентификация влияния изменений на сеть и обследование их влияния на существующие средства УПРАВЛЕНИЯ РИСКОМ.

- **Разрабатываемая сеть.** Новая или существующая МЕДИЦИНСКАЯ ИТ СЕТЬ, содержащая в основном новые компоненты. Целью оценки является идентификация любых возможных РИСКОВ, связанных с МЕДИЦИНСКОЙ ИТ СЕТЬЮ, находящейся в разработке, и обеспечение реализации достаточных средств управления и ослабления РИСКОВ для поддержания их внутри установленных уровней критериев допустимости.

ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ необходимо учесть статус разработки МЕДИЦИНСКОЙ ИТ СЕТИ и прийти к обоснованному заключению о том, какой статус соответствует сети в организации, а также соответственным образом определиться с методом ОЦЕНКИ РИСКА.

5.4.4 Идентификация производителя

После того как ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ количественно описала свои МЕДИЦИНСКИЕ ИТ СЕТИ, необходимо идентифицировать производителей различных компонентов. Выполнение этого действия обеспечит идентификацию всех производителей данных компонентов.

Ответственности производителей и поставщиков определены в подразделах 3.5 и 3.6 МЭК 80001-1:2010 соответственно.

Факторы, которые следует учесть организациям любых размеров:

- Является ли производитель и поставщик одним и тем же лицом?

- Обеспечивают ли ПРОЦЕССЫ закупки ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ получение доступа к любой сопроводительной технической информации? Она может поступать как от производителя, так и от поставщика, если они являются разными организациями.

- Кто может запрашивать получение информации у производителя/поставщика?

- Кто может поручить (или принудить, если необходимо) производителю/поставщику принять меры для ослабления РИСКА?

- Какова сложность цепочки поставок, например используются ли субпоставщики?

5.4.5 Поддержка от внешних отделов ИТ и биомедицинской инженерии

Важно, чтобы ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ обеспечивала формирование грамотных СОГЛАШЕНИЙ об ОТВЕТСТВЕННОСТИ с внешними поддерживающими организациями для обеспечения достаточной поддержки и ослабления любых идентифицированных РИСКОВ, связанных с компонентами МЕДИЦИНСКОЙ ИТ СЕТИ (см. раздел 6). В настоящем пункте ИТ относится скорее к базовым сетевым компонентам, чем к МЕДИЦИНСКИМ ПРИБОРАМ.

Чтобы прояснить, какая модель поддержки используется, следует рассмотреть, как осуществляется и поддерживается обслуживание. Для этого ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ потребуется ответить на следующие вопросы:

- Какие организации несут ответственность за предоставление поддержки?

- Были ли заключены контракты на поддержку с каждой из этих организаций?

- Четко ли указаны предоставляемые каждым контрактом услуги для поддержки сети и ее компонентов (например, серия базовых задач поддержки, таких как, восстановление забытых паролей для обеспечения новых стационарных компьютеров)?

- Действительно ли поддержка достаточна для текущих и возможно будущих ее потребностей?

6 СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ

В подразделе 3.2 МЭК 80001-1:2010 указано, что «Ответственность за МЕНЕДЖМЕНТ РИСКА МЕДИЦИНСКОЙ ИТ СЕТИ не выходит за рамки ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ». Для выполнения этого обязательства ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ потребуется своевременное получение информации от производителей, с которыми она связана. Доступность подобных материалов может обеспечиваться за счет СОГЛАШЕНИЙ ОБ ОТВЕТСТВЕННОСТИ.

Приложение А
(справочное)

Примеры конфигураций МЕДИЦИНСКИХ ИТ СЕТЕЙ

А.1 Общие положения

В данном приложение представлено чётыре примера конфигураций МЕДИЦИНСКОЙ ИТ СЕТИ в качестве иллюстраций к 5.4.2. Первый пример (А.2) представляет конфигурации системы 1a и 1b по таблице С.1 МЭК 80001-1. Последующие три примера (А.3—А.5) являются вариантами системной конфигурации 2b по таблице С.1 МЭК 80001-1:2010, сложность которых возрастает.

На представленных ниже диаграммах МЕДИЦИНСКИЙ ПРИБОР, подсоединяемый к ИТ СЕТИ общего назначения, показан в виде набора оборудования, существующего в своей собственной конкретной сети. Подобным же образом МЕДИЦИНСКАЯ ИТ СЕТЬ может состоять из одного или нескольких дискретных МЕДИЦИНСКИХ ПРИБОРОВ, непосредственно соединенных с ИТ СЕТЬЮ общего назначения.

А.2 Конфигурация изолированной сети

Пример, представленный на рисунке А.1, аналогичен системной конфигурации 1, описанной в таблице С.1 МЭК 80001-1:2010. Так как в данном примере явно не указано, поступило ли оборудование от одного или нескольких производителей МЕДИЦИНСКИХ ПРИБОРОВ, данная интерпретация применима как к 1a, так и к 1b.

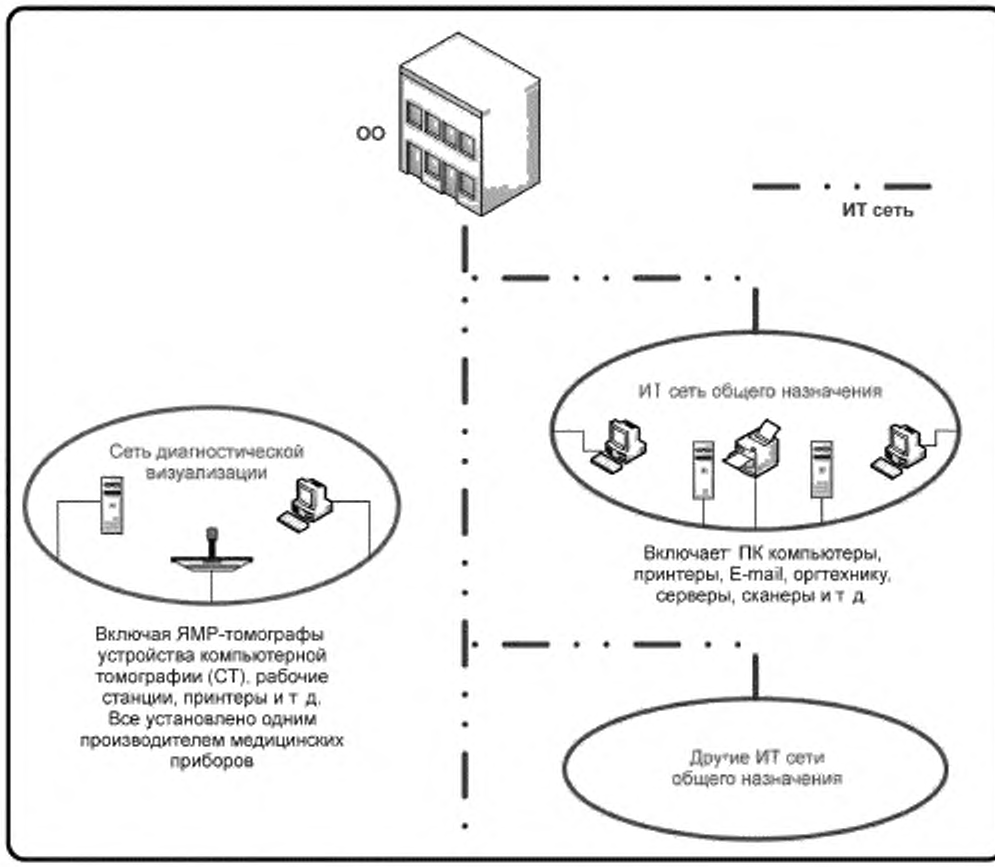

Рисунок А.1 — Изолированная МЕДИЦИНСКАЯ ИТ СЕТЬ, не входящая в область применения МЭК 80001-1

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ является поставщиком рентгенологических услуг для некоторого малочисленного сообщества. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ представляет из себя одно предприятие и не связана ни с какими другими ОТВЕТСТВЕННЫМИ ОРГАНИЗАЦИЯМИ. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ располагает двумя разделенными сетями, функционирующими внутри организации. Первая является ИТ сетью общего назначения, использующейся для решения повседневных бизнес-применений. Вторая сеть предназначена для МЕДИЦИНСКИХ ПРИБОРОВ и содержит оборудование для диагностической визуализации, которое было установлено одним производителем МЕДИЦИНСКИХ ПРИБОРОВ. Так как эти сети независимы друг от друга, данная конфигурация не входит в область применения МЭК 80001-1.

А.3 Независимая МЕДИЦИНСКАЯ ИТ СЕТЬ

Пример, представленный на рисунке А.2, аналогичен системной конфигурации 2b, описанной в таблице С.1 МЭК 80001-1:2010.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ является поставщиком рентгенологических услуг для некоторого малочисленного сообщества. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ представляет из себя одно предприятие и не связана ни с какими другими ОТВЕТСТВЕННЫМИ ОРГАНИЗАЦИЯМИ. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ располагает двумя сетями, функционирующими внутри организации. Первая является ИТ сетью общего назначения, использующейся для решения повседневных бизнес-применений. Вторая сеть предназначена для МЕДИЦИНСКИХ ПРИБОРОВ и содержит оборудование для диагностической визуализации, которое было приобретено у производителей МЕДИЦИНСКИХ ПРИБОРОВ. Эти две сети были соединены вместе для образования МЕДИЦИНСКОЙ ИТ СЕТИ. МЕДИЦИНСКАЯ ИТ СЕТЬ обычно хранит рентгенологические изображения на сервере, предоставляемом ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ. Хранящиеся на нем рентгенологические изображение могут быть извлечены и распространены посредством ИТ сети общего назначения.

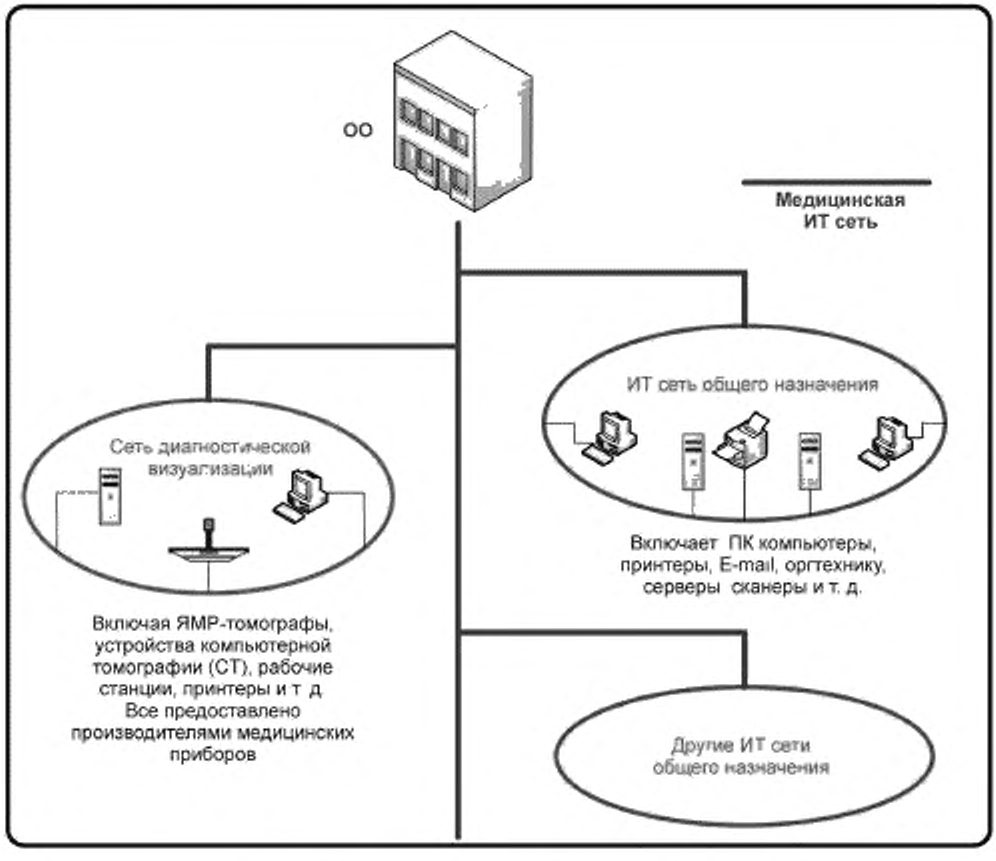

Рисунок А.2 — Изолированная МЕДИЦИНСКАЯ ИТ СЕТЬ

А.4 Совместная МЕДИЦИНСКАЯ ИТ СЕТЬ

Пример, представленный на рисунке А.3, является расширением системной конфигурации 2b, описанной в таблице С.1 МЭК 80001-1:2010, и включает в себя взаимосвязь МЕДИЦИНСКИХ ИТ СЕТЕЙ, созданных на территории двух организаций.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ является поставщиком рентгенологических услуг для некоторого малочисленного сообщества, включающего два отдельных учреждения. Каждое учреждение располагает МЕДИЦИНСКОЙ ИТ СЕТЬЮ, соответствующей конфигурации, определенной в А.3. В данном примере две такие сети соединены вместе с помощью виртуальной частной сети (VPN).

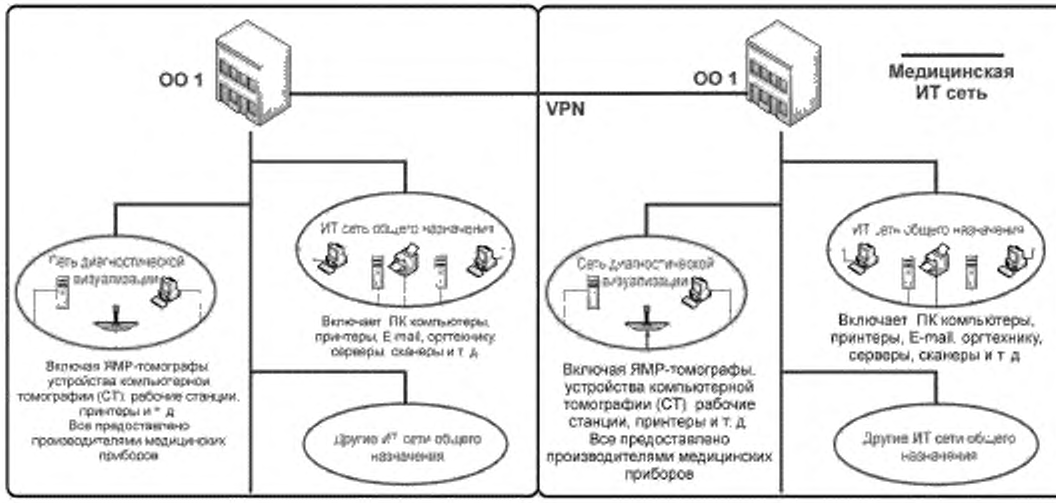

Рисунок А.3 — Совместная МЕДИЦИНСКАЯ ИТ СЕТЬ

А.5 Централизованная МЕДИЦИНСКАЯ ИТ СЕТЬ

Пример, представленный на рисунке А.3, является расширением системной конфигурации 2b, описанной в таблице С.1 МЭК 80001-1:2010, и включает в себя взаимосвязь множества сетей МЕДИЦИНСКИХ ПРИБОРОВ, расположенных в одной ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ является больницей неотложной помощи, предоставляющей множество разных услуг многочисленному сообществу таких, как диагностическая визуализация и патологические исследования. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ располагает множеством МЕДИЦИНСКИХ ПРИБОРОВ, функционирующих в отделенных (изолированных) сетях, которые были приобретены и установлены индивидуальными производителями МЕДИЦИНСКИХ ПРИБОРОВ. Тем не менее, данные сети соединены с одной МЕДИЦИНСКОЙ ИТ СЕТЬЮ, находящейся внутри ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

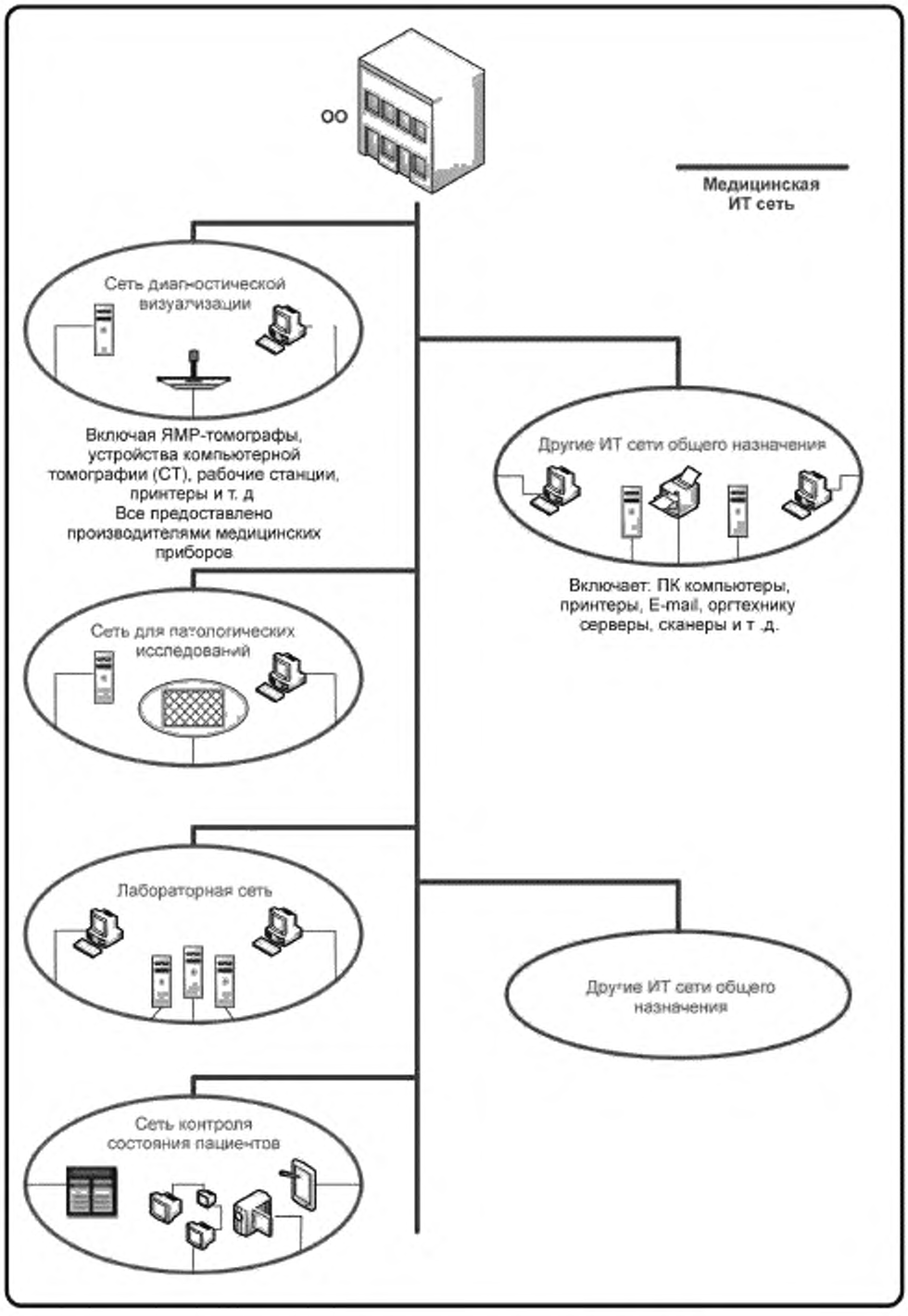

Рисунок А.4 — Централизованная МЕДИЦИНСКАЯ ИТ СЕТЬ

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 80001-1:2010	—	*
* Соответствующий национальный стандарт отсутствует.		

Библиография

[1] IEC 80001-2-1:2012 Application of risk management for IT-networks incorporating medical devices — Part 2-1: Step-by-step risk management of medical IT-networks — Practical applications and examples

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, информационная безопасность, менеджмент рисков, информационно-вычислительные сети, медицинские приборы

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 02.11.2018. Подписано в печать 19.11.2018 Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,51.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

gost.e-ecolog.ru