ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р МЭК 80001-1— 2015

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 1

Роли, ответственности и действия

IEC 80001-1:2010
Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities
(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 аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии России от 28 декабря 2015 г. № 2222-ст

4 Настоящий стандарт идентичен международному стандарту МЭК 80001-1:2010 «Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 1. Роли, ответственности и действия» (IEC 80001-1:2010 «Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (подраздел 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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, 2016

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

Содержание

1 Область применения ... 1
2 Термины и определения ... 2
3 Роли и ответственности ... 5
3.1 Общие положения ... 5
3.2 ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ ... 5
3.3 Ответственность ВЫСШЕГО РУКОВОДСТВА ... 5
3.4 СПЕЦИАЛИСТ ПО УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ ... 7
3.5 Производители МЕДИЦИНСКИХ ПРИБОРОВ ... 8
3.6 Поставщики прочих информационных технологий ... 9
4 МЕНЕДЖМЕНТ РИСКОВ в жизненном цикле МЕДИЦИНСКИХ ИТ-СЕТЕЙ ... 10
4.1 Обзор ... 10
4.2 МЕНЕДЖМЕНТ РИСКОВ, осуществляемый ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ ... 12
4.3 Планирование и документальное оформление МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ ... 12
4.4 МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ ... 15
4.5 УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ ... 17
4.6 МЕНЕДЖМЕНТ РИСКОВ в действующей сети ... 19
5 Управление документацией ... 20
5.1 Процедура управления документацией ... 20
5.2 ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ ... 20
Приложение А (справочное) Обоснование ... 21
Приложение В (справочное) Обзор отношений при реализации МЕНЕДЖМЕНТА РИСКОВ ... 24
Приложение С (справочное) Об области применения настоящего стандарта ... 25
Приложение D (справочное) Связь с [10] ... 28
Библиография ... 32

Введение

Все большее число МЕДИЦИНСКИХ ПРИБОРОВ проектируется для электронного обмена данными с другим оборудованием пользователя, включая также и различные МЕДИЦИНСКИЕ ПРИБОРЫ. Обмен подобной информацией осуществляется через информационную сеть (ИТ-СЕТЬ), предназначенной для передачи данных более общего характера.

В то же время ИТ-СЕТИ становятся все более востребованными для формирования информационной среды клиники и используются для передачи разнообразной информации: от жизненно-важных данных о пациенте, требующих немедленной передачи и ответа, до информации об общей деятельности компании и электронной почты с возможно вредоносным содержанием (например, вирусами).

Во многих юрисдикциях проектирование и производство МЕДИЦИНСКИХ ПРИБОРОВ подчиняется техническим регламентам и стандартам, признаваемым регулирующими государственными органами, которые традиционно уделяют особое внимание производителям МЕДИЦИНСКИХ ПРИБОРОВ и требуют, чтобы МЕДИЦИНСКИЕ ПРИБОРЫ соответствовали их конструктивным характеристикам, а ПРОЦЕСС проектирования и изготовления МЕДИЦИНСКИХ ПРИБОРОВ был документально оформлен. МЕДИЦИНСКИЕ ПРИБОРЫ не могут быть выпущены в продажу в этих юрисдикциях без подтверждения соответствия данным требованиям.

Использование МЕДИЦИНСКИХ ПРИБОРОВ персоналом медицинского учреждения также подчиняется техническим регламентам. Лица из персонала медицинского учреждения, использующие МЕДИЦИНСКИЕ ПРИБОРЫ, должны быть соответственно подготовлены и квалифицированы, а также они должны уделять наибольшее внимание выполнению определенных ПРОЦЕССОВ, специально разработанных для защиты пациентов от недопустимого РИСКА.

В то же время, включение МЕДИЦИНСКИХ ПРИБОРОВ в ИТ-СЕТИ клиники является наименее регулируемой областью деятельности. В соответствии с [1] если предполагается подключение МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ, то производители МЕДИЦИНСКИХ ПРИБОРОВ должны включать в СОПРОВОДИТЕЛЬНЫЕ ДОКУМЕНТЫ всю необходимую информацию. Существуют также общие стандарты по информационным технологиям, включающие планирование, проектирование и обслуживание ИТ-СЕТЕЙ, например [9]. Тем не менее до публикации настоящего стандарта ни один из стандартов не затрагивал вопрос о том, как МЕДИЦИНСКИЕ ПРИБОРЫ могут быть подключены к ИТ-СЕТЯМ, включая ИТ-СЕТИ общего назначения, для достижения ИНТЕРОПЕРАБЕЛЬНОСТИ без ущерба для организации и предоставления медицинских услуг, осуществляющихся с обеспечением БЕЗОПАСНОСТИ, ЭФФЕКТИВНОСТИ, а также ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ.

Существует ряд возможных проблем, связанных с подключением МЕДИЦИНСКИХ ПРИБОРОВ в ИТ-СЕТИ:

- не рассматривается РИСК от применения ИТ-СЕТЕЙ при оценке уровня РИСКА клиники;
- отсутствует поддержка производителями МЕДИЦИНСКОГО ПРИБОРА процесса подключения их изделия к ИТ-СЕТИ (например, недоступны или недостаточно надежны данные, предоставляемые производителем ОПЕРАТОРУ ИТ-СЕТИ);
- МЕДИЦИНСКИЕ ПРИБОРЫ работают неправильно или частично выполняют свои функции (например, из-за несовместимости или ненадлежащей конфигурации) в результате их объединения с другим оборудованием в одной ИТ-СЕТИ;
- МЕДИЦИНСКИЕ ПРИБОРЫ работают неправильно вследствие объединения ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МЕДИЦИНСКИХ ПРИБОРОВ и других приложений (например, открытых систем обмена электронной почтой или компьютерных игр) в одной ИТ-СЕТИ;
- отсутствие у многих МЕДИЦИНСКИХ ПРИБОРОВ управления безопасностью;
- противоречие между необходимостью строгого управления изменениями в МЕДИЦИНСКИХ ПРИБОРАХ и необходимостью быстрой реакции на угрозу кибератаки.

Если эти проблемы появляются, то они вызывают непредвиденные последствия. Настоящий стандарт предназначен для ОТВЕТСТВЕННЫХ ОРГАНИЗАЦИЙ, производителей МЕДИЦИНСКИХ ПРИБОРОВ и поставщиков других информационных технологий.

Положения нормативных и справочных разделов настоящего стандарта основаны на следующих принципах:

- Подключение или отключение МЕДИЦИНСКОГО ПРИБОРА или других компонентов к ИТ-СЕТИ должно выполняться в соответствии с предварительно выполненным проектом; проектирование может быть выполнено без участия производителя МЕДИЦИНСКОГО ПРИБОРА.

- Во избежание неприемлемых РИСКОВ, включая возможный РИСК для пациентов из-за подключения МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ, до такого подключения, а также для любых изменений в ходе всего жизненного цикла формируемой МЕДИЦИНСКОЙ ИТ-СЕТИ должен быть реализован МЕНЕДЖМЕНТ РИСКОВ. При определении допустимого РИСКА необходимо учитывать много факторов, таких как ответственность по возмещению ущерба, стоимость, а также влияние на выполняемую целевую задачу кроме требований, описанных в настоящем стандарте.

- Помимо подключения МЕДИЦИНСКИХ ПРИБОРОВ также необходимо уделить внимание вопросам демонтажа, обслуживания, изменения или модификации оборудования, его элементов и компонентов.

- Производитель МЕДИЦИНСКОГО ПРИБОРА несет ответственность за МЕНЕДЖМЕНТ РИСКОВ МЕДИЦИНСКОГО ПРИБОРА в процессе его проектирования, разработки и изготовления. Настоящий стандарт не рассматривает ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ для МЕДИЦИНСКОГО ПРИБОРА.

- От производителя МЕДИЦИНСКОГО ПРИБОРА, предназначенного для подключения к ИТ-СЕТИ, может потребоваться информация о МЕДИЦИНСКОМ ПРИБОРЕ, необходимая ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ для осуществления МЕНЕДЖМЕНТА РИСКОВ в соответствии с настоящим стандартом. Такая информация может содержаться в являющихся частью СОПРОВОДИТЕЛЬНЫХ ДОКУМЕНТОВ инструкциях, специально предназначенных для лиц, выполняющих подключение МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ.

- Такие СОПРОВОДИТЕЛЬНЫЕ ДОКУМЕНТЫ должны содержать инструкции по подключению МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТИ, по передаче данных МЕДИЦИНСКИХ ПРИБОРОВ через ИТ-СЕТЬ и о минимальных характеристиках ИТ-СЕТИ, необходимых для ПРЕДНАЗНАЧЕННОГО ИСПОЛЬЗОВАНИЯ МЕДИЦИНСКОГО ПРИБОРА, включенного в ИТ-СЕТЬ. СОПРОВОДИТЕЛЬНЫЕ ДОКУМЕНТЫ должны предупреждать о возможных опасных ситуациях, связанных с отказом или сбоями в ИТ-СЕТИ, а также о неправильном соединении в ИТ-СЕТИ или об информации, передаваемой через ИТ-СЕТЬ.

- СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ могут устанавливать роли и ответственности лиц, занимающихся подключением МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ, устанавливать все аспекты жизненного цикла создаваемой МЕДИЦИНСКОЙ ИТ-СЕТИ и все действия, которые формируют данную стадию жизненного цикла.

- ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ необходимо назначить конкретному лицу соответствующие роли, определенные в настоящем стандарте. Настоящий стандарт определяет ответственности для этих ролей. Наиболее важной ролью является роль СПЕЦИАЛИСТА ПО УПРАВЛЕНИЮ РИСКАМИ МЕДИЦИНСКОЙ ИТ-СЕТИ. Данная роль может быть назначена одному из членов ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ или внешнему подрядчику.

- СПЕЦИАЛИСТ ПО УПРАВЛЕНИЮ РИСКАМИ МЕДЦИНСКОЙ ИТ-СЕТИ несет ответственность за включение процедуры МЕНЕДЖМЕНТА РИСКОВ в ПРОЦЕССЫ:

- планирования и проектирования новых подключений МЕДИЦИНСКИХ ПРИБОРОВ в сеть или внесения изменений в эти подключения;

- ввода МЕДИЦИНСКОЙ ИТ-СЕТИ в эксплуатацию и последующего использования МЕДИЦИНСКОЙ ИТ-СЕТИ; и

- УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и управления изменениями ИТ-СЕТИ на протяжении всего жизненного цикла ИТ-СЕТИ.

- МЕНЕДЖМЕНТ РИСКОВ следует применять для обеспечения следующих ОСНОВНЫХ СВОЙСТВ для ИТ-СЕТИ, включающей в себя МЕДИЦИНСКИЙ ПРИБОР:

- БЕЗОПАСНОСТЬ (отсутствие неприемлемого РИСКА физической травмы, или ущерба здоровью людей, или ущерба имуществу, или окружающей среде);

- ЭФФЕКТИВНОСТЬ (способность достигать желаемых результатов по отношению к пациенту и ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ); и

- ЗАЩИТА ДАННЫХ И СИСТЕМЫ [рабочее состояние МЕДИЦИНСКОЙ ИТ-СЕТИ, в котором информационные средства (данные и системы) в достаточной степени защищены от нарушения конфиденциальности, полноты и доступа].

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 1

Роли, ответственности и действия

Health informatics. Risk management for IT-networks incorporating medical devices.
Part 1. Roles, responsibilities and activities

Дата введения — 2016—11—01

1 Область применения

Признавая тот факт, что МЕДИЦИНСКИЕ ПРИБОРЫ подключают к ИТ-СЕТЯМ для достижения желаемых преимуществ (например, ИНТЕРОПЕРАБЕЛЬНОСТИ), настоящий стандарт определяет роли, ответственности и действия, необходимые для МЕНЕДЖМЕНТА РИСКОВ в ИТ-СЕТЯХ, содержащих МЕДИЦИНСКИЕ ПРИБОРЫ, для обеспечения БЕЗОПАСНОСТИ, ЭФФЕКТИВНОСТИ и ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ (ОСНОВНЫХ СВОЙСТВ). Настоящий стандарт не устанавливает допустимые уровни РИСКА.

Примечание — Действия по МЕНЕДЖМЕНТУ РИСКОВ, описанные в настоящем стандарте, рассмотрены в процессах, описанных в [4]. Связь между [4] и настоящим стандартом представлена в приложении А.

Настоящий стандарт применяется после того, как МЕДИЦИНСКИЙ ПРИБОР был приобретен ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ и планируется его подключение в ИТ-СЕТЬ.

Примечание — Настоящий стандарт не охватывает МЕНЕДЖМЕНТ РИСКОВ МЕДИЦИНСКОГО ПРИБОРА до выпуска его в продажу.

Настоящий стандарт применяется на всем жизненном цикле ИТ-СЕТЕЙ, содержащих МЕДИЦИНСКИЕ ПРИБОРЫ.

Примечание — Действия по управлению жизненным циклом, описанные в настоящем стандарте, очень похожи на действия, описанные в [10]. Связь между [10] и настоящим стандартом представлена в приложении D.

Настоящий стандарт применяется в тех случаях, когда нет отдельного производителя МЕДИЦИНСКИХ ПРИБОРОВ, принимающего на себя ответственность за обеспечение ОСНОВНЫХ СВОЙСТВ ИТ-СЕТИ с МЕДИЦИНСКИМ ПРИБОРОМ.

Примечания

1 Если отдельный производитель специфицирует весь МЕДИЦИНСКИЙ ПРИБОР, включающий в себя сеть, то установка или сборка МЕДИЦИНСКОГО ПРИБОРА, выполняемая в соответствии с СОПРОВОДИТЕЛЬНЫМИ ДОКУМЕНТАМИ производителя, не подчиняется положениям настоящего стандарта независимо от того, кто устанавливает или собирает МЕДИЦИНСКИЙ ПРИБОР.

2 Если отдельный производитель специфицирует весь МЕДИЦИНСКИЙ ПРИБОР, включающий в себя сеть, то дополнения к данному МЕДИЦИНСКОМУ ПРИБОРУ или модификации его конфигурации, кроме тех, что установлены производителем, подчиняются положениям настоящего стандарта.

Настоящий стандарт применяется к ОТВЕТСТВЕННЫМ ОРГАНИЗАЦИЯМ, производителям МЕДИЦИНСКИХ ПРИБОРОВ и поставщикам других информационных технологий для МЕНЕДЖМЕНТА РИСКОВ в ИТ-СЕТИ, содержащей МЕДИЦИНСКИЕ ПРИБОРЫ, в соответствии со спецификацией, определенной ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ.

Издание официальное

Настоящий стандарт не применим для персонального использования, в котором пациент, ОПЕРАТОР и ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ являются одним и тем же лицом.

Примечание — Если МЕДИЦИНСКИЙ ПРИБОР используется на дому под контролем или руководством поставщика, то этот поставщик считается ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ. Персональное использование, при котором пациент приобретает и использует МЕДИЦИНСКИЙ ПРИБОР без контроля или руководства поставщика, не входит в область применения настоящего стандарта.

Настоящий стандарт не рассматривает требования законов или актов государственого регулирования.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **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, определение 3.4.

2.2 **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 КОНФИГУРАЦИЕЙ.

Примечание — Адаптировано из ИСО/МЭК 20000-1, 9.2 (управление изменениями) и 10.1 (управление версиями).

2.3 **РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ** (CHANGE PERMIT): Результат ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ, представленный в виде документа, позволяющего реализовать сформированное изменение или тип изменения без дополнительных действий по МЕНЕДЖМЕНТУ РИСКОВ в рамках установленных ограничений.

2.4 **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, 9.1.

2.5 **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.

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

2.7 **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, 8.2 (управление инцидентами) и 8.3 (управление проблемами).

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

Примечание — Адаптировано из ИСО 14971, определение 2.2.

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

[ИСО 14971:2007, определение 2.3]

2.10 **ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ** (INTENDED USE): Применение изделия, ПРОЦЕССА или службы в соответствии с техническими условиями, инструкциями и информацией, предоставленной производителем.

[ИСО 14971: 2007, определение 2.5]

2.11 **ИНТЕРОПЕРАБЕЛЬНОСТЬ** (INTEROPERABILITY): Свойство, позволяющее разнообразным системам и компонентам работать вместе для достижения установленной цели.

2.12 **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, определение 3.1.1.

2 В настоящем стандарте область применения МЕДИЦИНСКОЙ ИТ-СЕТИ определяется ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ на основании того, где в МЕДИЦИНСКОЙ ИТ-СЕТИ располагаются МЕДИЦИНСКИЕ ПРИБОРЫ, а также заданным применением сети. В область применения могут входить ИТ-инфраструктура, медицинское обслуживание на дому и неклинические применения. См. также 4.3.3.

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

2.14 **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 использовать 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 были 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 был разработан.

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

[GHTF SG1/N29R16:2005]

2.15 **ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МЕДИЦИНСКОГО ПРИБОРА** (MEDICAL DEVICE SOFTWARE): Система программного обеспечения, разработанная с целью включения в МЕДИЦИНСКИЙ ПРИБОР или предназначенная для использования как самостоятельный МЕДИЦИНСКИЙ ПРИБОР.

[МЭК 62304:2006, определение 3.12]

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

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

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

[МЭК 60601-1:2005, определение 3.73]

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

[ИСО 14971:2007, определение 2.13]

Примечание — Термин «действия» охватывает и использование ресурсов.

2.20 **ОСТАТОЧНЫЙ РИСК** (RESIDUAL RISK): РИСК, остающийся после выполнения мер по УПРАВЛЕНИЮ РИСКОМ.

[ИСО 14971:2007, определение 2.15]

2.21 **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.

2.22 **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, определение 3.101.

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

[ИСО 14971:2007, определение 2.16]

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

[ИСО 14971:2007, определение 2.17]

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

[ИСО/МЭК руководство 51:1999, определение 3.12]

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

[ИСО 14971:2007, определение 2.19]

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

[ИСО 14971:2007, определение 2.21]

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

[ИСО 14971:2007, определение 2.22]

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

[ИСО 14971:2007, определение 2.23]

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

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

2.31 ВЫСШЕЕ РУКОВОДСТВО (TOP MANAGEMENT). Лицо или группа лиц, осуществляющих направление(я) деятельности и управление ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ, отвечающих за МЕДИЦИНСКУЮ ИТ-СЕТЬ на самом высоком уровне.

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

2.32 ВЕРИФИКАЦИЯ (VERIFICATION): Подтверждение на основе предоставления объективных свидетельств того, что установленные требования были выполнены.

Примечания

1 Термин «верифицирован» используют для обозначения соответствующего статуса.

2 Деятельность по подтверждению может включать:

осуществление альтернативных расчетов;

сравнение спецификации нового проекта с аналогичной спецификацией апробированного проекта;

проведение испытаний и демонстраций; и

анализ документов до их выпуска.

[ИСО 14971:2007, определение 2.28]

3 При проектировании и разработке ВЕРИФИКАЦИЯ охватывает ПРОЦЕСС проверки результатов реализуемых действий для определения соответствия результатов установленным для них требованиям.

3 Роли и ответственности

3.1 Общие положения

Подключение и модификация оборудования или программного обеспечения в МЕДИЦИНСКУЮ ИТ-СЕТЬ должно осуществляться на основе четко определенных ответственностей. Должны быть определены, как минимум, стороны ответственности и требования, идентифицированные в 3.2—3.6.

Для конкретной рассматриваемой МЕДИЦИНСКОЙ ИТ-СЕТИ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна установить и вести ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Вся документация, связанная с требованиями настоящего стандарта к ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, так же как и вся документация о подтверждении этих требований, должна вноситься в ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ. Данный файл должен содержать актуальную информацию об УПРАВЛЕНИИ КОНФИГУРАЦИЕЙ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — Информация об УПРАВЛЕНИИ КОНФИГУРАЦИЕЙ может быть включена в ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ либо в виде подробной документации, либо как ссылка, например, на актуальную базу данных.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

3.2 ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ

Всю ответственность за МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ несет только ОТВЕСТВЕННАЯ ОРГАНИЗАЦИЯ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна быть владельцем ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ, охватывающего планирование, проектирование, установку, соединение приборов, конфигурацию, использование, выполнение, обслуживание и вывод из эксплуатации прибора.

Соответствие проверяют оценкой ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

3.3 Ответственности ВЫСШЕГО РУКОВОДСТВА

При выполнении МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКИХ ИТ-СЕТЕЙ ВЫСШЕЕ РУКОВОДСТВО должно нести ответственность:

a) за установление политики МЕНЕДЖМЕНТА РИСКОВ для подключения МЕДИЦИНСКИХ ПРИБОРОВ;

b) определение политики установления допустимого РИСКА, учитывая соответствующие международные стандарты и национальные или региональные регламенты;

c) предоставление достаточных ресурсов;

d) назначение квалифицированного персонала на должности управления, для проведения работ и выполнения оценки; и

e) анализ результатов действий, выполняемых в процессе МЕНЕДЖМЕНТА РИСКОВ, включая УПРАВЛЕНИЕ СОБЫТИЯМИ (см. 4.6.2), за определенные временные промежутки для обеспечения соответствия актуальным требованиям и эффективности ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ.

Все вышеперечисленное должно быть документально оформлено в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ. ВЫСШЕЕ РУКОВОДСТВО обязано назначить СПЕЦИАЛИСТА по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ, обладающего необходимой квалификацией, знаниями и компетентностью, требующимися для МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКИХ ИТ-СЕТЯХ (см. 3.4);

ВЫСШЕЕ РУКОВОДСТВО должно назначать людей, ответственных за описанные ниже задачи, и следить за тем, чтобы они взаимодействовали со СПЕЦИАЛИСТОМ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ;

f) сбор, анализ, оценку и хранение информации, необходимой для МЕНЕДЖМЕНТА РИСКОВ;

g) управление жизненным циклом МЕДИЦИНСКИХ ПРИБОРОВ, подключенных к ИТ-СЕТЯМ;

h) рассмотрение и установление значения ОСТАТОЧНОГО РИСКА по поручению ВЫСШЕГО РУКОВОДСТВА;

i) обслуживание МЕДИЦИНСКИХ ИТ-СЕТЕЙ; и

j) выбор и закупку МЕДИЦИНСКИХ ПРИБОРОВ.

ВЫСШЕЕ РУКОВОДСТВО должно гарантировать, что в ПРОЦЕССЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКИХ ИТ-СЕТЕЙ участвует подразделение, ответственное:

h) за МЕДИЦИНСКИЕ ИТ-СЕТИ;

i) общую ИТ-деятельность;

m) управление жизненным циклом МЕДИЦИНСКИХ ПРИБОРОВ, подключенных к ИТ-СЕТЯМ.

Пример — Биомедицинская техника, радиологическая техника;

n) использование МЕДИЦИНСКИХ ПРИБОРОВ.

Пример — Опытные пользователи из больничных отделений;

o) обслуживание и техническую поддержку МЕДИЦИНСКИХ ПРИБОРОВ.

Пример — Отдел биомедицинской техники.

ВЫСШЕЕ РУКОВОДСТВО должно гарантировать, что:

p) все инспектирование, эксплуатация, установка и техническое обслуживание МЕДИЦИНСКИХ ИТ-СЕТЕЙ на протяжении жизненного цикла выполняются согласно плану МЕНЕДЖМЕНТА РИСКОВ в соответствии с результатами ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ ИТ-СЕТИ для всех, кто выполняет данные задачи;

q) все стороны, выполняющие инспектирование, эксплуатацию, установку, сервисное обслуживание, выявление неисправностей и техническое обслуживание МЕДИЦИНСКИХ ИТ-СЕТЕЙ в соответствии с данным стандартом, обладают достаточной информацией о своей ответственности, включая ответственности сторон по поддержанию эффективности механизмов УПРАВЛЕНИЯ РИСКОМ.

Примечание — Ответственности ВЫСШЕГО РУКОВОДСТВА изображены на рисунке 1.



Рисунок 1 — Обязанности ВЫСШЕГО РУКОВОДСТВА

Соответствие требованиям настоящего подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

3.4 СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен нести ответственность за управление ПРОЦЕССОМ МЕНЕДЖМЕНТА РИСКОВ.

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен осуществлять инспекцию исполнения ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ для поддержки ОСНОВНЫХ СВОЙСТВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен нести ответственность за следующие задачи МЕНЕДЖМЕНТА РИСКОВ ИТ-СЕТЕЙ с МЕДИЦИНСКИМИ ПРИБОРАМИ:

a) общее управление ПРОЦЕССОМ МЕНЕДЖМЕНТА РИСКОВ;

b) подготовка отчета о ПРОЦЕССЕ МЕНЕДЖМЕНТА РИСКОВ перед ВЫСШИМ РУКОВОДСТВОМ; и

c) управление необходимыми коммуникациями между внутренними и внешними участниками МЕНЕДЖМЕНТА РИСКОВ. Подобными участниками в зависимости от обстоятельств могут быть:

1) производители МЕДИЦИНСКОГО ПРИБОРА;

2) прочие поставщики ИТ-оборудования, программного обеспечения и ИТ-услуг;

3) внутренний отдел ИТ и другие отделы эксплуатации оборудования;

4) пользователи в больнице;

5) отдел технической поддержки, ответственный за МЕДИЦИНСКИЕ ПРИБОРЫ (например, для биомедицинской техники).

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен нести ответственность за выполнение ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ. Она включает, но не ограничивается ответственностью:

d) за сбор всей связанной с РИСКАМИ информации о МЕДИЦИНСКИХ ПРИБОРАХ;

e) планирование подключения МЕДИЦИНСКИХ ПРИБОРОВ в соответствии с инструкциями, предоставленными различными производителями МЕДИЦИНСКИХ ПРИБОРОВ, и политикой ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ;

f) выполнение ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ каждый раз, когда в ИТ-СЕТЬ добавляется МЕДИЦИНСКИЙ ПРИБОР;

g) выполнение ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ каждый раз, когда подключенный к ИТ-СЕТИ МЕДИЦИНСКИЙ ПРИБОР меняется;

h) подтверждение полномочий при запуске в эксплуатацию МЕДИЦИНСКОЙ ИТ-СЕТИ после внесения в нее изменений;

i) информирование ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ о недопустимом РИСКЕ, связанном с МЕДИЦИНСКОЙ ИТ-СЕТЬЮ, и ОПАСНОСТЯХ, возникающих по причине изменений в конфигурации; и

j) контроль всех проектов МЕДИЦИНСКОЙ ИТ-СЕТИ и изменений, вносимых в МЕДИЦИНСКУЮ ИТ-СЕТЬ, за которую несет ответственность СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Данные задачи могут быть делегированы, но СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ МЕДИЦИНСКОЙ ИТ-СЕТИ остается ответственным за обеспечение их надлежащего выполнения.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

3.5 Производители МЕДИЦИНСКИХ ПРИБОРОВ

В соответствии с действующими регламентами, а также связанными с ними стандартами каждый производитель МЕДИЦИНСКИХ ПРИБОРОВ должен предоставить ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ СОПРОВОДИТЕЛЬНЫЕ ДОКУМЕНТЫ, описывающие ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ и содержащие инструкции, необходимые для безопасного и эффективного использования МЕДИЦИНСКОГО ПРИБОРА.

Для МЕДИЦИНСКОГО ПРИБОРА, который может быть подключен к ИТ-СЕТИ, производитель МЕДИЦИНСКОГО ПРИБОРА должен предоставить инструкции по выполнению такого подключения, которые включают, но не ограничиваются следующим:

a) цель подключения МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ;

b) требуемые характеристики ИТ-СЕТИ, к которой подключается МЕДИЦИНСКИЙ ПРИБОР;

c) требуемая конфигурация ИТ-СЕТИ, к которой подключается МЕДИЦИНСКИЙ ПРИБОР;

d) технические спецификации подключения к сети МЕДИЦИНСКОГО ПРИБОРА, включая спецификации по защите информации;

e) предусмотренный информационный поток между МЕДИЦИНСКИМ ПРИБОРОМ и МЕДИЦИНСКОЙ ИТ-СЕТЬЮ, а также другими приборами в МЕДИЦИНСКОЙ ИТ-СЕТИ и если это имеет значение для ОСНОВНЫХ СВОЙСТВ, то предусмотренная маршрутизация в МЕДИЦИНСКОЙ ИТ-СЕТИ; и

f) список опасных ситуаций, возникающих из-за отказов ИТ-СЕТИ обеспечить характеристики, требующиеся для предназначенного подключения МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ.

Соответствие требованиям данного подраздела проверяют путем экспертизы доступных СОПРОВОДИТЕЛЬНЫХ ДОКУМЕНТОВ, предоставленных производителем МЕДИЦИНСКОГО ПРИБОРА, и других инструкций по реализации подобного подключения.

Примечание — В случаях если предоставленный материал не соответствует нуждам ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, занимающейся МЕНЕДЖМЕНТОМ РИСКОВ, может быть предоставлен дополнительный материал в рамках СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна получить СОПРОВОДИТЕЛЬНЫЕ ДОКУМЕНТЫ МЕДИЦИНСКОГО ПРИБОРА, подключенного к МЕДИЦИНСКОЙ ИТ-СЕТИ. Данные документы должны храниться и в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна получить дополнительную документацию по МЕДИЦИНСКОМУ ПРИБОРУ, подключенному к ИТ-СЕТИ, необходимую для МЕНЕДЖМЕНТА РИСКОВ МЕ-

ДИЦИНСКОЙ ИТ-СЕТИ, включая любые известные опасные ситуации, которые должна контролировать ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ. Данные документы должны храниться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ между ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ и производителем МЕДИЦИНСКОГО ПРИБОРА можно использовать для выявления необходимой документации и обмена данной документацией.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

3.6 Поставщики прочих информационных технологий

Поставщики прочих (не для МЕДИЦИНСКИХ ПРИБОРОВ) информационных технологий могут предоставлять:

a) компоненты инфраструктуры;

b) службы инфраструктуры;

c) клиентские приборы, не являющиеся МЕДИЦИНСКИМИ ПРИБОРАМИ;

d) серверы;

e) прикладное программное обеспечение или

f) микропрограммное обеспечение.

В соответствии с действующими регламентами, а также связанными с ними стандартами каждый поставщик прочих информационных технологий (оборудования и/или программного обеспечения) должен предоставить документально оформленную информацию, применимую к предоставляемой им технологии, в следующем составе:

g) технические описания и технические руководства;

h) требующиеся характеристики ИТ-СЕТИ;

i) рекомендованные конфигурации изделия;

j) известные несовместимости и ограничения;

k) требования к функционированию;

l) меры по устранению неисправностей в изделии и отзывы об изделии; и

m) замечания по кибербезопасности (предупреждения об известных слабых местах в защите).

Соответствие требованиям данного подраздела проверяют путем подтверждения наличия документально оформленной информации, предоставленной каждым поставщиком прочих информационных технологий.

Примечание — В случаях, если предоставленный материал не соответствует нуждам ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, занимающейся МЕНЕДЖМЕНТОМ РИСКОВ, то может быть предоставлен дополнительный материал в рамках СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна получить документально оформленную информацию, установленную выше для прочих информационных технологий, включенных в МЕДИЦИНСКУЮ ИТ-СЕТЬ. Эта документально оформленная информация должна храниться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна получить дополнительную документально оформленную информацию для прочих информационных технологий, так как это необходимо для дальнейшей поддержки действий по МЕНЕДЖМЕНТУ РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ. Данная дополнительная документально оформленная информация должна храниться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Пример — Дополнительной информацией являются:
- стратегии испытаний и критерии оценки испытаний;
- предоставление информации о режимах отказа;
- статистические данные о надежности системы;
- обоснования безопасности; и
- рабочие характеристики.

Примечание — СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ между ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ и поставщиком прочих информационных технологий можно использовать для выявления необходимой документации и обмена данной документацией.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

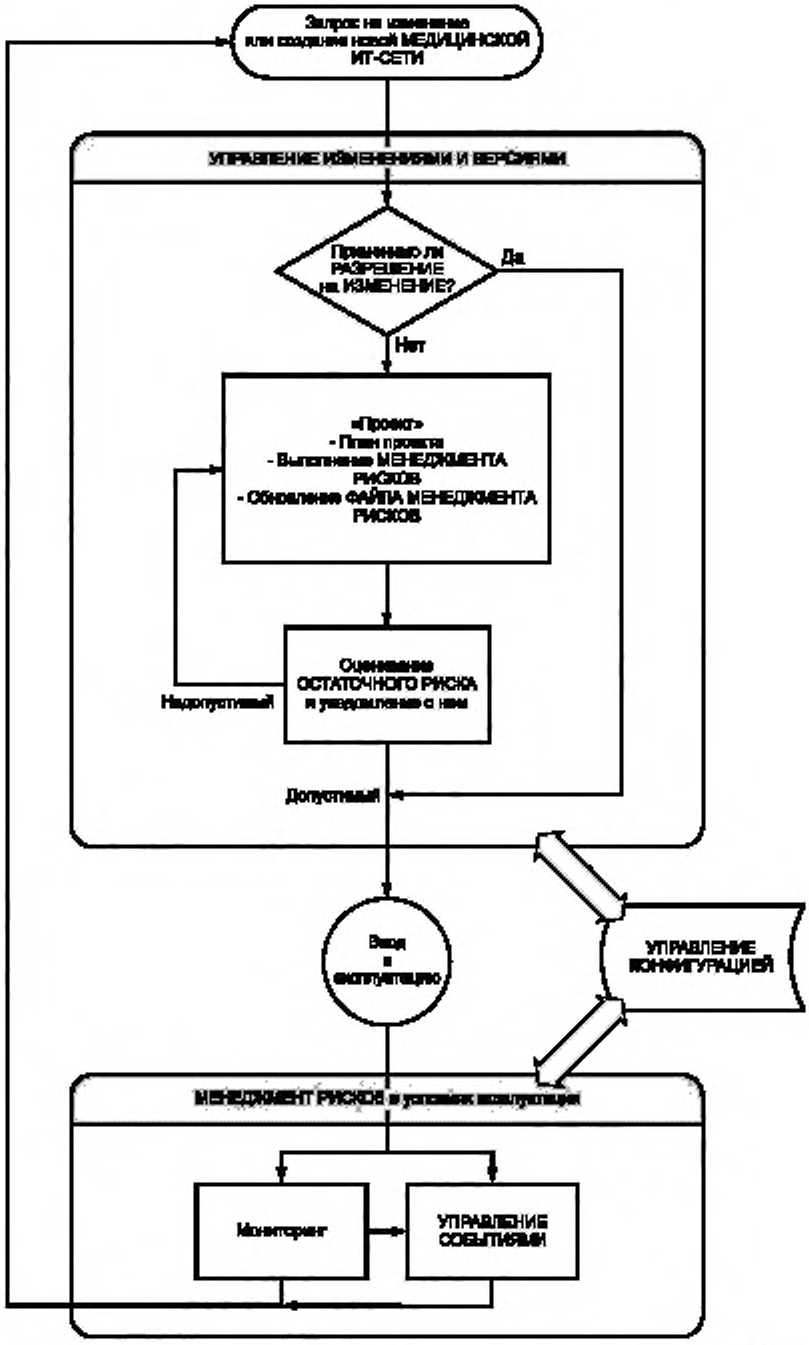
4 МЕНЕДЖМЕНТ РИСКОВ в жизненном цикле МЕДИЦИНСКИХ ИТ-СЕТЕЙ

4.1 Обзор

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна обеспечивать ОСНОВНЫЕ СВОЙСТВА МЕДИЦИНСКОЙ ИТ-СЕТИ на протяжении всего их жизненного цикла.

Примечание — Жизненный цикл МЕДИЦИНСКИХ ИТ-СЕТЕЙ, включая МЕНЕДЖМЕНТ РИСКОВ, представлен на рисунке 2.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.



Примечание — Запрос на изменение может быть запросом на списывание МЕДИЦИНСКОГО ПРИБОРА или МЕДИЦИНСКОЙ ИТ-СЕТИ. Данное списывание требует планирования и МЕНЕДЖМЕНТА РИСКОВ, подобно другим изменениям.

Рисунок 2 — Жизненный цикл МЕДИЦИНСКИХ ИТ-СЕТЕЙ, включая МЕНЕДЖМЕНТ РИСКОВ

4.2 МЕНЕДЖМЕНТ РИСКОВ, осуществляемый ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ

4.2.1 ПОЛИТИКА МЕНЕДЖМЕНТА РИСКОВ для подключения МЕДИЦИНСКИХ ПРИБОРОВ

Для поддержки жизненного цикла МЕДИЦИНСКОЙ ИТ-СЕТИ ВЫСШЕМУ РУКОВОДСТВУ необходимо определить и документально оформить политику МЕНЕДЖМЕНТА РИСКОВ для подключения МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТИ. Политика МЕНЕДЖМЕНТА РИСКОВ должна включать в себя:

a) обеспечение баланса трех ОСНОВНЫХ СВОЙСТВ и миссии ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ;

b) средства установления критериев допустимости РИСКА для каждого из ОСНОВНЫХ СВОЙСТВ, учитывая все соответствующие международные стандарты и национальные или региональные регламентирующие документы; и

c) описание ПРОЦЕССОВ или ссылку на ПРОЦЕССЫ, применяемые в МЕДИЦИНСКИХ ИТ-СЕТЯХ, включая, как минимум:

1) УПРАВЛЕНИЕ СОБЫТИЯМИ,

2) УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ,

3) УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ, и

4) контроль.

Примечание — Действия, выполняемые на жизненном цикле МЕДИЦИНСКОЙ ИТ-СЕТИ, могут быть отображены в политике управления ИТ-услугами (например, в соответствии с [10]) при наличии строгой связи с политикой МЕНЕДЖМЕНТА РИСКОВ.

Политика должна быть описана таким образом, чтобы она могла быть интерпретирована для всех действий по МЕНЕДЖМЕНТУ РИСКОВ.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.2.2 ПРОЦЕСС МЕНЕДЖМЕНТА РИСКОВ

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен сформировать и поддерживать ПРОЦЕСС для выявления ОПАСНОСТЕЙ, прогнозирования и оценки связанных с ними РИСКОВ, для контроля данных РИСКОВ и контроля эффективности УПРАВЛЕНИЯ РИСКОМ, учитывая предписанное применение МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — Внесение последующих изменений в МЕДИЦИНСКУЮ ИТ-СЕТЬ может привнести новые РИСКИ и требует дополнительного анализа.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.3 Планирование и документальное оформление МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ

4.3.1 Обзор

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна планировать МЕНЕДЖМЕНТ РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ, предоставляя:

a) описание связанных с РИСКОМ ресурсов.

Примечание — См. 4.3.2 для описания и примеров, связанных с РИСКОМ ресурсов;

b) документацию на ИТ-СЕТЬ; и

c) план МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — Оценка и документальное оформление структуры сети являются существенными при предоставлении информации, необходимой для АНАЛИЗА РИСКА и ОЦЕНИВАНИЯ РИСКА.

В связи с природой ИТ-СЕТЕЙ должны учитывать как текущее состояние ИТ-СЕТИ, так и планируемые изменения.

Первоначальную разработку новых МЕДИЦИНСКИХ ИТ-СЕТЕЙ так же, как и изменения в существующих МЕДИЦИНСКИХ ИТ-СЕТЯХ, на которые не распространяется документально оформленное РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ, должны выполнять в соответствии с проектами.

Примечания

1 МЕДИЦИНСКАЯ ИТ-СЕТЬ может иметь несколько параллельных или последовательных проектов.

2 См. также 4.5.2.3 о проектах МЕДИЦИНСКОЙ ИТ-СЕТИ и 4.5.2.2 о РАЗРЕШЕНИЯХ на ИЗМЕНЕНИЕ.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.3.2 Описание ресурсов, связанных с РИСКОМ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна установить список ресурсов ИТ-СЕТЕЙ, взаимодействующих с МЕДИЦИНСКИМИ ПРИБОРАМИ. Типичными ресурсами являются, но не ограничиваются аппаратные средства, программное обеспечение и данные, жизненно необходимые для ПРЕДНАЗНАЧЕННОГО ИСПОЛЬЗОВАНИЯ МЕДИЦИНСКОГО ПРИБОРА и предписанного применения МЕДИЦИНСКОЙ ИТ-СЕТИ.

Список ресурсов может включать, например:

a) конкретные компоненты МЕДИЦИНСКОЙ ИТ-СЕТИ и всех подключенных к ней МЕДИЦИНСКИХ ПРИБОРОВ и другое оборудование (например, средства создания изображений, компоненты сети) ИТ-инфраструктуры;

b) функциональные характеристики ИТ-инфраструктуры для МЕДИЦИНСКОЙ ИТ-СЕТИ (например, эксплуатационные свойства, такие как пропускная способность);

c) информация об УПРАВЛЕНИИ КОНФИГУРАЦИЕЙ;

d) программное обеспечение медицинского применения;

e) данные о конфигурации аппаратных средств и программного обеспечения;

f) определение характеристик данных пациента, идентифицируемых в МЕДИЦИНСКОЙ ИТ-СЕТИ или используемых подключенным МЕДИЦИНСКИМ ПРИБОРОМ, включая их природу, объем и уязвимость,

g) информация о поддержке процедуры предоставления медицинских услуг, включая историю применения и сведения об ОПЕРАТОРЕ/пользователе; и

h) описание защиты и других материалов, связанных с информацией по БЕЗОПАСНОСТИ всей системы в целом (в случае, если защита является компонентом БЕЗОПАСНОСТИ).

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.3.3 Документация на МЕДИЦИНСКУЮ ИТ-СЕТЬ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна создавать и вести документацию на сеть, необходимую для поддержания МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ при формировании интерфейсов между МЕДИЦИНСКИМИ ПРИБОРАМИ и всеми компонентами сети (как программными, так и аппаратными). Данная документация должна включать в себя, но не ограничиваться следующим:

a) описание физической и логической конфигураций сети.

Примечания

1 Конфигурация сети включает определение границ сети.

2 Документация может содержать описание электрических свойств ИТ-СЕТИ, которые могут оказать влияние на функционирование МЕДИЦИНСКОЙ ИТ-СЕТИ и подключенных к ней приборов. Например, заземление, гальваническая связь (развязка), блуждающие токи и питание через Ethernet;

b) прикладные стандарты и заявления о соответствии;

c) физическая и логическая структура клиента/сервера;

d) защищенность, безотказность и полнота данных сети;

e) требования к коммуникационной сети для каждого МЕДИЦИНСКОГО ПРИБОРА, установленные производителем; и

f) будущие (запланированные/разумно предсказуемые) изменения/обновления/усовершенствования.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.3.4 СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ

Каждый раз, когда к ИТ-СЕТИ подсоединяется МЕДИЦИНСКИЙ ПРИБОР или изменяется конфигурация подобного соединения, ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна сформулировать обязательное требование по подготовке одного или более документально оформленных СОГЛАШЕНИЙ ОБ ОТВЕТСТВЕННОСТИ (например, контрактах), определяющих ответственности всех значимых заинтересованных сторон.

СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ может охватывать один и более проектов или сопровождение одной или более МЕДИЦИНСКИХ ИТ-СЕТЕЙ и должно определять ответственность для всех аспектов жизненного цикла МЕДИЦИНСКОЙ ИТ-СЕТИ, а также всех действий на каждой стадии этого жизненного цикла.

Примечание — Для поддержания процесса подключения МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТИ производители МЕДИЦИНСКИХ ПРИБОРОВ предоставляют техническую информацию, необходимую для создания

ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ документации по МЕНЕДЖМЕНТУ РИСКОВ. Если для выполнения ПРОЦЕССА требуется информация, которая, по мнению производителя МЕДИЦИНСКОГО ПРИБОРА, носит деликатный характер, то предоставление такой информации определяется СОГЛАШЕНИЕМ ОБ ОТВЕТСТВЕННОСТИ и может защищаться соглашением о неразглашении.

СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ должно содержать (или ссылаться на документы, которые содержат), как минимум:

a) имя лица, ответственного за действия по МЕНЕДЖМЕНТУ РИСКОВ, на которые распространяется СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ;

b) описание области применения этих действий, на которую распространяется СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ, включая краткое содержание требований и/или ссылку на сами требования;

c) список МЕДИЦИНСКИХ ПРИБОРОВ и другого оборудования, которые должны быть подключены к ИТ-СЕТИ или изменены, вместе с именами производителей МЕДИЦИНСКИХ ПРИБОРОВ или организаций, ответственных за предоставление технической информации, необходимой для выполнения проекта;

d) список документов, которые должны предоставлять производители МЕДИЦИНСКИХ ПРИБОРОВ и поставщики другого оборудования, содержащих инструкции по подключению и отключению от ИТ-СЕТИ;

e) техническую информацию, которую должны предоставлять производители МЕДИЦИНСКИХ ПРИБОРОВ и поставщики другого оборудования, необходимую для выполнения АНАЛИЗА РИСКОВ в ИТ-СЕТИ; и

f) определение ролей и ответственностей, чтобы справляться с потенциально неблагоприятными событиями.

При необходимости ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна предоставить сводную информацию по обязанностям.

Примечание — Производитель МЕДИЦИНСКОГО ПРИБОРА несет ответственность за предоставление технической документации по использованию интерфейсов МЕДИЦИНСКОГО ПРИБОРА для соединения с ИТ-СЕТЬЮ, если подобное соединение предполагалось производителем. Поставщик другого оборудования не несет никаких юридических обязательств, и поэтому может потребоваться специальное соглашение для того, чтобы получить доступ к технической документации.

Если помимо перечисленных документов, предоставляемых производителями или организациями, необходимо также сотрудничество производителей МЕДИЦИНСКИХ ПРИБОРОВ, поставщиков оборудования и других организаций, то СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ должно:

g) выявлять характер требующегося сотрудничества; и

h) устанавливать:

- ответственных за запрос на такое сотрудничество;
- ответственных за реакцию на подобные запросы; и
- критерии, с помощью которых будут делаться выводы об адекватности подобной реакции.

Примечание — СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ рекомендуется периодически обновлять, так как данная информация может претерпевать изменения на протяжении жизненного цикла МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.3.5 План по МЕНЕДЖМЕНТУ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна формировать и поддерживать план по МЕНЕДЖМЕНТУ РИСКОВ для каждой МЕДИЦИНСКОЙ ИТ-СЕТИ. План по МЕНЕДЖМЕНТУ РИСКОВ должен включать:

a) описание МЕДИЦИНСКОЙ ИТ-СЕТИ, включая:

1) выявленные заинтересованные стороны в ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, которые должны быть проинформированы об ОПАСНОСТЯХ, чтобы гарантировать их осведомленность о РИСКЕ,

2) предписанное применение и ожидаемую пользу от использования МЕДИЦИНСКОЙ ИТ-СЕТИ,

3) причину подключения каждого МЕДИЦИНСКОГО ПРИБОРА, и

4) применение каждого МЕДИЦИНСКОГО ПРИБОРА, подключенного к МЕДИЦИНСКОЙ ИТ-СЕТИ, не оговаривавшееся производителем в ПРЕДНАЗНАЧЕННОМ ИСПОЛЬЗОВАНИИ;

b) описание действий, ролей и ответственностей всех сторон по УПРАВЛЕНИЮ РИСКАМИ, участвующих в эксплуатации/обслуживании МЕДИЦИНСКОЙ ИТ-СЕТИ;

c) требования к контролю МЕДИЦИНСКОЙ ИТ-СЕТИ (см. 4.6.1);

d) критерии допустимости РИСКА, основанные на политике ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ по установлению допустимого РИСКА, включая случаи, когда вероятность нанесения ВРЕДА не может быть определена.

Если проект предполагает внесение изменений в существующую МЕДИЦИНСКУЮ ИТ-СЕТЬ, то план по МЕНЕДЖМЕНТУ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен быть обновлен.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4 МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ

4.4.1 Обзор

Данный подраздел описывает ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКОВ, которые обеспечивают реализацию проекта МЕДИЦИНСКОЙ ИТ-СЕТИ, а также решение о вводе в эксплуатацию того или иного изменения.

Действия по МЕНЕДЖМЕНТУ РИСКОВ, включающие АНАЛИЗ РИСКА, ОЦЕНИВАНИЕ РИСКА, УПРАВЛЕНИЕ РИСКОМ, оценка и уведомление об ОСТАТОЧНОМ РИСКЕ, а также его принятие должны быть документально оформлены. Данная документация может быть включена в план по МЕНЕДЖМЕНТУ РИСКОВ или существовать в виде отдельных документов в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ, связанном с МЕДИЦИНСКОЙ ИТ-СЕТЬЮ. После выполнения ПРОЦЕССА УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ должны появиться планы действий в результате ОЦЕНКИ РИСКА.

Примечание — Для каждой МЕДИЦИНСКОЙ ИТ-СЕТИ существует отдельный набор документов по МЕНЕДЖМЕНТУ РИСКОВ, потому что меры по УПРАВЛЕНИЮ РИСКОМ для любого проекта или изменения не должны вступать в противоречие с существующими мерами по УПРАВЛЕНИЮ РИСКОМ МЕДИЦИНСКОЙ ИТ-СЕТИ или с мерами по УПРАВЛЕНИЮ РИСКОМ, предложенными в параллельном проекте.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.2 АНАЛИЗ РИСКА

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна выявлять наиболее вероятные ОПАСНОСТИ возможные в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Для каждой выявленной ОПАСНОСТИ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна дать оценку соответствующих РИСКОВ, используя доступную информацию или данные.

Примечание — РИСКИ, которые необходимо проанализировать, охватывают весь жизненный цикл, в первую очередь реализацию изменения и регулярное использование МЕДИЦИНСКОЙ ИТ-СЕТИ.

Если вероятность причинения ВРЕДА не может быть предварительно оценена, то должны быть перечислены возможные последствия для ОЦЕНИВАНИЯ РИСКА и УПРАВЛЕНИЯ РИСКОМ.

Результат этой деятельности должен быть внесен в ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.3 ОЦЕНИВАНИЕ РИСКА

Для каждой выявленной ОПАСНОСТИ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна принять решение, используя критерии, определенные в плане по УПРАВЛЕНИЮ РИСКАМИ. Возможны два варианта:

a) предварительная оценка дала настолько малую вероятность РИСКА(ОВ), что его снижение не требуется. В данном случае основание для решения должно быть документально оформлено в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ;

b) предварительная оценка дала недопустимое значение РИСКА(ОВ). В данном случае меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы в соответствии с 4.4.4.

Соответствие требованиям данного пункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.4 УПРАВЛЕНИЕ РИСКОМ

4.4.4.1 Анализ возможностей УПРАВЛЕНИЯ РИСКОМ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна выявлять и документально оформлять предложенные меры по УПРАВЛЕНИЮ РИСКОМ для каждого недопустимого РИСКА до тех пор, пока ОСТАТОЧНЫЙ РИСК не будет признан как допустимый.

Должны использовать один или несколько способов УПРАВЛЕНИЯ РИСКОМ из перечисленных ниже в порядке приоритета:

a) управление, присущее проекту (например, физическая изоляция сети от внешних угроз);

b) защитные меры (например, добавление аварийной сигнализации);

c) информация для обеспечения уверенности (например, оповещения, пользовательская документация, обучение).

Примечания

1 УПРАВЛЕНИЕ РИСКОМ может включать в себя меры, например, такие как:

- инструкции и ограничения, документально оформленные в РАЗРЕШЕНИИ на ИЗМЕНЕНИЕ (см. 2.3 и 4.5.2.2);
- компоненты сети;
- изменение конфигурации сети;
- организационные рекомендации; или
- внесение изменений в подключенные МЕДИЦИНСКИЕ ПРИБОРЫ.

2 Для каждого РИСКА в проекте должно быть внимательно рассмотрено, как лучше всего реализовать управление для обеспечения способности к длительной эксплуатации. Например, с помощью внесения изменений в МЕДИЦИНСКУЮ ИТ-СЕТЬ или с помощью разрешенных производителем изменений МЕДИЦИНСКОГО ПРИБОРА.

До той степени, до которой УПРАВЛЕНИЕ РИСКОМ обеспечивает компромиссы между ОСНОВНЫМИ СВОЙСТВАМИ, ОСНОВНЫЕ СВОЙСТВА должны рассматриваться в порядке приоритета: БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМ.

Если во время анализа возможностей УПРАВЛЕНИЯ РИСКОМ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ определяет, что требующееся уменьшение РИСКА практически не осуществимо, то ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна провести и документально оформить анализ соотношения РИСК/польза для ОСТАТОЧНОГО РИСКА (см. 4.4.5).

Соответствие требованиям данного пункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.4.2 Меры УПРАВЛЕНИЯ РИСКОМ

Если выбраны конкретные меры УПРАВЛЕНИЯ РИСКОМ требующие внесения изменения в МЕДИЦИНСКУЮ ИТ-СЕТЬ, то должны выполняться ПРОЦЕССЫ УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ.

Выбранные меры УПРАВЛЕНИЯ РИСКОМ должны фиксироваться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подпункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.4.3 Реализация мер УПРАВЛЕНИЕ РИСКОМ

Выбранные меры УПРАВЛЕНИЯ РИСКОМ должны быть реализованы.

Меры УПРАВЛЕНИЯ РИСКОМ в МЕДИЦИНСКОМ ПРИБОРЕ должны реализовываться только производителем МЕДИЦИНСКОГО ПРИБОРА или ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ, в соответствии с инструкциями по использованию или осуществляющей реализацию таких мер при документально оформленном разрешении производителя МЕДИЦИНСКОГО ПРИБОРА.

Не рекомендуется внесение ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ каких бы то ни было изменений в МЕДИЦИНСКИЙ ПРИБОР без документально оформленного согласия на то производителя МЕДИЦИНСКОГО ПРИБОРА. Если же подобное изменение было предпринято, то ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна уведомить производителя и соблюсти все необходимые нормативные требования для ввода модифицированного МЕДИЦИНСКОГО ПРИБОРА в эксплуатацию.

Любой ОСТАТОЧНЫЙ РИСК должен быть документально оформлен в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подпункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.4.4 ВЕРИФИКАЦИЯ мер УПРАВЛЕНИЯ РИСКОМ

Реализация всех мер УПРАВЛЕНИЯ РИСКОМ в операционной системе должна быть ВЕРИФИЦИРОВАНА и документально оформлена в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Эффективность мер УПРАВЛЕНИЯ РИСКОМ должна быть ВЕРИФИЦИРОВАНА и документально оформлена в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — Может возникнуть необходимость провести верификацию эффективности мер УПРАВЛЕНИЯ РИСКОМ в тестовой среде до их реализации в операционной системе.

Соответствие требованиям данного подпункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.4.5 Новые РИСКИ, возникающие в связи с УПРАВЛЕНИЕМ РИСКОМ

Реализованные меры УПРАВЛЕНИЯ РИСКОМ и установленная операционная система должны быть проверены на новые, недопустимые РИСКИ (например, при ухудшении ОСНОВНЫХ СВОЙСТВ или других важных параметров, существенных при реализации заданного применения МЕДИЦИНСКОЙ ИТ-СЕТИ).

Данное оценивание должно быть документально оформлено в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подпункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.4.5 Оценивание ОСТАТОЧНОГО РИСКА и уведомление о риске

Должно быть проведено оценивание ОСТАТОЧНОГО РИСКА, основанное на оценке эффективности реализованных мер УПРАВЛЕНИЯ РИСКОМ, осуществленной для предварительной версии.

Как отдельные ОСТАТОЧНЫЕ РИСКИ, так и совокупный ОСТАТОЧНЫЙ РИСК должны быть оценены и определена их допустимость.

Примечание — Информацию по ОЦЕНИВАНИЮ РИСКА см. в 4.4.3.

Если отдельный ОСТАТОЧНЫЙ РИСК или совокупный ОСТАТОЧНЫЙ РИСК не будет считаться допустимым, то следует применить дополнительные меры УПРАВЛЕНИЯ РИСКОМ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна определить и документально оформить краткую информацию по ОСТАТОЧНОМУ РИСКУ, содержащую список всех отдельных РИСКОВ и совокупный ОСТАТОЧНЫЙ РИСК, остающийся после реализации мер УПРАВЛЕНИЯ РИСКОМ (см. 4.4.4.3), включая ОСТАТОЧНЫЕ РИСКИ, связанные с конкретным проектом МЕДИЦИНСКОЙ ИТ-СЕТИ, и ОСТАТОЧНЫЙ РИСК в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Если снижение ОСТАТОЧНОГО РИСКА до допустимого уровня практически не осуществимо в рамках политики ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ (см. 3.3) по определению ОСТАТОЧНОГО РИСКА (см. 3.3), то лицо, которое по поручению РУКОВОДСТВА должно выполнить анализ ОСТАТОЧНЫХ РИСКОВ (это может быть СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ), должно провести и документально оформить результаты анализа соотношения РИСК/польза для сравнения отдельного или совокупного ОСТАТОЧНОГО РИСКА с пользой для здоровья, полученной от подключенного МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ, а также принять решение о принятии или непринятии ОСТАТОЧНОГО РИСКА в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — Информацию по анализу соотношения РИСК/польза см. [4].

Соответствие требованиям данного пункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.5 УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

4.5.1 ПРОЦЕСС УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна применять и документально оформлять ПРОЦЕСС УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ.

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ обеспечивает выполнение ПРОЦЕССА УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ для МЕДИЦИНСКОЙ ИТ-СЕТИ, а также его включение в процесс МЕНЕДЖМЕНТА РИСКОВ.

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен использовать результаты ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ для определения условий принятия и допустимости изменений, осуществляющихся в ПРОЦЕССЕ УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ.

Примечание — Если два или несколько параллельных проекта недостаточно согласованы, то возможны непредвиденные последствия.

ПРОЦЕСС УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ должен документально оформляться и применяться для управления версиями МЕДИЦИНСКОЙ ИТ-СЕТИ во всех ПРОЦЕССАХ МЕНЕДЖМЕНТА РИСКОВ на протяжении УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.5.2 Принятие решения о способе применения МЕНЕДЖМЕНТА РИСКОВ

4.5.2.1 Краткий обзор

Для любой новой МЕДИЦИНСКОЙ ИТ-СЕТИ или изменения существующей МЕДИЦИНСКОЙ ИТ-СЕТИ должен быть инициирован ПРОЦЕСС УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна учесть природу изменений, чтобы определить, отвечает ли требованиям действующее РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ. Если действующего РАЗРЕШЕНИЯ на ИЗМЕНЕНИЕ не существует, то должен инициироваться проект МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного подпункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.5.2.2 РАЗРЕШЕНИЯ на ИЗМЕНЕНИЯ

Если в результате выполнения МЕНЕДЖМЕНТА РИСКОВ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ решает, что заданный тип стандартного изменения возможно осуществить с допустимым РИСКОМ при устанавливаемых ограничениях, то ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ может сформировать РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ, позволяющее осуществление подобных стандартных изменений и устанавливающее ограничения для них.

Примечания

1 Например, РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ может позволить изменять число МЕДИЦИНСКИХ ПРИБОРОВ определенного типа в МЕДИЦИНСКОЙ ИТ-СЕТИ в пределах установленного диапазона.

2 Если выполненные изменения всегда соответствуют требованиям РАЗРЕШЕНИЯ на ИЗМЕНЕНИЕ и заданным в нем ограничениям, то для каждого случая использования РАЗРЕШЕНИЯ на ИЗМЕНЕНИЕ можно не выполнять УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и МЕНЕДЖМЕНТ РИСКОВ.

РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ должно устанавливать, какая информация фиксируется для каждого разрешенного изменения.

РАЗРЕШЕНИЯ на ИЗМЕНЕНИЯ должны храниться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Примечание — РАЗРЕШЕНИЯ НА ИЗМЕНЕНИЕ могут составляться только в результате ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ (см 4.4.4.2).

Соответствие требованиям данного подпункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.5.2.3 Проекты МЕДИЦИНСКОЙ ИТ-СЕТИ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна составлять и поддерживать план проекта по подключению нового типа МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТИ, по внесению изменений в МЕДИЦИНСКУЮ ИТ-СЕТЬ, по внесению изменений в МЕДИЦИНСКИЕ ПРИБОРЫ, подключенные к МЕДИЦИНСКОЙ ИТ-СЕТИ, по списыванию МЕДИЦИНСКИХ ПРИБОРОВ или МЕДИЦИНСКОЙ ИТ-СЕТИ или любой другой деятельности, способной привести к новому РИСКУ. Типовым начальным планом проекта должен быть план разработки новой МЕДИЦИНСКОЙ ИТ-СЕТИ. Такой план проекта должен включать:

a) требования к действиям по МЕНЕДЖМЕНТУ РИСКОВ, включающим:

1) действия по созданию и обновлению любых документов ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ, необходимых для данного проекта, таких как план МЕНЕДЖМЕНТА РИСКОВ или документы по МЕНЕДЖМЕНТУ РИСКОВ,

2) план по выполнению требований, установленных в плане МЕНЕДЖМЕНТА РИСКОВ для соответствующих МЕДИЦИНСКИХ ИТ-СЕТЕЙ, и

3) действия по ВЕРИФИКАЦИИ мер УПРАВЛЕНИЯ РИСКОМ;

b) описание проекта, включая:

1) определение МЕДИЦИНСКИХ ИТ-СЕТЕЙ, разработанных в проекте или связанных с ним,

2) спецификацию требований к проекту, и

3) спецификацию минимального набора документов, необходимых для проекта МЕДИЦИНСКОЙ ИТ-СЕТИ;

c) описание области применения запланированных изменений МЕДИЦИНСКОЙ ИТ-СЕТИ, включая описания (но не ограничиваясь):

1) физической и логической конфигурации МЕДИЦИНСКОЙ ИТ-СЕТИ до и после осуществления запланированных изменений,

2) информационного потока до и после осуществления запланированных изменений,

3) компонентов, которые требуется получить или удалить,

4) спецификаций немедицинских компонентов сети, где это необходимо, и

5) ограничений на расширение существующей МЕДИЦИНСКОЙ ИТ-СЕТИ.

План проекта должен корректироваться каждый раз, когда в нем необходимо отразить внесенные в проект изменения.

План проекта должен храниться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ в соответствии с ПРОЦЕССАМИ, выполняемыми на следующих стадиях жизненного цикла: УПРАВЛЕНИЕ СОБЫТИЯМИ, УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ.

Примечание — Если изменения ИТ-СЕТИ осуществляются постоянно, то план проекта может быть утвержден как протокольный документ, пригодный для повторного использования и содержащий все эти неотъемлемые элементы.

Соответствие требованиям данного полункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.5.3 Ввод в эксплуатацию

Переход МЕДИЦИНСКОЙ ИТ-СЕТИ к «условиям эксплуатации» (рисунок 2) является целью всех проектов и инициатив по изменениям. Перед вводом в эксплуатацию ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна проанализировать ОСТАТОЧНЫЙ РИСК МЕДИЦИНСКОЙ ИТ-СЕТИ.

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ обязан проверить всю краткую информацию по ОСТАТОЧНОМУ РИСКУ проектов или изменений, чтобы определить допустимость РИСКА, связанного с взаимодействием с последними или еще ожидающими решения проектами и изменениями (например, подключение МЕДИЦИНСКОГО ПРИБОРА к функционирующей развивающейся ИТ-СЕТИ).

СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен принять внесение установленного изменения в МЕДИЦИНСКУЮ ИТ-СЕТЬ до ее ввода в эксплуатацию.

Принятие ОСТАТОЧНОГО РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ должно быть документально оформлено, а информация о конфигурации должна вноситься в ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Соответствие требованиям данного пункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.6 МЕНЕДЖМЕНТ РИСКОВ в действующей сети

4.6.1 Контроль

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна определить и поддерживать ПРОЦЕСС контроля каждой установленной МЕДИЦИНСКОЙ ИТ-СЕТИ для обнаружения возникающих РИСКОВ, обеспечения эффективности мер УПРАВЛЕНИЯ РИСКОМ и точности предположительной оценки РИСКА.

Требования к контролю должны быть установлены как часть плана МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ. Ниже приведены примеры того, что должно подвергаться контролю:

a) изменения окружающей среды (включая локальную/связанную среду, а также уязвимость ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ соответствующих компонентов и сети);

b) обратная связь в процессе функционирования или характеристик работы, например: обратная связь с пользователем, проблемы скорости, высокая частота ошибок, отказ, атаки вредоносного программного обеспечения;

c) информация о подключенных компонентах;

d) информация о похожих МЕДИЦИНСКИХ ИТ-СЕТЯХ;

e) обнаруженные события; и

f) аудит нетехнических мер УПРАВЛЕНИЯ РИСКОМ, таких как организационные правила и процедуры.

Если в ходе контроля выявляется реальное или потенциальное увеличение РИСКА, связанное с МЕДИЦИНСКОЙ ИТ-СЕТЬЮ или ее компонентами (возможное или фактическое негативное влияние), то инициируется ПРОЦЕСС УПРАВЛЕНИЯ СОБЫТИЯМИ и существенная информация доводится до сведения соответствующих представителей ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ.

Примечание — В некоторых случаях контролирующие органы могут потребовать от ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ предоставить соответствующий отчет.

Соответствие требованиям данного пункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

4.6.2 УПРАВЛЕНИЕ СОБЫТИЯМИ

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна выполнять УПРАВЛЕНИЕ СОБЫТИЯМИ для того, чтобы:

a) фиксировать и документально оформлять негативные события;

b) оценивать события и предлагать изменения, осуществляемые через УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ, если это необходимо;

c) отслеживать все корректирующие и защитные действия, ведущие к устранению негативных событий;

d) уведомлять СПЕЦИАЛИСТА по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ и/или других членов ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ о существенных обнаруживаемых событиях и их результатах.

Соответствие требованиям данного пункта проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

5 Управление документацией

5.1 Процедура управления документацией

Все документы, связанные с жизненным циклом МЕДИЦИНСКОЙ ИТ-СЕТИ, должны пересматривать, исправлять, анализировать и принимать в соответствии с процедурой управления документацией.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ.

5.2 ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ

В дополнение к требованиям, представленным в других разделах данного стандарта, ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ должен обеспечить прослеживаемость каждой выявленной ОПАСНОСТИ для выполнения:

a) АНАЛИЗА РИСКА;

b) ОЦЕНИВАНИЯ РИСКА;

c) реализации и ВЕРИФИКАЦИИ мер УПРАВЛЕНИЯ РИСКОМ; и

d) оценки допустимости любого(ых) ОСТАТОЧНОГО(ЫХ) РИСКА(ОВ) и его (их) принятия.

Примечания

1 Записи и другие документы, составляющие ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ, могут быть частью других документов или файлов. ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ не должен физически содержать все записи и другие документы, но в нем должны храниться хотя бы ссылки или указатели на все требующиеся документы. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна быть способна своевременно собрать информацию, на которую ссылается ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

2 ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ может быть представлен в любой форме и с помощью любых средств.

3 Организациям, для которых «обоснованием гарантии» является средство организации ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ, следует обратиться к [5] (в разработке) для получения дополнительной информации.

Соответствие требованиям данного подраздела проверяют путем экспертизы ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

Приложение А
(справочное)

Обоснование

А.1 Общие положения

Взаимодействие МЕДИЦИНСКИХ ПРИБОРОВ и информационных систем управления привело к необходимости изменения методов поддержания БЕЗОПАСНОСТИ и ЭФФЕКТИВНОСТИ МЕДИЦИНСКИХ ПРИБОРОВ после начала их эксплуатации. И хотя ответственность, лежащая на производителе МЕДИЦИНСКОГО ПРИБОРА за выпуск безопасного и эффективного МЕДИЦИНСКОГО ПРИБОРА, не изменилась, среда (т. е. ИТ-СЕТЬ), в которой оказывается МЕДИЦИНСКИЙ ПРИБОР, претерпевает постоянные изменения. Производитель МЕДИЦИНСКИХ ПРИБОРОВ не способен предвидеть все возможные ее изменения и гарантировать корректную работу МЕДИЦИНСКОГО ПРИБОРА во всех возможных случаях.

В то же время ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ (часто называемая организацией по предоставлению услуг здравоохранения или HDO) выставляет требования, связанные с ее способностью предоставлять высококачественные медицинские услуги, а также с защитой и конфиденциальностью данных пациентов, которые должны выполнять в условиях все той же, постоянно меняющейся, среды. Выполнение данных требований не может быть достигнуто без корректной работы МЕДИЦИНСКИХ ПРИБОРОВ, являющихся частью этой среды, т. е. подключенных к ИТ-СЕТИ.

Настоящий стандарт подтверждает необходимость взаимодействия между заинтересованными в поставке и подключении МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТЯМ сторонами для выполнения всех этих требований в сегодняшних условиях интенсивно меняющихся технологий. Настоящий стандарт определяет необходимые роли и ответственности, а также ПРОЦЕСС управления РИСКАМИ, возникающими в связи с включением МЕДИЦИНСКИХ ПРИБОРОВ в инфраструктуру информационных технологий организации, предоставляющей услуги здравоохранения. И хотя ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ берет на себя ответственность за принятие решений о подключении МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТЯМ, эти решения частично основаны на заявлениях и информации поставщиков для данной организации. В некоторых случаях документации, предоставленной при выпуске продукции на рынок, достаточно для поддержания решений ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. В других случаях ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ может понадобиться дополнительная информация, которая обычно может и не предоставляться. Настоящий стандарт предлагает использовать СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ для определения информации, необходимой в процессах на всех стадиях жизненного цикла МЕДИЦИНСКОЙ ИТ-СЕТИ, и ответственности за предоставление и контроль доступа к данной информации.

Для того чтобы обеспечить соответствие требованиям настоящего стандарта, необходимо собирать и хранить документацию в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКОВ для каждой МЕДИЦИНСКОЙ ИТ-СЕТИ.

А.2 Раздел 3. Роли и ответственности

Данный раздел выявляет роли и ответственности, которые необходимы при взаимодействии для управления РИСКОМ в процессе подключения МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТЯМ.

Организация, предоставляющая услуги в области здравоохранения, владеющая и использующая МЕДИЦИНСКУЮ ИТ-СЕТЬ, несет полную ответственность за ее функционирование. Она и есть ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ. Чтобы гарантировать, что МЕНЕДЖМЕНТУ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ уделено надлежащее внимание, ВЫСШЕМУ РУКОВОДСТВУ ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ требуется в соответствии с настоящим стандартом определить политику, предоставить ресурсы, назначить квалифицированный персонал и проанализировать результаты деятельности по МЕНЕДЖМЕНТУ РИСКОВ. Очень важно, чтобы обязанность выполнения ПРОЦЕССА МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ была возложена на одного из сотрудников. Главная обязанность ВЫСШЕГО РУКОВОДСТВА — это назначение СПЕЦИАЛИСТА по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ и обеспечение того, чтобы другие сотрудники ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ содействовали этому специалисту по управлению РИСКАМИ подключения МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТИ.

Концепция РИСКА зависит от влияния отказа на клиническое заболевание, а также от вероятности самого отказа, поэтому ответственности производителей МЕДИЦИНСКИХ ПРИБОРОВ отличаются от ответственностей поставщиков информационных технологий. Производители МЕДИЦИНСКИХ ПРИБОРОВ осознают влияние отказа сети на клиническое заболевание, которое основано на ПРЕДНАЗНАЧЕННОМ ИСПОЛЬЗОВАНИИ МЕДИЦИНСКОГО ПРИБОРА, в то время как поставщики ИТ могут предложить информацию только о режимах отказов, вероятностях и т. п., связанную с ИТ-оборудованием. По этим причинам эти две роли рассматриваются независимо друг от друга.

От производителя МЕДИЦИНСКОГО ПРИБОРА требуется наличие СОПРОВОДИТЕЛЬНЫХ ДОКУМЕНТОВ. Эти СОПРОВОДИТЕЛЬНЫЕ ДОКУМЕНТЫ должны быть предоставлены ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, так как содержание данных документов является очень важным для выполнения действий по МЕНЕДЖМЕНТУ РИСКОВ ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ во время подключения МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТИ. Следует отметить, что могут возникать различные интерпретации информации в СОПРОВОДИТЕЛЬНЫХ ДОКУМЕНТАХ.

Поэтому в 3.5 перечисления a)–f) определяют минимальное содержание таких СОПРОВОДИТЕЛЬНЫХ ДОКУМЕНТОВ, так как существуют МЕДИЦИНСКИЕ ПРИБОРЫ, от которых не требуется демонстрации соответствия (например, медицинские приборы лабораторной диагностики). Однако настоятельно рекомендуется, чтобы производители МЕДИЦИНСКОГО ПРИБОРА обеспечивали выполнение требований подраздела 14.13 [1].

Виды и вероятности отказов сети также зависят от элементов, которые не контролируются ни производителями МЕДИЦИНСКИХ ПРИБОРОВ, ни поставщиками других информационных технологий, таких как проектирование систем, конфигурации, топологии, ИТ-процессов и процедур, ни фактическим (в отличие от предназначенного) использованием МЕДИЦИНСКОГО ПРИБОРА и т. д. Таким образом, только ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ обладает наиболее полной информацией о РИСКАХ в МЕДИЦИНСКОЙ ИТ-СЕТИ и несет основную ответственность за МЕНЕДЖМЕНТ РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ.

А.3 Раздел 4. МЕНЕДЖМЕНТ РИСКОВ на жизненном цикле МЕДИЦИНСКИХ ИТ-СЕТЕЙ

Основной предпосылкой настоящего стандарта является тот факт, что РИСК должен рассматриваться для всех изменений перед тем, как они будут внесены в МЕДИЦИНСКУЮ ИТ-СЕТЬ. Настоящий стандарт требует выполнения МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКИХ ИТ-СЕТЯХ. Одна ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ может работать с несколькими МЕДИЦИНСКИМИ ИТ-СЕТЯМИ. Требуемые в настоящем стандарте действия, обеспечивающие МЕНЕДЖМЕНТ РИСКОВ, в основном соответствуют действиям, описанным в [4], но выходят за рамки понятия БЕЗОПАСНОСТИ [4], включая управление РИСКАМИ в обеспечение ЭФФЕКТИВНОСТИ и РИСКИ в ЗАЩИЩЕННОСТИ СИСТЕМЫ И ДАННЫХ. Это требует внесения изменений в определенные термины [4]. В настоящем стандарте понятие ВРЕД является более широким и включает снижение ЭФФЕКТИВНОСТИ и нарушение защищенности. Для этого требуется, чтобы при определении БЕЗОПАСНОСТИ было указано, какой тип ВРЕДА учитывается при оценке РИСКА. Поэтому определением БЕЗОПАСНОСТИ становится «отсутствие недопустимого РИСКА физической травмы или ущерба здоровью человек, или ущерба имуществу, или окружающей среде». С такими изменениями действия, обеспечивающими МЕНЕДЖМЕНТ РИСКОВ, описанные в [4], могут быть использованы и в настоящем стандарте. Так как эти действия применяются в процессе менеджмента жизненного цикла МЕДИЦИНСКОЙ ИТ-СЕТИ, то они описаны в контексте эксплуатируемой МЕДИЦИНСКОЙ ИТ-СЕТИ. Раздел 4 состоит из подразделов, которые описывают действия, обеспечивающие МЕНЕДЖМЕНТ РИСКОВ, выполняемые в процессе внесения изменений в МЕДИЦИНСКУЮ ИТ-СЕТЬ или во время работы МЕДИЦИНСКОЙ ИТ-СЕТИ. Таблица А.1 показывает связь между действиями, обеспечивающими МЕНЕДЖМЕНТ РИСКОВ, описанными в [4] с действиями, описанными в настоящем стандарте.

Подраздел 4.2 МЕНЕДЖМЕНТ РИСКОВ, осуществляемый ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ

Подраздел 4.2 описывает действия и ожидаемые результаты, требуемые на уровне ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Данные результаты применимы к МЕДИЦИНСКИМ ИТ-СЕТЯМ, реализуемым ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ.

Подраздел 4.3 Планирование и документальное оформление МЕНЕДЖМЕНТА РИСКОВ в МЕДИЦИНСКОЙ ИТ-СЕТИ

Подраздел 4.3 описывает действия и ожидаемые результаты работы, необходимые для каждой МЕДИЦИНСКОЙ ИТ-СЕТИ в отдельности, которые требуются перед началом действий, обеспечивающих МЕНЕДЖМЕНТ РИСКОВ.

Таблица А.1 — Связь между [4] и МЭК/ТО 80001-1

Раздел (подраздел) [4]		Раздел (подраздел) МЭК/ТО 80001-1	
4	Анализ риска		
4.1	ПРОЦЕСС АНАЛИЗА РИСКОВ	Нет	
4.2	ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ и выявление характеристик, связанных с БЕЗОПАСНОСТЬЮ		
4.3	Выявление ОПАСНОСТЕЙ	4.4.2	Анализ рисков
4.4	Оценка РИСКА(ОВ) для каждой опасной ситуации: - «Необходимо рассматривать разумно предсказуемые последовательности или комбинации событий, приводящие к возникновению опасных ситуаций, и регистрировать возникшую опасную ситуацию». - «Для каждой выявленной опасной ситуации должна быть получена оценка РИСКА(ОВ)»	4.4.2	«Для каждой выявленной ОПАСНОСТИ, ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна дать оценку соответствующих РИСКОВ, используя доступную информацию или данные…»
5	Оценивание риска	4.4.3	Оценивание риска
6	Управление риском	4.4.4	Управление риском

Окончание таблицы А.1

Раздел (подраздел) [4]		Раздел (подраздел) МЭК/ТО 80001-1	
6.1	Снижение риска	Нет	
6.2	Анализ возможностей УПРАВЛЕНИЯ РИСКОМ	4.4.4.1	Анализ возможностей УПРАВЛЕНИЯ РИСКОМ
		4.4.4.2	Меры УПРАВЛЕНИЯ РИСКОМ
6.3	Реализация мер по УПРАВЛЕНИЮ РИСКОМ	4.4.4.3	Реализация мер по УПРАВЛЕНИЮ РИСКОМ
		4.4.4.4	Верификация мер по УПРАВЛЕНИЮ РИСКОМ
6.4	Оценивание остаточного риска		(Рассмотрено в 4.4.4.1)
6.5	Анализ соотношения РИСК/польза		(Рассмотрено в 4.4.4.1 и 4.4.5)
6.6	Риски, возникающие вследствие выполнения мер по УПРАВЛЕНИЮ РИСКОМ	4.4.4.5	Новые риски, возникающие в связи с УПРАВЛЕНИЕМ РИСКОМ
7	Оценивание допустимости совокупного остаточного риска	4.4.5	Оценивание ОСТАТОЧНОГО РИСКА и уведомление о риске

Подраздел 4.5 УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

Подраздел 4.5 описывает действия, обеспечивающие МЕНЕДЖМЕНТ РИСКОВ, требующиеся в процессе изменения МЕДИЦИНСКОЙ ИТ-СЕТИ, перед тем как она перейдет на стадию эксплуатации в реальных условиях. Такие действия включают в себя внесение изменений в существующую МЕДИЦИНСКУЮ ИТ-СЕТЬ, также как и изначальное создание МЕДИЦИНСКОЙ ИТ-СЕТИ или преобразование НЕМЕДИЦИНСКОЙ ИТ-СЕТИ в МЕДИЦИНСКУЮ. На данной стадии традиционные действия, обеспечивающие МЕНЕДЖМЕНТ РИСКОВ, осуществляются в соответствии с проектом. СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ несет ответственность за объединение всех действий проекта, обеспечивающих МЕНЕДЖМЕНТ РИСКОВ, в один ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ для МЕДИЦИНСКОЙ ИТ-СЕТИ.

Некоторые меры по КОНТРОЛЮ РИСКА, определенные для МЕДИЦИНСКОЙ ИТ-СЕТИ, могут включать в себя действия, осуществляющиеся во время стадии эксплуатации в реальных условиях, такие как клинические процедуры, для смягчения последствий отключения питания в ИТ-СЕТИ.

В случае часто выполняемых действий, обеспечивающих МЕНЕДЖМЕНТ РИСКОВ, желательно избегать их ненужного повторения. Настоящий стандарт предлагает использовать РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ, как один из способов для решения этого вопроса. Если МЕНЕДЖМЕНТ РИСКОВ показывает, что стандартное изменение, например добавление пользователя, может быть осуществлено с допустимым РИСКОМ, подчиняющимся установленным ограничениям (например, ограничение по типу числу пользователей), то ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ может утвердить РАЗРЕШЕНИЕ на ИЗМЕНЕНИЕ, которое разрешает подобные стандартные изменения и устанавливает их ограничения.

Подраздел 4.6. МЕНЕДЖМЕНТ РИСКОВ в действующей сети

Подраздел 4.6 описывает действия, обеспечивающие МЕНЕДЖМЕНТ РИСКОВ, требующиеся после пуска в эксплуатацию МЕДИЦИНСКОЙ ИТ-СЕТИ (эксплуатация в реальных условиях). Для достижения допустимого РИСКА при использовании (при эксплуатации в реальных условиях) МЕДИЦИНСКОЙ(ИХ) ИТ-СЕТИ(ЕЙ) осуществляется мониторинг, представляющий собой непрерывный анализ всех действий, обеспечивающих МЕНЕДЖМЕНТ РИСКОВ и УПРАВЛЕНИЕ РИСКАМИ. Мониторинг предоставляет свидетельства того, что совокупный РИСК для ОСНОВНЫХ СВОЙСТВ в МЕДИЦИНСКОЙ(ИХ) ИТ-СЕТИ(ЯХ) допустим.

УПРАВЛЕНИЕ СОБЫТИЯМИ устанавливает действия, которые выполняются, если в процессе использования МЕДИЦИНСКОЙ ИТ-СЕТИ в условиях эксплуатации произошло реальное или возможное негативное событие.

Приложение В
(справочное)

Обзор отношений при реализации МЕНЕДЖМЕНТА РИСКОВ

На рисунке В.1 представлен обзор различных ролей и отношений, реализуемых при выполнении работ, обеспечивающих МЕНЕДЖМЕНТ РИСКОВ, включая подключение МЕДИЦИНСКИХ ПРИБОРОВ к ИТ-СЕТЯМ.

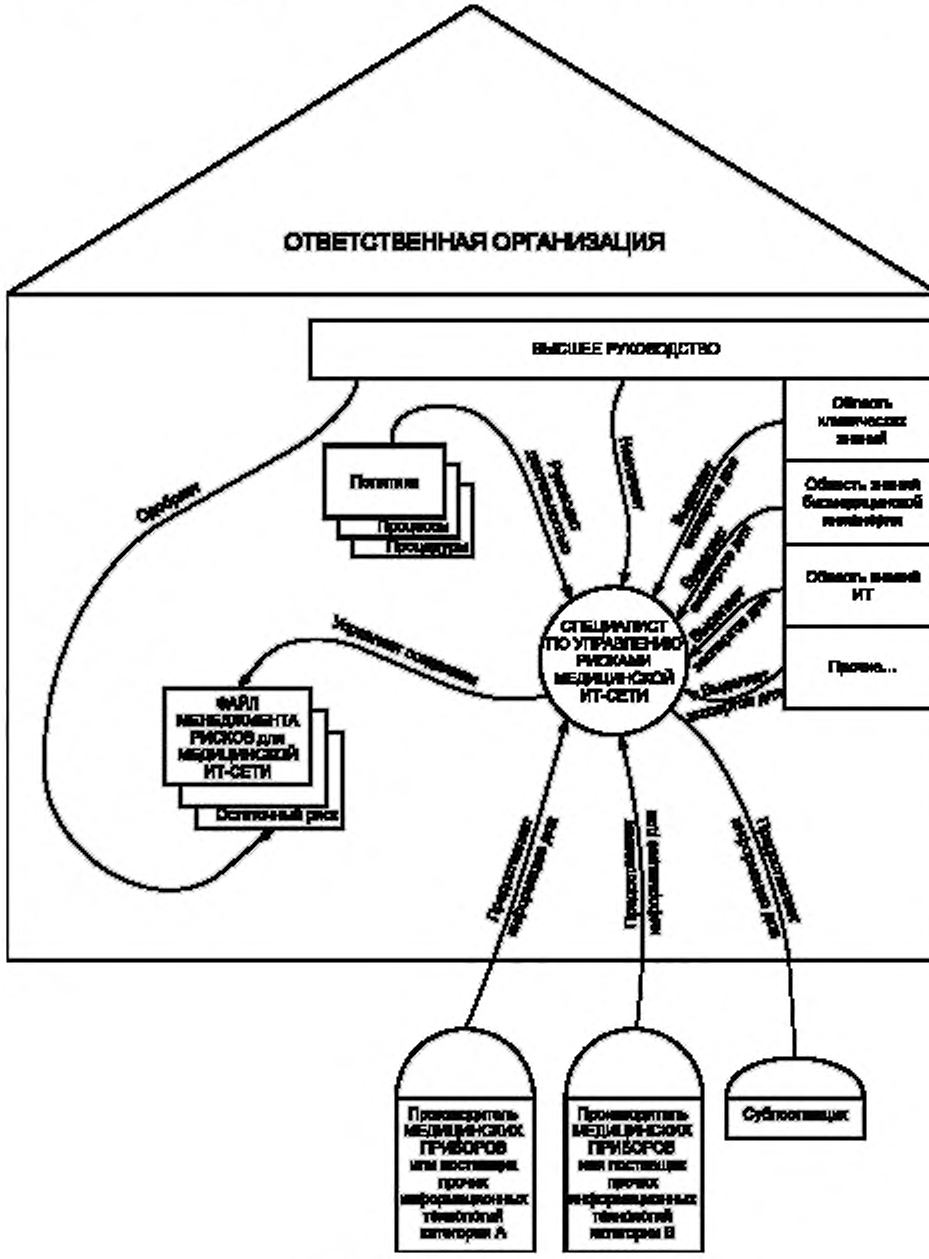


Рисунок В.1 — Обзор ролей и отношений

Приложение С
(справочное)

Об области применения настоящего стандарта

С.1 Обзор

Определение области применения МЭК/ТО 80001-1 является исходной информацией, которая определяет, какие ИТ-СЕТИ входят в область применения настоящего стандарта. В данном приложении представлены дополнительные указания, включая примеры ИТ-СЕТЕЙ, как входящих, так и не входящих в область применения настоящего стандарта.

С.2 Когда применяется настоящий стандарт

В таблице С.1 представлены указания по различным возможным сценариям ИТ-СЕТЕЙ, реализуемым в клинической среде, а также о применении в них ПРОЦЕССОВ, описанных в настоящем стандарте.

Таблица С.1 — Возможные конфигурации ИТ-СЕТЕЙ, которые могут быть реализованы в клинической среде

Конфигурация систем		Описание конфигурации	Компоненты сети	Сеть	Ответственный за сеть	Стандарт
1	a	МЕДИЦИНСКИЕ ПРИБОРЫ одного производителя объединены с НЕМЕДИЦИНСКИМИ ПРИБОРАМИ того же производителя МЕДИЦИНСКИХ ПРИБОРОВ и установлены в соответствии с его требованиями в отдельной ИТ-СЕТИ	МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ одного производителя МЕДИЦИНСКИХ ПРИБОРОВ	Физически изолированная	Производитель МЕДИЦИНСКОГО ПРИБОРА	14971
	b	МЕДИЦИНСКИЕ ПРИБОРЫ различных производителей объединены с НЕМЕДИЦИНСКИМИ ПРИБОРАМИ одного производителя МЕДИЦИНСКИХ ПРИБОРОВ, установленные в соответствии с требованиями этого производителя МЕДИЦИНСКИХ ПРИБОРОВ в отдельной ИТ-СЕТИ	МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ различных производителей МЕДИЦИНСКИХ ПРИБОРОВ	Физически изолированная	Производитель МЕДИЦИНСКОГО ПРИБОРА	14971
2	a	МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ одного производителя МЕДИЦИНСКИХ ПРИБОРОВ и МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ других производителей МЕДИЦИНСКИХ ПРИБОРОВ, соединенные третьей стороной (например, больницей) в одну ИТ-СЕТЬ	МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ различных производителей МЕДИЦИНСКИХ ПРИБОРОВ	Совместно используемая	ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ	80001-1
	b	МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ одного производителя МЕДИЦИНСКИХ ПРИБОРОВ и МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ, другого производителя МЕДИЦИНСКИХ ПРИБОРОВ, а также НЕМЕДИЦИНСКИЕ ПРИБОРЫ и приложения, соединены в совместно используемую ИТ-СЕТЬ третьей стороной	МЕДИЦИНСКИЕ И НЕМЕДИЦИНСКИЕ ПРИБОРЫ различных производителей МЕДИЦИНСКИХ И НЕМЕДИЦИНСКИХ ПРИБОРОВ	Совместно используемая	ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ	80001-1
3		Конфигурации с НЕМЕДИЦИНСКИМИ ПРИБОРАМИ различных производителей, использующие ИТ-СЕТЬ для передачи электронной защищенной медицинской информации	Различные производители НЕМЕДИЦИНСКИХ ПРИБОРОВ	Совместно используемая	ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ	Вне области применения 80001-1[a)]

[a)] Для рассмотренных случаев действуют местные национальные законодательные акты о защите медицинских данных, но ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ может также принять решение применять МЭК 80001-1.

Ниже приведено несколько примеров, которые помогут лучше понять различные конфигурации сетей, описанные в таблице С.1:

- Конфигурация 1a. Устройства наблюдения за пациентом, установленные в его собственной отдельной сети или те же устройства, соединенные шлюзом с больничной ИТ-СЕТЬЮ, предназначенной для НЕМЕДИЦИНСКИХ ПРИБОРОВ;

- Конфигурация 1в. Устройства наблюдения за пациентом от субпоставщика А объединены с подключенными к сети инфузионными устройствами от субпоставщика В и предоставляются одним субпоставщиком (*A*, *B* или *C*) в качестве комплексного управляемого решения;

- Конфигурация 2a. Различные МЕДИЦИНСКИЕ ПРИБОРЫ от разных производителей МЕДИЦИНСКИХ ПРИБОРОВ размещены в больнице и подключены к общей ИТ-СЕТИ;

- Конфигурация 2b. Инфузионные устройства вместе с другими больничными приложениями и/или устройствами наблюдения за пациентом подключены к совместно используемой отдельной ИТ-СЕТИ, которая соединена шлюзом с больничной ИТ-СЕТЬЮ, предназначенной для МЕДИЦИНСКИХ УСТРОЙСТВ, например для аварийного уведомления;

- Конфигурация 3. Больничные системы, обменивающиеся индивидуальными данными пациента и связанной с ним электронной защищенной медицинской информацией (ePHI).

Приложение D
(справочное)

Связь с [10]

D.1 Общие положения

МЭК/ТО 80001-1 использует концепцию жизненного цикла при выполнении МЕНЕДЖМЕНТА РИСКОВ ИТ-СЕТИ, содержащей МЕДИЦИНСКИЕ ПРИБОРЫ. Как и большинство ИТ-СЕТЕЙ, МЕДИЦИНСКИЕ ИТ-СЕТИ могут быть невероятно сложными и динамичными системами, в которых в ходе контроля часто выявляется необходимость изменений. Для реализации таких изменений требуется тщательная подготовка. В связи с тем что производство МЕДИЦИНСКИХ ПРИБОРОВ регулируется положениями законов о системах качества и подтверждения соответствия, в большинстве случаев производители МЕДИЦИНСКИХ ПРИБОРОВ часто не способны достаточно быстро изменять свои МЕДИЦИНСКИЕ ПРИБОРЫ. Согласно регулирующим их правилам и положениям, изменения и обслуживание приборов требуют строго формальных стратегий и процедур, которые, в свою очередь, часто требуют непосредственного привлечения производителя МЕДИЦИНСКИХ ПРИБОРОВ. В случае МЕДИЦИНСКИХ ИТ-СЕТЕЙ и ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ и производитель МЕДИЦИНСКОГО ПРИБОРА должны идентифицировать эти по существу разные ограничения на менеджмент услуг. Помимо этого, подключение МЕДИЦИНСКИХ ПРИБОРОВ может привести к появлению зависимости между МЕДИЦИНСКОЙ ИТ-СЕТЬЮ и МЕДИЦИНСКИМИ ПРИБОРАМИ, в результате которой изменения в одном приводят к необходимости изменений в другом.

МЕНЕДЖМЕНТ РИСКОВ в процессе жизненного цикла МЕДИЦИНСКОЙ ИТ-СЕТИ необходимо осуществлять в привязке к конкретным условиям эксплуатации, необходимым для обеспечения предоставления медицинских услуг. По этой причине концепции управления ИТ-услугами, описанные в [10], были проверены на соответствие требованиям МЭК/ТО 80001-1. В данном приложении приведена простая сводная таблица, демонстрирующая связь между МЭК/ТО 80001-1 и [10], которая может быть полезна при поиске стратегий услуг, которые могут удовлетворять потребности в услугах, выполняемых МЕДИЦИНСКОЙ ИТ-СЕТЬЮ. Данная информация также предназначена помочь в переговорах сторон, несущих ответственность за ИТ-СЕТИ и МЕДИЦИНСКИЕ ПРИБОРЫ (т. е. переговоров между ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ, производителем МЕДИЦИНСКИХ ПРИБОРОВ и поставщиками других информационных технологий).

Соответствие с [10] не эквивалентно соответствию с МЭК/ТО 80001-1.

D.2 Терминология и определения

Если МЕДИЦИНСКИЕ ПРИБОРЫ требуют обслуживания, ремонта, модификации и в итоге замены, то у ИТ-СЕТЕЙ возникают инциденты и проблемы, которые необходимо разрешать, а также необходимость в серьезных изменениях, требующих тщательной реализации. Есть много общего в обслуживании и МЕДИЦИНСКОГО(ИХ) ПРИБОРА(ОВ), и ИТ-СЕТИ(ЕЙ). Для сравнения на рисунке D.1, взятом из [10], показана связь между процессами предоставления услуг ИТ-СЕТЯМИ.



Рисунок D.1 — Процессы управления услугами ([10], рисунок 1)

Таблица D.1 связывает терминологию и разделы МЭК/ТО 80001-1 с терминологией и разделами [10]. Номера соответствуют разделам стандартов.

Таблица D.1 — Связь между настоящим стандартом и [9] или [10]

МЭК/ТО 80001-1	[9] или [10]
2.4 УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ В МЭК/ТО 80001-1 УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ является процессом, который хранится в базе данных управления конфигурациями (CMDB)	2.5 База данных управления конфигурациями CMDB — это база данных, применяющаяся для управления конфигурациями [9]
2.7 УПРАВЛЕНИЕ СОБЫТИЯМИ Природа событий не определена в МЭК/ТО 80001-1. Эти события связаны, как и с ИТ-СЕТЬЮ так и с МЕДИЦИНСКИМ ПРИБОРОМ	2.7 Инцидент Инцидент и проблема связаны с событиями, которыми занимается УПРАВЛЕНИЕ СОБЫТИЯМИ в МЭК/ТО 80001-1 [9]
2.21 СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ Соглашение между, например, поставщиками, производителями, поставщиками услуг, специалистом по системной интеграции и ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ	2.13 Соглашение об уровне услуг 2.14 Управление услугами Определяют связь между владельцем ИТ сети и поставщиком услуг. [9]
2.22 ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ	2.15 Поставщик услуг ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ, согласно ее политике, обязана сертифицировать поставщика услуг по ИТ-СЕТИ. [9]
2.29 ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ	2.9 Запись; 2.3 запись об изменении; 2.11 запрос на изменение. Элемент(ы) ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ. 2.5 База данных управления конфигурациями (CMBD) Элемент ФАЙЛА МЕНЕДЖМЕНТА РИСКОВ (описание актива). Примечание — ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ может храниться в базе данных, которая включает в себя CMBD. [9]
3.3 Ответственности РУКОВОДСТВА	3.1 Ответственность руководства Оба стандарта рассматривают ответственности руководителей старшего звена. [9] и [10] предоставляют больше организационной свободы
3.4 СПЕЦИАЛИСТ по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ Специалист по управлению РИСКАМИ несет ответственность за ПРОЦЕСС МЕНЕДЖМЕНТА РИСКОВ	3.1 Ответственность руководства МЕНЕДЖМЕНТ РИСКОВ не является задачей, специально возложенной на руководство. 6.6.7 Документы и записи Записи должны подвергаться анализу. В МЭК/ТО 80001-1 эта ответственность возложена на СПЕЦИАЛИСТА по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ. [10]
3.5 Производитель(и) МЕДИЦИНСКИХ ПРИБОРОВ 3.6 Поставщики прочих информационных технологий Данный раздел устанавливает, какую информацию должны предоставлять поставщики для ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ	7.1 Процесс взаимоотношений. Общие положения 6.6.5 Безопасность и доступность информации [9] 7.3 Управление поставщиками Оба стандарта требуют формализации отношений посредством контракта. Разделы 6.6.5 и 7.3 затрагивают поставщиков компонентов МЕДИЦИНСКОЙ ИТ-СЕТИ
4.2.1 Политика МЕНЕДЖМЕНТА РИСКОВ для подключения МЕДИЦИНСКИХ ПРИБОРОВ	3.1 Ответственность руководства

Продолжение таблицы D.1

МЭК/ТО 80001-1	[9] или [10]
4.2.2 ПРОЦЕСС МЕНЕДЖМЕНТА РИСКОВ Охватывает БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ	6.6.3 Практическая деятельность по оценке рисков, связанных с защитой [9] Защита является одним из ОСНОВНЫХ СВОЙСТВ МЕДИЦИНСКОЙ ИТ-СЕТИ. МЭК/ТО 80001-1 описывает общий ПРОЦЕСС МЕНЕДЖМЕНТА РИСКОВ ИТ-СЕТИ
4.3 Планирование и документальное оформление МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ	4.1 Планирование управления услугами (План) 4.4.2 Управление усовершенствованиями 5.1 Вопросы для анализа ИСО/МЭК 20000 может включать в себя МЕНЕДЖМЕНТ РИСКОВ. МЭК/ТО 80001-1 определяет требования к управлению услугами МЕДИЦИНСКИХ ИТ-СЕТЕЙ
4.3.2 Описание ресурсов, связанных с РИСКОМ	6.6.2 Идентификация и классификация информационных ресурсов Область применения должна учитывать все ОСНОВНЫЕ СВОЙСТВА
4.3.3 Документация на МЕДИЦИНСКУЮ ИТ-СЕТЬ Данный пункт определяет информацию, связанную с ПРОЦЕССОМ МЕНЕДЖМЕНТА РИСКОВ	4.1.1 Область применения управления услугами 6.6.2 Идентификация и классификация информационных ресурсов Содержание данной информации пересекается с 4.3.3 в МЭК/ТО 80001-1
4.3.4 СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ	7.3 Управление поставщиками (1ый параграф) Оба раздела предназначены для прояснения целей сотрудничества всем заинтересованным сторонам
4.3.5 План МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ	6.6.3 Практика оценки рисков, связанных с защитой Защита является одним из ОСНОВНЫХ СВОЙСТВ МЕДИЦИНСКОЙ ИТ-СЕТИ. МЭК/ТО 80001-1 описывает общий ПРОЦЕСС МЕНЕДЖМЕНТА РИСКОВ ИТ-СЕТИ
4.4.4 УПРАВЛЕНИЕ РИСКОМ	9.1.5 Верификация и аудит конфигурации 9.2.1 Планирование и реализация ИСО/МЭК 20000 охватывает множество элементов, требующих ВЕРИФИКАЦИИ. ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ детально рассмотрена в МЭК/ТО 80001-1
4.5 УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ	9 Процессы управления 10 Процесс выпуска версии Управление изменениями и конфигурацией, а также выпуск версий и запуск в эксплуатацию рассмотрены в разделах 9 и 10. Эти действия включены в ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКОВ, описанные в разделе 4 МЭК/ТО 80001-1
4.5.2.3 Проекты МЕДИЦИНСКОЙ ИТ-СЕТИ При серьезных изменениях в проекте требуется оценка РИСКА этих изменений до их реализации	9.2.1 Планирование и реализация ИСО/МЭК 20000 выделяет все изменения, которые должны быть запланированы до их реализации. МЭК/ТО 80001-1 требует для всех изменений осуществление МЕНЕДЖМЕНТА РИСКОВ, включающего в себя планирование
4.5.3 Ввод в эксплуатацию	9.2.1 Планирование и реализация 10.1.6 Верификация и приемка выпускаемой версии МЭК/ТО 80001-1 возлагает ответственность за ввод в эксплуатацию на СПЕЦИАЛИСТА по УПРАВЛЕНИЮ РИСКАМИ в МЕДИЦИНСКОЙ ИТ-СЕТИ

Окончание таблицы D.1

МЭК/ТО 80001-1	[9] или [10]
4.6.1 Контроль	10.1.8 Внедрение, передача и установка 10.1.9 Действия после выпуска и внедрения Контроль может относиться, как к организационным, так и к техническим мерам по УПРАВЛЕНИЮ РИСКОМ
5.1 Процедура управления документацией	3.2 Требования к документации
5.2 ФАЙЛ МЕНЕДЖМЕНТА РИСКОВ МЕДИЦИНСКОЙ ИТ-СЕТИ	5.2 Записи об изменениях 6.6.7 Документы и записи 10.1.7 Документация

Библиография

[1] IEC 60601-1:2005, Medical electrical equipment — Part 1: General requirements for basic safety and essential performance

[2] IEC 61907:2009, Communication network dependability engineering

[3] IEC 62304:2006, Medical device software — Software life-cycle processes

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

[5] ISO/IEC 15026-2:2011, Systems and software engineering — Systems and software assurance — Part 2: Assurance case

[6] ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

[7] ISO 16484-2:2004, Building automation and control systems (BACS) — Part 2: Hardware

[8] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary

[9] ISO/IEC 20000-1:2005, Information technology — Service management — Part 1:Specification

[10] ISO/IEC 20000-2:2005, Information technology — Service management — Part 2: Code of practice

[11] ISO 31000:2009, Risk management — Principles and guidelines

[12] GHTF/SG1/N29R16:2005, Information Document Concerning the. Definition of the Term «Medical Device». Global Harmonization Task Force (GHTF) — Study Group 1 (SG1)

УДК 004:61:006.354 ОКС 11.040.01 35.240.80 П85 ОКСТУ 4002

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

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *В.И. Варенцова*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 26.04.2016. Подписано в печать 04.05.2016. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,10. Тираж 30 экз. Зак. 1227.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ» 123995 Москва, Гранатный пер., 4
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru