ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56839— 2015/IEC/TR 80001-2-1:2012

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-1

Пошаговый менеджмент рисков медицинских информационно-вычислительных сетей. Практическое применение и примеры

(IEC/TR 80001-2-1:2012,
Application of risk management for IT-networks incorporating medical devices — Part 2-1. Step-by-step risk management of medical IT-networks — Practical applications and examples, IDT)

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2015 г. № 2227-ст

4 Настоящий стандарт идентичен международному документу IEC/TR 80001-2-1:2012 «Применение менеджмента рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 2-1. Пошаговый менеджмент рисков медицинских информационно-вычислительных сетей. Практическое применение и примеры» (IEC/TR 80001-2-1:2012 «Application of risk management for IT-networks incorporating medical devices — Part 2-1. Step-by-step risk management of medical IT-networks — Practical applications and examples», IDT).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Январь 2019 г.

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

© Стандартинформ, оформление, 2016, 2019

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Предварительные требования . . . 5
5 Ознакомление с терминами, используемыми в МЕНЕДЖМЕНТЕ РИСКА . . . 5
5.1 Обзор . . . 5
5.2 ОПАСНОСТИ . . . 6
5.3 ОПАСНЫЕ СИТУАЦИИ . . . 6
5.4 Предсказуемые последовательности событий и причин . . . 7
5.5 НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ . . . 7
5.6 Меры УПРАВЛЕНИЯ РИСКОМ (снижение РИСКОВ) . . . 8
5.7 Степень РИСКА . . . 8
5.8 Проверка формулировок . . . 9
6 Шаги . . . 9
6.1 Обзор шагов . . . 9
6.2 Базовый пример использования 10 шагов . . . 9
7 МЭК 80001-1:2010, подраздел 4.4. Последовательность шагов . . . 13
7.1 Общие положения . . . 13
7.2 Применение требований, представленных в 4.4.1. Документальное оформление всех элементов МЕНЕДЖМЕНТА РИСКА . . . 13
7.3 Примечание к ОЦЕНКЕ РИСКА . . . 13
7.4 10-шаговый ПРОЦЕСС . . . 13
7.5 Рассмотренные шаги и их связь с МЭК 80001-1 и ИСО 14971 . . . 20
8 Практические примеры . . . 21
8.1 Общие положения . . . 21
8.2 Пример 1. Беспроводной контроль ПАЦИЕНТА во время его транспортировки . . . 21
8.3 Пример 2. Удаленное отделение интенсивной терапии (ОИТ)/Дистанционное медицинское обслуживание . . . 24
8.4 Пример 3. Палата послеанестезиологической помощи (PACU) . . . 26
8.5 Пример 4. Ультразвук. Уязвимость в операционной системе (ОС) . . . 32
Приложение А (справочное) Распространенные ОПАСНОСТИ, ОПАСНЫЕ СИТУАЦИИ и их причины, которые следует учесть при работе с МЕДИЦИНСКИМИ ИТ-СЕТЯМИ . . . 35
Приложение В (справочное) Список вопросов, которые следует рассмотреть во время идентификации ОПАСНОСТЕЙ МЕДИЦИНСКОЙ ИТ-СЕТИ . . . 39
Приложение С (справочное) Уровни МЕДИЦИНСКИХ ИТ-СЕТЕЙ, на которых могут встречаться ошибки . . . 40
Приложение D (справочное) Шкалы вероятности, тяжести и допустимости РИСКА, используемые в примерах настоящего стандарта . . . 42
Приложение Е (справочное) КОНТРОЛЬ эффективности ослабления РИСКА . . . 45
Приложение F (справочное) АНАЛИЗ РИСКА для небольших изменений в МЕДИЦИНСКОЙ ИТ-СЕТИ . . . 47
Приложение G (справочное) Пример формы временного окна для изменения . . . 48
Приложение Н (справочное) Шаблон для примеров . . . 49
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам . . . 51
Библиография . . . 52

Введение

Настоящий стандарт представляет собой пошаговое руководство по применению МЕНЕДЖМЕНТА РИСКА для создания и изменения МЕДИЦИНСКОЙ ИТ-СЕТИ. В нем представлены легко применяемые шаги, примеры и информация, помогающая при выявлении и управлении РИСКАМИ. В настоящем стандарте рассмотрены все соответствующие требования МЭК 80001-1:2010, а также там, где необходимо, ссылки на другие разделы и подразделы МЭК 80001-1 (например, передача управлению версиями и контролю).

В центре настоящего стандарта — МЕНЕДЖМЕНТ РИСКА. Целью настоящего стандарта не является предоставление полного описания или объяснения всех требований, которые в полной мере рассмотрены в МЭК 80001-1.

Настоящий стандарт рассматривает ПРОЦЕСС, состоящий из 10 шагов, основанный на подразделе 4.4 МЭК 80001-1:2010, который непосредственно ориентирован на АНАЛИЗ РИСКА, ОЦЕНИВАНИЕ РИСКА и УПРАВЛЕНИЕ РИСКОМ. Данные действия входят в ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА для всего жизненного цикла. Они не могут служить первым шагом ПРОЦЕССА, так как МЕНЕДЖМЕНТ РИСКА охватывает всю модель ПРОЦЕССА, в которой всякому действию предшествует планирование.

Согласно подразделу 1.3, для соответствия цели настоящего стандарта должны выполняться «необходимые предварительные условия» до выполнения 10 шагов. Также очевидно, что все выделенные в настоящем стандарте шаги должны быть выполнены до того момента, когда становится возможным запуск любой новой МЕДИЦИНСКОЙ ИТ-СЕТИ в эксплуатацию или до внесения изменения в существующую МЕДИЦИНСКУЮ ИТ-СЕТЬ. Подчеркивается, что подраздел 4.5 МЭК 80001-1:2010 «УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ» посвящен и применяется непосредственно к новым МЕДИЦИНСКИМ ИТ-СЕТЯМ, а также к внесению изменений в существующие сети.

Настоящий стандарт будет полезен лицам, ответственным за команду или являющимся частью команды, осуществляющей МЕНЕДЖМЕНТ РИСКА в процессе изменения или создания (что является крайним изменением) МЕДИЦИНСКОЙ ИТ-СЕТИ. МЕДИЦИНСКИЕ ПРИБОРЫ, рассматриваемые в контексте МЭК 80001, относятся к тем МЕДИЦИНСКИМ ПРИБОРАМ, которые могут быть подключены к сети.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ РИСКОВ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ С МЕДИЦИНСКИМИ ПРИБОРАМИ

Часть 2-1

Пошаговый менеджмент рисков медицинских информационно-вычислительных сетей. Практическое применение и примеры

Health informatics. Risk management for IT-networks incorporating medical devices.
Part 2-1. Step-by-step risk management of medical IT-networks. Practical applications and examples

Дата введения — 2016—11—01

1 Область применения

Настоящий стандарт содержит пошаговую информацию, предназначенную помочь ОТВЕТСТВЕННЫМ ОРГАНИЗАЦИЯМ в реализации ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА в соответствии с требованиями МЭК 80001-1. А именно: детальный разбор шагов, требующихся для реализации подраздела 4.4 МЭК 80001-1:2010, а также руководство в форме рассмотрения терминов МЕНЕДЖМЕНТА РИСКА, шагов МЕНЕДЖМЕНТА РИСКА, объяснения каждого шага, рассмотрения примеров для каждого шага, шаблонов, а также списков ОПАСНОСТЕЙ и их причин, которые следует рассмотреть.

Шаги, определенные в настоящем стандарте, считаются универсально применимыми. Применение данных шагов может масштабироваться, как это описано в настоящем стандарте.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок следует применять только указанное издание. Для недатированных — последнее издание ссылочного стандарта (включая любые поправки):

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

3 Термины и определения

В настоящем стандарте применены следующие термины и определения:

3.1 **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.

[МЭК 80001-1:2010, статья 2.3]

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

[МЭК 80001-1:2010, статья 2.2]

Издание официальное

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

[МЭК 80001-1:2010, статья 2.4]

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

[МЭК 80001-1:2010, статья 2.5]

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

[МЭК 80001-1:2010, статья 2.6]

3.6 **ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ** (ЭМП) [ELECTROMAGNETIC INTEFERENCE (EMI)]: Любое электромагнитное явление, способное негативно сказаться на функционировании прибора, оборудования или системы.

[МЭК 60601-1-2:2007, статья 3.5]

3.7 **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.

[МЭК 80001-1:2010, статья 2.7]

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

[МЭК 80001-1:2010, статья 2.8]

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

[МЭК 80001-1:2010, статья 2.9]

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

[МЭК 14971:2007, статья 2.4]

3.11 **ДАННЫЕ О ЗДОРОВЬЕ** (HEALTH DATA): ЛИЧНЫЕ ДАННЫЕ, указывающие на состояние физического или психического здоровья.

Примечание — Вышеописанное в общих чертах определяет в рамках настоящего стандарта личные данные и их подраздел ДАННЫЕ О ЗДОРОВЬЕ, что позволяет пользователям настоящего стандарта легко применять эти понятия к разным нормативным актам и регламентам о конфиденциальности данных. Например, в Европе такие требования могут быть приняты, а термин может быть заменен на «Персональные данные» и «Уязвимые данные». В США термин ДАННЫЕ О ЗДОРОВЬЕ может быть заменен на «Защищенную информацию о здоровье (PHI)», а также при необходимости могут быть внесены поправки и в сам текст.

[МЭК 80002-2:2012, статья 3.7]

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

[МЭК 80001-1:2010, статья 2.10]

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

[МЭК 80001-1:2010, статья 2.11]

3.14 **ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ** (IT): Технология (компьютерные системы, сети, программное обеспечение), использующаяся для ОБРАБОТКИ, хранения, сбора и распространения информации.

3.15 **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.

[МЭК 80001-1:2010, статья 2.12]

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

[МЭК 80001-1:2010, статья 2.13]

3.17 **ЛОКАЛЬНАЯ СЕТЬ** (LOCAL AREA NETWORK): Компьютерная сеть, охватывающая маленькую физическую область, такую как дом или офис, или же маленькую группу зданий, такую как школа или аэропорт.

3.18 **ПРОИЗВОДИТЕЛЬ** (MANUFACTURER): Физическое или юридическое лицо, ответственное за проектирование, изготовление, упаковывание и/или маркировку МЕДИЦИНСКОГО ПРИБОРА, сборку системы или модификацию медицинского прибора перед выпуском его на рынок или вводом в эксплуатацию, независимо от того, выполняет ли эти операции вышеупомянутое лицо или третья сторона от его имени.

[ИСО 14971:2007, статья 2.8]

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

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

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

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

Примечания

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

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

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

3 Аксессуары, специально предназначенные производителями для использования совместно с медицинским прибором, для которого они 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 включаются в определение «медицинский прибор».

[МЭК 80001-1:2010, статья 2.14]

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

[МЭК 80001-1:2010, статья 2.16]

3.21 **КОНТРОЛЬ** (MONITORING): Непрерывный надзор за деятельностью по МЕНЕДЖМЕНТУ РИСКА и возможностями УПРАВЛЕНИЯ РИСКОМ, выбранными для достижения доступного РИСКА при использовании МЕДИЦИНСКИХ ИТ-СЕТЕЙ.

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

[МЭК 80001-1:2010, статья 2.18]

3.23 **ПАЦИЕНТ** (PATIENT): Человек, ожидающий медицинской помощи или получающий ее.

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

[МЭК 80001-1:2010, статья 2.19]

3.25 **КАЧЕСТВО ОБСЛУЖИВАНИЯ** (QUALITY OF SERVICE, QoS): Возможность или средства обеспечения производительности сети на различных уровнях с помощью управления трафиком (задержкой, потерей, искажением пакета, скоростью передачи данных в бит/сек) различных потоков данных.

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

[МЭК 80001-1:2010, статья 2.20]

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

[МЭК 80001-1:2010, статья 2.21]

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

[МЭК 80001-1:2010, статья 2.23]

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

[МЭК 80001-1:2010, статья 2.23]

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

[МЭК 80001-1:2010, статья 2.24]

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

[МЭК 80001-1:2010, определение 2.25]

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

[МЭК 80001-1:2010, статья 2.26]

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

[МЭК 80001-1:2010, статья 2.27]

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

[МЭК 80001-1:2010, статья 2.28]

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

[МЭК 80001-1:2010, статья 2.29]

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

[МЭК 80001-1:2010, статья 2.30]

3.37 **ВЫСШЕЕ РУКОВОДСТВО** (TOP MANAGEMENT): Лицо или группа работников, осуществляющих направление деятельности и управление ОТВЕСТВЕННОЙ ОРГАНИЗАЦИЕЙ, отвечающих за МЕДИЦИНСКУЮ ИТ-СЕТЬ на самом высоком уровне.

[МЭК 80001-1:2010, статья 2.31]

3.38 **НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ** [UNINTENDED CONSEQUENCE (UC)]: Нежелательный и негативный исход события, приводящий к ухудшению одного и более ОСНОВНЫХ СВОЙСТВ.

3.39 **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;
- анализ документов до их выпуска.

[ИСО 14971:2007, статья 2.28]

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

[МЭК 80001–1:2010, статья 2.32]

4 Предварительные требования

Перед тем как приступить к выполнению шагов, определенных в настоящем стандарте, должны быть соблюдены требования подразделов 3.1—4.3 МЭК 80001-1:2010. Кроме того, ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ (ОО) должна быть готова выполнить требования, представленные в подразделах 4.5—5.2. Необходимо, например, чтобы были установлены политика и ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКА; завершен план МЕНЕДЖМЕНТА РИСКА; составлены все требующиеся СОГЛАШЕНИЯ ОБ ОТВЕТСТВЕННОСТИ; определены масштабы вероятности, тяжести и допустимости РИСКА.

Для выполнения МЕНЕДЖМЕНТА РИСКА любой системы она должна быть определена. В случае МЕДИЦИНСКИХ ИТ-СЕТЕЙ подвергающаяся анализу сеть должна быть хорошо определена и может даже содержать некоторые существующие механизмы управления. Это важно для шагов 3 и 4. Для новых МЕДИЦИНСКИХ СЕТЕЙ это выполняется в рамках технического проекта.

В дополнение к определению анализируемой системы для выполнения предварительной оценки РИСКА требуется фундаментальная информация, касающаяся конкретной цели ОО, ее нужд и проблем. Все это называется «контекстом» использования и включает в себя следующую информацию:

- тяжесть состояния больных (необходимость интенсивной терапии);
- рабочий процесс медицинского учреждения;
- медицинский персонал и уровень его квалификации;
- сценарий ПРЕДУСМОТРЕННОГО/клинического или бизнес-применения;
- клиническую и бизнес-важность систем/приложений, использующих сеть.

Данные шаги, описанные в настоящем стандарте, как правило, выполняются командой, состоящей из членов ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Рекомендуется собирать такую команду из представителей различных отделов, включая отделы ИТ, биомедицинской инженерии, медицинский отдел и отдел МЕНЕДЖМЕНТА РИСКА. Состав команды должен соответствовать существующим внутри организации структурным подразделениям.

5 Ознакомление с терминами, используемыми в МЕНЕДЖМЕНТЕ РИСКА

5.1 Обзор

МЕНЕДЖМЕНТ РИСКА является очень большой областью для исследования. Настоящий стандарт предоставляет введение в эту область с использованием примеров, для понимания которых требуются минимальные знания. В нем содержатся пошаговые инструкции для выполнения ПРОЦЕССА ОЦЕНКИ РИСКА.

МЭК 80001-1 описывает философию МЕНЕДЖМЕНТА РИСКА. Так как существует несколько доступных философий МЕНЕДЖМЕНТА РИСКА, данная философия может как совпадать, так и частично противоречить методам и технике МЕНЕДЖМЕНТА РИСКА, уже использующимся в ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ (ОО). ОО следует принять соответствующие меры для устранения разногласий между методологией и терминологией.

На рисунке 1 показан базовый набор основных понятий от ОПАСНОСТИ к ОПАСНОЙ СИТУАЦИИ и до НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ.

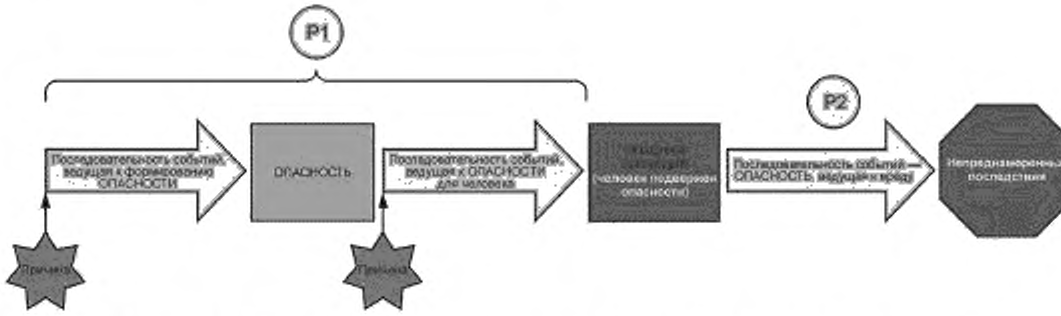


Рисунок 1 — Базовый набор основных понятий от ОПАСНОСТИ к ОПАСНОЙ СИТУАЦИИ и до НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

5.2 ОПАСНОСТИ

МЭК 80001-1 рассматривает ОСНОВНЫЕ СВОЙСТВА (БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ И ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМЫ), каждое из этих свойств может быть подвержено одной или нескольким ОПАСНОСТЯМ и ОПАСНЫМ СИТУАЦИЯМ.

ОПАСНОСТИ необходимо рассматривать как категории сущностей, которые могут неблагоприятно влиять на одно или более ОСНОВНЫХ СВОЙСТВ. Конкретными примерами могут служить электрическая энергия, подвешенные массы, высокие температуры и т. п., но функциональные отказы и отказы в процессе работы также должны рассматриваться как ОПАСНОСТИ. Например, отказ включения дефибриллятора, когда он требуется, представляет собой опасность. В случае МЕДИЦИНСКИХ ИТ-СЕТЕЙ многие из ОПАСНЫХ СИТУАЦИЙ, которые могут возникнуть, связаны с ОПАСНОСТЬЮ «потери работоспособности» (например, МЕДИЦИНСКАЯ ИТ-СЕТЬ не осуществляет передачу данных).

ОПАСНОСТИ организованы иерархически. Например, рассматривая ОПАСНОСТЬ «энергии», ее можно разделить на тепловую, механическую и электрическую энергии, которые в свою очередь тоже являются ОПАСНОСТЯМИ. При дальнейшей декомпозиции получим высокую температуру, вращение и высокое напряжение, которые также являются ОПАСНОСТЯМИ. Такой иерархический подход позволяет организовать АНАЛИЗ РИСКА и соответствующую документацию. Например, высокие температуры в шкафу коммуникаций могут послужить причиной отказов в ИТ-оборудовании. ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ также могут приводить к отказам в ИТ-СЕТЯХ.

Многие ОПАСНОСТИ заложены в свойства прибора или системы, в то время как некоторые появляются на протяжении жизни системы. Например, высокая температура — это ОПАСНОСТЬ. Варочная поверхность должна быть горячей (свойство, присущее системе), но перегретая поверхность машины может быть результатом отказа в ней. В качестве еще одного примера могут служить острые края, которые также являются видом ОПАСНОСТИ. Нож предназначен быть острым, но металлический заусенец на металлическом корпусе может образоваться в процессе изготовления. Потеря работоспособности сети как ОПАСНОСТЬ может возникнуть во время использования сетевых приборов.

5.3 ОПАСНЫЕ СИТУАЦИИ

ОПАСНОСТЬ является возможным источником НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ. Острый нож, покрытый льдом пешеходный тротуар, даже метель может считаться ОПАСНОСТЬЮ. ОПАСНАЯ СИТУАЦИЯ — это обстоятельства, при которых люди, имущество или окружающая среда подвержены одной или нескольким ОПАСНОСТЯМ. Для того чтобы НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ были возможны, должна сформироваться ОПАСНАЯ СИТУАЦИЯ. Например, если никто не ходит по покрытому льдом пешеходному тротуару (нет ОПАСНОЙ СИТУАЦИИ), то покрытый льдом пешеходный тротуар по-прежнему будет являться ОПАСНОСТЬЮ, но НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ не будет, если не возникает ОПАСНАЯ СИТУАЦИЯ.

Множество разных ОПАСНЫХ СИТУАЦИЙ может образоваться по причине одной ОПАСНОСТИ, и у каждой будет свой уровень РИСКА. Например, в случае ОПАСНОСТИ «потеря способности к подключению» может возникнуть несколько ОПАСНЫХ СИТУАЦИЙ, таких как отказ при попытке обновить медицинские записи, задержка передачи новых указаний врача, отсутствие возможности определения правильности работы оборудования, отсутствие возможности обновить формуляр на инфузионном насосе IV, отказ при передаче активного аварийного сигнала и т. п.

С учетом предоставленной в ОПАСНОЙ СИТУАЦИИ информации, а также определения МЕДИЦИНСКОЙ ИТ-СЕТИ и контекста (сценария медицинского применения, рабочего процесса/функционирования медицинского учреждения, остроты заболевания пациента, уязвимости данных и т. п.), можно определить НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ. При потере способности к подключению информация о том, какие данные были потеряны и кому они принадлежали, является важным фактором в определении НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ. Риск от потери данных об аварийных сигналах в случае пациента, нуждающегося в интенсивной терапии, будет отличаться от РИСКА, возникающего при потере электронной медицинской карты в поликлинике.

5.4 Предсказуемые последовательности событий и причин

Предсказуемая последовательность событий преобразует ОПАСНОСТЬ в ОПАСНУЮ СИТУАЦИЮ. Последовательность событий может также привести к ОПАСНОСТИ, не «заложенной» в МЕДИЦИНСКОЙ ИТ-СЕТИ, а затем и к ОПАСНОЙ СИТУАЦИИ. Исходное событие называется «причиной». В случае МЕДИЦИНСКОЙ ИТ-СЕТИ причиной может послужить перегрузка сети, которая приводит к ОПАСНОСТИ, такой как потеря способности к подключению. ОПАСНАЯ СИТУАЦИЯ возникает, когда пациент или организация подвергаются ОПАСНОСТИ, которая может повлечь за собой возможное негативное влияние на одно или более из трех ОСНОВНЫХ СВОЙСТВ.

Причина отвечает на вопрос: «почему кто-то/что-то оказались в ОПАСНОЙ СИТУАЦИИ?» Для простоты представьте причину в виде точки, в которой возникли трудности (ошибка проектирования, отказ компонента сети и т. п.), и в этой же точке могут быть эффективно применены меры по УПРАВЛЕНИЮ РИСКОМ.

5.5 НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ

ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА, использованный в МЭК 80001-1, основан на ПРОЦЕССЕ МЕНЕДЖМЕНТА РИСКА по ИСО 14971. Важно отметить, что область действия РИСКОВ, рассмотренная в МЭК 80001-1 и в настоящем стандарте, шире, чем в ИСО 14971, хотя и там, и там используются идентичные термины. ВРЕД, согласно определению ИСО 14971, связан только с БЕЗОПАСНОСТЬЮ из всех ОСНОВНЫХ СВОЙСТВ МЭК 80001 (физической травмой), в то время как в МЭК 80001-1 ВРЕД распространяется на все три ОСНОВНЫХ СВОЙСТВА: БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМЫ. Чтобы избежать интерпретации одной предметной области МЕНЕДЖМЕНТА РИСКА (включающей только БЕЗОПАСНОСТЬ), настоящий стандарт объясняет МЕНЕДЖМЕНТ РИСКА, используя более нейтральный термин — «НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ» (или НП). Физическая травма в таком случае будет НЕПРЕДНАМЕРЕННЫМ ПОСЛЕДСТВИЕМ РИСКА для БЕЗОПАСНОСТИ. Помимо физической травмы ОПАСНОСТЬ может также служить возможным источником нарушения защиты или сниженной эффективности. МЕНЕДЖМЕНТ РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ требует множество различных дисциплин, в которых используются зависящие от предметной области термины, касающиеся РИСКА, МЕНЕДЖМЕНТА РИСКА или ОПАСНОСТЕЙ. Термин «НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ» применяется в настоящем стандарте в качестве термина общего описания.

В таблице 1 представлен обзор связи между используемыми терминами.

Таблица 1 — Связь между ОСНОВНЫМИ СВОЙСТВАМИ, БЕЗОПАСНОСТЬЮ, ЭФФЕКТИВНОСТЬЮ И ЗАЩИЩЕННОСТЬЮ ДАННЫХ И СИСТЕМЫ и соответствующими НЕПРЕДНАМЕРЕННЫМИ ПОСЛЕДСТВИЯМИ в том виде, в котором она применяется в настоящем стандарте

ОСНОВНОЕ СВОЙСТВО	БЕЗОПАСНОСТЬ	ЭФФЕКТИВНОСТЬ	ЗАЩИЩЕННОСТЬ СИСТЕМЫ И ДАННЫХ
Определение ОСНОВНОГО СВОЙСТВА	Отсутствие недопустимой комбинации вероятности и тяжести физической травмы или ущерба здоровью людей, ущерба имуществу или окружающей среде	Способность достигать желаемых результатов по отношению к пациенту и ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ	Рабочее состояние МЕДИЦИНСКОЙ ИТ-СЕТИ, при котором информационные средства (данные и системы) в достаточной степени защищены от нарушения конфиденциальности, полноты и доступа
Описание НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ	Физическая травма или ущерб здоровью людей, ущерб имуществу или окружающей среде	Снижение ЭФФЕКТИВНОСТИ	Нарушение ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ

Для более подробного анализа связи между защитой ИТ и терминами МЕНЕДЖМЕНТА РИСКА для БЕЗОПАСНОСТИ см. МЭК/ТО 80001-2-2. Фраза «Нарушение ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ» имеет примерно то же самое значение, что и вторжение в область ИТ-защиты (например, защиты от кибератак). Системная уязвимость — системный признак, который, при очевидной годности системы для использования, становится ОПАСНОСТЬЮ, которая может в свою очередь привести к событию нарушения. Хотя иногда уязвимости и ВРЕД следуют друг за другом в повседневном использовании, уязвимости могут привести к ВРЕДУ, но не могут рассматриваться как непосредственная опасность, однако они могут рассматриваться как угроза иметь более ощутимую, непосредственную опасность с возможностью ВРЕДА [создать ОПАСНУЮ СИТУАЦИЮ для ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ (например, уязвимость системы, эксплуатация которой ведет к значительным последствиям)].

Информацию по вопросу применения МЕНЕДЖМЕНТА РИСКА для защищенности на организационном уровне можно найти в ИСО/МЭК 27001:2005, ИСО/МЭК 27002:2005, ИСО/МЭК 27799:2008. Для случаев подключения МЕДИЦИНСКОГО ПРИБОРА к ИТ-СЕТИ могут быть использованы ПРОЦЕССЫ МЕНЕДЖМЕНТА РИСКА для ИТ-защищенности из стандарта ИСО/МЭК 27005:2011, которые могут быть адаптированы, чтобы дополнить основанный на ИСО 14971 ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА из МЭК 80001-1 (то есть БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМЫ).

5.6 Меры УПРАВЛЕНИЯ РИСКОМ (снижение РИСКОВ)

Меры по УПРАВЛЕНИЮ РИСКОМ также называются мерами снижения РИСКОВ. Меры снижения РИСКОВ могут применяться для уменьшения вероятности возникновения ОПАСНОЙ СИТУАЦИИ (уменьшение Р1 на рисунке 1). Кроме того, принимая во внимание ОПАСНУЮ СИТУАЦИЮ, средства УПРАВЛЕНИЯ РИСКОМ могут также применяться для ограничения вероятности возникновения НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ, возникающих по причине ОПАСНОЙ СИТУАЦИИ (уменьшение Р2 на рисунке 1).

Например, прерывание соединения может привести к ОПАСНОЙ СИТУАЦИИ, в которой дежурный лечащий врач не будет уведомлен об активации сигнала тревоги у постели ПАЦИЕНТА. Для уменьшения Р1 может быть добавлена резервная линия связи, что позволит совершить аварийное переключение. В этом случае прерывание соединения не вызовет ОПАСНОЙ СИТУАЦИИ. Для уменьшения Р2 аварийный сигнал о «прерывании соединения» может отображаться в централизованном месте, уведомляя лечащего врача о ситуации. В данном случае ОПАСНАЯ СИТУАЦИЯ появляется, но вероятность возникновения НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ ниже.

5.7 Степень РИСКА

Общепринятым является мнение, что незначительные уровни РИСКА всегда возможны, так как практически нулевой РИСК недостижим. Также общепринятым мнением считается существование верхнего предела, выше которого РИСК недопустим, исключая чрезвычайные обстоятельства, и поэтому либо РИСК должен быть снижен любой ценой, либо действия, вызывающие РИСК, не могут осуществляться или же должны быть прекращены.

РИСКИ ниже верхнего предела принято считать допустимыми, но в то же время они могут содержать ОСТАТОЧНЫЕ РИСКИ, которые можно и необходимо снижать просто потому, что подобные РИСКИ достаточно несложно существенно снизить. Также возможно поддержание настолько малого уровня ОСТАТОЧНОГО РИСКА для заданной ОПАСНОЙ СИТУАЦИИ, что уменьшение этого РИСКА не является ни эффективным, ни необходимым. Таким образом, значения РИСКА можно разделить на области, обусловленные:

- верхним пределом, выше которого РИСКИ считаются недопустимыми;
- нижним пределом, ниже которого РИСКИ считаются «широко допустимыми» и, таким образом, не требующими никаких действий по снижению РИСКА;
- диапазон между верхним и нижним пределами, в котором допустимость РИСКА или необходимость его снижения требует дополнительного рассмотрения. Это рассмотрение должно основываться на заранее определенной политике, включающей в себя и снижение РИСКА, если это практически обосновано, и выполняться специальной командой специалистов (ИТ, врачей) или наблюдательными советами, учитывая обоснования, или утверждаться руководством.

Обратите внимание, что «практически обосновано» является более узким термином, чем «физически возможно». Данный термин включает в себя анализ времени, усилий и затрат, входящих в реализацию возможности УПРАВЛЕНИЯ РИСКОМ, которые должны быть пропорциональны снижению

РИСКА, которое они обеспечивают. Возможно существование РИСКА, который был снижен настолько, насколько это являлось практически обоснованным, но в то же время все еще его уровень является высоким. В свою очередь, организации могут выполнить дальнейшее снижение РИСКА, если меры по УПРАВЛЕНИЮ РИСКОМ легко применимы. Для среднего диапазона политика МЕНЕДЖМЕНТА РИСКА может либо требовать, либо настоятельно рекомендовать снижение РИСКА, если таковое практически обосновано. Рекомендуется в отчет об ОСТАТОЧНОМ РИСКЕ включать анализ его реализуемости.

5.8 Проверка формулировок

Таблица 2 демонстрирует методы проверки точной и надлежащей формулировки причин, ОПАСНЫХ СИТУАЦИЙ и НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ.

Таблица 2 — Методы проверки точной и надлежащей формулировки причин, ОПАСНЫХ СИТУАЦИЙ и НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

	Должно быть явно определено для:	Слишком общие примеры (сложно определить степень РИСКА)	Более точные примеры (легче определить степень РИСКА)
Причина	Установления P1	«Потеря соединения» является очень общим примером	«Потеря питания», «Убирающие выдергивают вилку из розетки» даже более легко оценивается
ОПАСНАЯ СИТУАЦИЯ вместе с определенным контекстом	Установления возможных негативных НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и возможных значений P2	Картинка на дисплее отрывистая и неполная	Картинка на дисплее отрывистая и неполная. Задержка в предоставлении ухода, так как удаленный врач не способен оценить ЭКГ ПАЦИЕНТА
НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ	Установления тяжести РИСКА (S)	Задержка терапии	Задержка терапии на время до 15 минут приводит к травмам ПАЦИЕНТА, таким как незначительные повреждения органов

6 Шаги

6.1 Обзор шагов

ШАГ 1. Идентифицировать ОПАСНОСТИ.

ШАГ 2. Идентифицировать причины и возникающие ОПАСНЫЕ СИТУАЦИИ.

ШАГ 3. Определить НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ и оценить их возможную тяжесть.

ШАГ 4. Оценить вероятности НЕПРЕДНАМЕРЕННОГО ПОСЛЕДСТВИЯ.

Оценивая вероятность и тяжесть НЕПРЕДНАМЕРЕННОГО ПОСЛЕДСТВИЯ, Вы оцениваете РИСК.

Повторить ШАГИ 1—4, выполняя их как снизу вверх, так и сверху вниз.

Одна ОПАСНОСТЬ может приводить к множеству ОПАСНЫХ СИТУАЦИЙ, одна ОПАСНАЯ СИТУАЦИЯ может возникать по множеству причин, одна причина может приводить к множеству ОПАСНЫХ СИТУАЦИЙ.

ШАГ 5. Оценить РИСК с учетом заданных критериев допустимости РИСКА.

ШАГ 6. Идентифицировать и документально оформить предложенные меры по УПРАВЛЕНИЮ РИСКОМ, а также повторить оценку РИСКА (т. е. вернуться к ШАГУ 3).

ШАГ 7. Реализовать меры по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 8. Верифицировать меры по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 9. Провести оценку любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ.

ШАГ 10. Провести оценку и составить отчет о совокупном ОСТАТОЧНОМ РИСКЕ.

6.2 Базовый пример использования 10 шагов

6.2.1 Общие положения

Ниже описан базовый пример выполнения 10 шагов, иллюстрирующий ПРОЦЕСС и проясняющий определение терминов. Данный пример не является примером МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ

ИТ-СЕТИ, а является примером, на который может ориентироваться ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ, владеющая МЕДИЦИНСКОЙ ИТ-СЕТЬЮ. В настоящем стандарте представлено множество других примеров, которые связаны именно с ИТ-СЕТЯМИ.

В начале АНАЛИЗА РИСКА необходимо определить анализируемую систему. В рассматриваемом примере система — это обученный хирург в обуви с закрытыми носками, находящийся в операционной и использующий скальпель Модели X. См. рисунок 2.

6.2.2 Начальный РИСК. Шаги 1—5 (рисунок 2)

ШАГ 1. Идентифицировать ОПАСНОСТЬ: *Острые края скальпеля.*

ШАГ 2. Идентифицировать причины и возникающие ОПАСНЫЕ СИТУАЦИИ. Причина — *Скользкая ручка.*

Последовательность событий — *Врач роняет скальпель, скальпель беспрепятственно падает на ногу врача.*

ОПАСНАЯ СИТУАЦИЯ — *Врач подвержен угрозе от неконтролируемого острого края.*

ШАГ 3. Документально оформить НП (НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ) и дать предварительную оценку возможной тяжести НП. *НП — это резаная рана, степень тяжести низкая.*

ШАГ 4. Дать предварительную оценку вероятности НП. *Периодически вероятно.*

Примечание — Это общая вероятность (P1 и P2) всей цепи, включая нанесение резаной раны.

ШАГ 5. Провести оценку РИСКА с учетом заданных критериев допустимости РИСКА. *Умеренный* (используйте таблицу D.3). Оценка включает в себя ответ на вопрос: «Достаточно ли мал РИСК для запуска в эксплуатацию?»

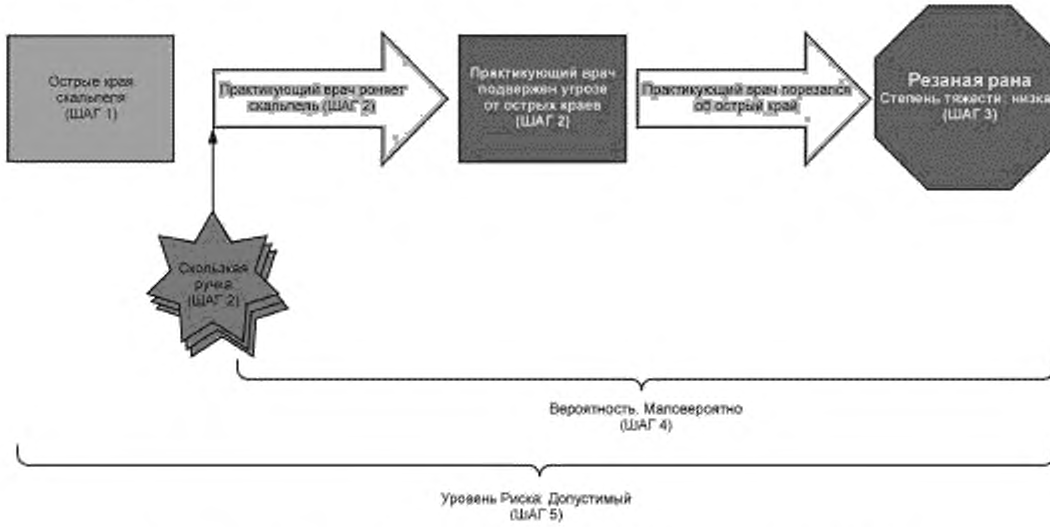


Рисунок 2 – Шаги 1—5. Идентификация ОПАСНОСТИ с помощью ОЦЕНКИ РИСКА

6.2.3 УПРАВЛЕНИЕ РИСКОМ и результирующий РИСК. Шаги 6—10 (рисунок 3)

ШАГ 6. Идентифицировать и документально оформить предложенные меры по УПРАВЛЕНИЮ РИСКОМ, а также провести оценку индивидуального ОСТАТОЧНОГО РИСКА. *Меры* по УПРАВЛЕНИЮ РИСКОМ — *Использовать скальпель Модели Y, оснащенный ручкой с защитой от скольжения. (Это уменьшает P1 и таким образом уменьшает общую вероятность.)*

Вернуться к ШАГУ 3.

Новая вероятность — Маловероятно.

Тяжесть осталась прежней, потому как НП не изменились.

Новый ОСТАТОЧНЫЙ РИСК теперь допустим.

ШАГ 7. Реализовать меры по УПРАВЛЕНИЮ РИСКОМ. *Пробный запуск.*

ШАГ 8. Верифицировать меры по УПРАВЛЕНИЮ РИСКОМ.

A) Верифицировать реализацию — *с помощью инспекции товарно-материальных запасов;*

B) Верифицировать эффективность — *пробное тестирование, научное исследование, проверка ПРОИЗВОДИТЕЛЯ и т. д.*

ШАГ 9. Провести оценку любых новых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ. *Например, скальпель Модели Y приводит к потере артикуляции хирурга. А это приведет к повторному запуску всего 10-шагового ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА.*

ШАГ 10. Провести оценку и составить отчет о совокупном ОСТАТОЧНОМ РИСКЕ. *Данный РИСК, как он описан выше, будет добавлен ко всем другим ОСТАТОЧНЫМ РИСКАМ. И тогда может быть задействована политика оценки совокупного ОСТАТОЧНОГО РИСКА.*

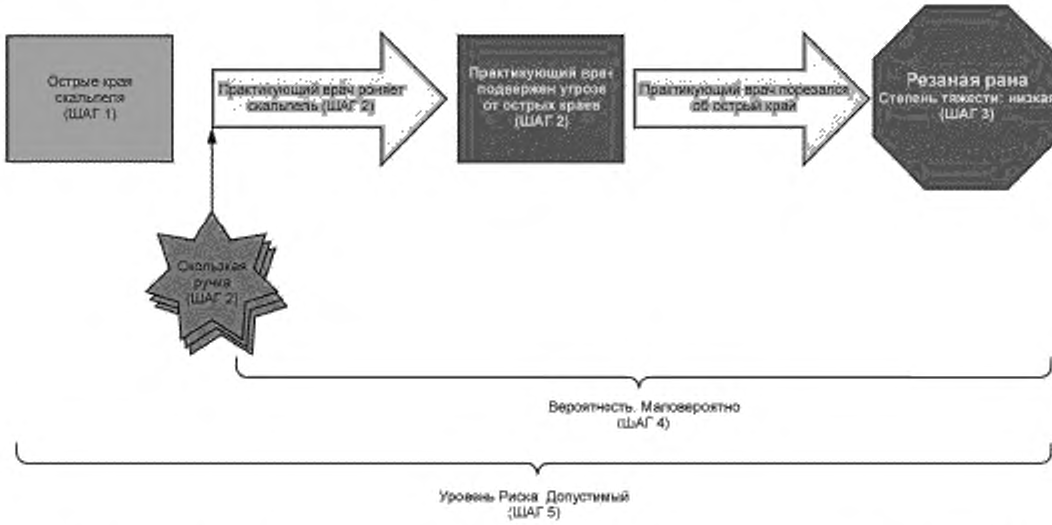


Рисунок 3 — Шаги 6—10. Меры по УПРАВЛЕНИЮ РИСКОМ с помощью совокупного ОСТАТОЧНОГО РИСКА

На рисунке 4 показано, как рассмотренный пример может быть представлен в формате сводного реестра ОЦЕНКИ РИСКА, использующегося в настоящем стандарте.

№ пп	ОПАСНОСТЬ	ОПАСНАЯ СИТУАЦИЯ	Причины, сопутствующие факторы	НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ	Начальный РИСК			Меры ослабления РИСКА/ УПРАВЛЕНИЯ РИСКОМ, предусмотренные проектом, защитные меры, или клинический ПРОЦЕСС, или информация для БЕЗОПАСНОСТИ	Ссылка на спецификации, политику или отчеты об испытаниях ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, а также на другие пункты настоящего стандарта (на все, которые используются для отслеживания)	ОСТАТОЧНЫЙ РИСК		
					Степень тяжести	Вероятность	РИСК (уровень)			Степень тяжести	Вероятность	РИСК (уровень)
1	HAZ01. Острые края	HS01. Врач подвержен угрозе от неконтролируемого острого края	C01. Скользкая рукоятка скальпеля модели X. Врач роняет скальпель, скальпель беспрепятственно падает на ногу врача	Порез ноги	Низкая	Периодически	Умеренный	RC01. Использовать скальпель модели Y, оснащенный рукояткой с защитой от скольжения	Ссылка. Управление материалами и протокол собрания Комитета управления процедурами ОО	Низкая	Маловероятно	Низкий

Рисунок 4 — Образец формата сводного реестра ОЦЕНКИ РИСКА

7 МЭК 80001-1:2010, подраздел 4.4. Последовательность шагов

7.1 Общие положения

МЕНЕДЖМЕНТ РИСКА, основанный на 10 шагах, описанный в данном разделе, является итеративным ПРОЦЕССОМ, который нельзя завершить за одну итерацию. По ряду соображений может быть необходимо и уместно вернуться к началу цикла и повторить любое действие в связи с результатами оценивания. Необходимо понимать, что повторение шагов поощряется на протяжении всех стадий ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА и является нормой.

Эти 10 шагов считаются универсально применимыми ко всем изменениям, большим и малым. Команда, выполняющая эти шаги, может применять их пропорционально размеру и эффекту изменения. Внесение изменения в существующую МЕДИЦИНСКУЮ ИТ-СЕТЬ, например, может потребовать лишь небольшое обновление уже доступной информации по МЕНЕДЖМЕНТУ РИСКА.

7.2 Применение требований, представленных в 4.4.1. Документальное оформление всех элементов МЕНЕДЖМЕНТА РИСКА

Для каждой МЕДИЦИНСКОЙ ИТ-СЕТИ создать и вести таблицу или базу данных, в которой указываются каждая ОПАСНАЯ СИТУАЦИЯ, которая может возникнуть во время работы сети, а также связанные с ней причины/вероятности и НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ/уровень тяжести. Для целей настоящего стандарта данная таблица будет именоваться как реестр ОЦЕНКИ РИСКА. В конечном реестре будут представлены сводные данные по индивидуальным и совокупным РИСКАМ, связанным с конкретной МЕДИЦИНСКОЙ ИТ-СЕТЬЮ. Данный реестр будет разработан, основываясь на шагах, описанных ниже, и станет развивающимся документом, изменяющимся вместе с изменениями в сети или в результате КОНТРОЛЯ, осуществляющегося после запуска в эксплуатацию.

Для крупных сетей реестр может быть довольно большим. Также необходимо учесть, что одна причина может повлечь множество ОПАСНЫХ СИТУАЦИЙ или множество причин могут повлечь одну ОПАСНУЮ СИТУАЦИЮ. Поэтому следует следить за форматированием реестра ОЦЕНКИ РИСКА. На базу данных может возлагаться управление связью между ОПАСНЫМИ СИТУАЦИЯМИ и причинами.

7.3 Примечание к ОЦЕНКЕ РИСКА

В 4.4.2 МЭК 80001-1:2010 представлено следующее требование. «Для каждой идентифицированной ОПАСНОСТИ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна оценить связанные с ней РИСКИ». И хотя данный шаг представлен всего лишь одним предложением в МЭК 80001-1:2010, он представляет собой многошаговый ПРОЦЕСС, требующий составление плана МЕНЕДЖМЕНТА РИСКА для МЕДИЦИНСКОЙ ИТ-СЕТИ и установление процедуры АНАЛИЗА РИСКА перед тем, как он может быть выполнен. Шаги 2—4, описанные ниже, применимы к этому действию.

В плане МЕНЕДЖМЕНТА РИСКА должны быть определены мера и критерии допустимости РИСКА (см. 4.3.5 МЭК 80001-1:2010), а также в него должны быть включены меры вероятности и тяжести риска. В приложении D представлена информации о мерах, использующихся в примерах данного раздела.

7.4 10-шаговый ПРОЦЕСС

7.4.1 ШАГ 1. Идентификация ОПАСНОСТЕЙ и ОПАСНЫХ СИТУАЦИЙ

Первым шагом МЕНЕДЖМЕНТА РИСКА является идентификация ОПАСНОСТЕЙ. При анализе сверху вниз следует начинать с ОПАСНОСТИ, а затем выявить пути, которые могут вызвать ОПАСНУЮ СИТУАЦИЮ (то есть определить ее причины). При восходящем анализе следует выявить все пути, которые могут привести к какому-либо отказу (то есть причины), затем определить, могут ли эти виды отказов повлечь за собой ОПАСНУЮ СИТУАЦИЮ. В обоих случаях в первую очередь идентифицируются ОПАСНОСТИ, именно поэтому это и является содержанием первого шага МЕНЕДЖМЕНТА РИСКА согласно МЭК 80001-1.

Рекомендуется применять оба метода (нисходящий и восходящий), чтобы получить полный список ОПАСНОСТЕЙ и ОПАСНЫХ СИТУАЦИЙ, связанных с МЕДИЦИНСКОЙ ИТ-СЕТЬЮ.

Анализ методом дерева отказов (FTA) является типичным нисходящим методом, а анализ типов и последствий отказов (FMEA) является типичным восходящим методом.

Потеря работоспособности и более конкретные ее вариации являются ОПАСНОСТЯМИ, которые следует учитывать. Для идентификации ОПАСНОСТЕЙ, связанных с анализируемой МЕДИЦИНСКОЙ ИТ-СЕТЬЮ, необходимо использовать список в приложении А и вопросы, представленные в приложении В.

7.4.2 ШАГ 2. Идентификация причин и вытекающих ОПАСНЫХ СИТУАЦИЙ

7.4.2.1 Общие положения

Для каждой идентифицированной ОПАСНОСТИ следует учесть причины и последовательности событий, которые могут привести к ОПАСНОСТИ или ОПАСНОЙ СИТУАЦИИ. Список распространенных возможных причин, представленный в приложении А, может облегчить процесс анализа. Примеры, приведенные в настоящем стандарте, могут посодействовать в идентификации полного списка причин и ОПАСНОСТЕЙ.

Если список возможных причин сформирован и установлены связи между причинами и ОПАСНЫМИ СИТУАЦИЯМИ, то можно идентифицировать дополнительные ОПАСНЫЕ СИТУАЦИИ и причины. Например, после идентификации причины ОПАСНОЙ СИТУАЦИИ следует повторно рассмотреть эту причину, чтобы определить, какие еще ОПАСНЫЕ СИТУАЦИИ может повлечь за собой данная причина, и таким образом установить связь между причинами (которые повлекли за собой хотя бы одну известную ОПАСНУЮ СИТУАЦИЮ) и другими ОПАСНЫМИ СИТУАЦИЯМИ. Следует продолжать этот процесс до тех пор, пока список ОПАСНЫХ СИТУАЦИЙ и связанных с ними причин не станет достаточно полным. И хотя важно идентифицировать все значимые ОПАСНЫЕ СИТУАЦИИ и связанные с ними причины, однако данный процесс является достаточно сложным и может оказаться непреодолимым, в особенности на первых этапах реализации МЕНЕДЖМЕНТА РИСКОВ. В целях уменьшения сложности следует рассмотреть вариант анализа, начинающийся с небольшого количества известных ОПАСНЫХ СИТУАЦИЙ. Затем число опасностей можно постепенно увеличивать, тем самым обходя чрезмерное требование идентифицировать все возможные ОПАСНЫЕ СИТУАЦИИ и связанные с ними причины.

Причины ОПАСНОСТЕЙ и ОПАСНЫХ СИТУАЦИЙ могут также носить и нетехнический характер. Ошибки пользователя и организационные нестыковки тоже должны учитываться. Для того чтобы охватить и эти области возможных причин, рекомендуется привлекать опытных пользователей для выполнения ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА.

Следует рассмотреть ОПАСНЫЕ СИТУАЦИИ, связанные с каждым из ОСНОВНЫХ СВОЙСТВ, — физическую травму, потерю эффективности или нарушение защиты.

7.4.2.2 Различные причины одной ОПАСНОЙ СИТУАЦИИ

Несколько различных причин могут повлечь за собой одну ОПАСНУЮ СИТУАЦИЮ. Чрезвычайно важно рассматривать все причины по отдельности. И хотя эффект (НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ/серьезность) ОПАСНОЙ СИТУАЦИИ от разных причин может быть одинаковым, вероятность и совокупный РИСК данной ОПАСНОЙ СИТУАЦИИ могут отличаться.

Например, все перечисленные ниже причины могут повлечь за собой ОПАСНОСТЬ потери работоспособности, или, более конкретно, потерю возможности соединения:

- кабель в коммуникационном канале поврежден из-за работы в канале;
- кабель в коммуникационном канале поврежден при установке;
- кабель непреднамеренно или преднамеренно отсоединен от коммутационного узла;
- непреднамеренное или преднамеренное отключение в комнате ПАЦИЕНТА;
- перегруженный канал;
- ошибки при проектировании сети;
- отказ коммутатора;
- ошибка конфигурации сети;
- конфликт IP-АДРЕСОВ;
- ЭМП (ЭЛЕКТРОМАГНИТНЫЕ ПОМЕХИ);
- выпадение сигнала РЧ (радиочастоты);
- вирус;
- износ оборудования, кабелей и прочего.

7.4.2.3 Различные ОПАСНЫЕ СИТУАЦИИ по одной причине

Также следует обратить внимание на то, что одна причина может повлечь за собой множество ОПАСНЫХ СИТУАЦИЙ, и в зависимости от деталей и контекста каждой отличающейся ОПАСНОЙ СИТУАЦИИ могут образоваться разные уровни РИСКА. Важно рассмотреть и зафиксировать все ОПАСНЫЕ СИТУАЦИИ, чтобы учесть все уровни РИСКА. Например, потеря соединения с сетью в отделении интенсивной терапии, таком как отделение реанимации новорожденных, характеризуется РИСКОМ для ПАЦИЕНТОВ более высокого уровня, чем когда соединение с сетью было потеряно в отделении плановой терапии.

Например, все из перечисленных ниже ОПАСНЫХ СИТУАЦИЙ могут возникать по причине неисправности кабеля:

- отказ при попытке передачи данных, связанных с ПАЦИЕНТОМ, таких как результаты лабораторных анализов и дозировка лекарственных средств,

- отказ при попытке отображения требующихся прописанных медикаментов;

- утрата контроля;

- отсутствие возможности принять ПАЦИЕНТА в кабинете неотложной помощи.

7.4.3 ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести

Для каждой ОПАСНОЙ СИТУАЦИИ необходимо определить возможные НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ для ПАЦИЕНТА, практикующего врача, организации и т. п. Дать оценку возможной тяжести этих НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ. НЕПРЕДНАМЕРЕННЫМ ПОСЛЕДСТВИЕМ могут стать нанесение травмы ПАЦИЕНТУ или практикующему врачу, потеря способности организации эффективно предоставлять качественные медицинские услуги ПАЦИЕНТАМ, уязвимые ДАННЫЕ О ЗДОРОВЬЕ и сопутствующие последствия для репутации ПАЦИЕНТА или организации. Все эти последствия напрямую связаны с ОСНОВНЫМИ СВОЙСТВАМИ, описанными в МЭК 80001-1, — БЕЗОПАСНОСТЬЮ, ЭФФЕКТИВНОСТЬЮ и ЗАЩИЩЕННОСТЬЮ ДАННЫХ И СИСТЕМЫ (см. таблицу 1).

7.4.4 ШАГ 4. Оценка НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

7.4.4.1 Общие положения

Для каждой ОПАСНОЙ СИТУАЦИИ/комбинации причин необходимо установить вероятность возникновения определенного НЕПРЕДНАМЕРЕННОГО ПОСЛЕДСТВИЯ (комбинацию P1 и P2 на рисунке 1). Данная вероятность может быть разделена на два компонента. Вероятность того, что причина в действительности приводит к ОПАСНОЙ СИТУАЦИИ (P1 на рисунке 1), и вероятность того, что после формирования ОПАСНОЙ СИТУАЦИИ возникает НЕПРЕДНАМЕРЕННОЕ ПОСЛЕДСТВИЕ определенной тяжести (P2 на рисунке 1). Организация может выбрать формальный метод объединения P1 и P2.

Как было сказано в 5.2, некоторые ОПАСНОСТИ уже заложены (присущи) в системе, а некоторые возникают вследствие определенной причины. Для упрощения задачи следует рассмотреть вероятность последовательности событий, которая в конечном счете ведет к ОПАСНОЙ СИТУАЦИИ. Такая вероятность называется P1 и она включает в себя создание ОПАСНОСТИ, если таковая не возникла ранее. Что касается потери работоспособности, в особенности для сети, то значимыми последовательностями событий, как правило, являются те, которые приводят к конкретной ОПАСНОСТИ потери работоспособности, таким как потеря данных, неправильные данные или неправильные сроки доставки данных.

Также признано считать, что оценка вероятности сложна и не точна. Для того чтобы в будущих реализациях сделать оценку более точной, могут использоваться контроль и УПРАВЛЕНИЕ СОБЫТИЯМИ. В приложении E содержится более подробная информация о контроле.

7.4.4.2 Оценки вероятностей

Для выполнения оценки вероятности возникновения ОПАСНОЙ СИТУАЦИИ может быть полезным провести оценку вероятности каждой связанной с опасностью причины отдельно и концептуально объединить их в предполагаемую вероятность для ОПАСНОЙ СИТУАЦИИ. Следует обратить внимание на то, что совокупная вероятность причинения ВРЕДА включает в себя вероятность возникновения ОПАСНОЙ СИТУАЦИИ и условную вероятность появления определенного НЕПРЕДНАМЕРЕННОГО ПОСЛЕДСТВИЯ при наличии ОПАСНОЙ СИТУАЦИИ. Следует использовать всю доступную информацию (определенные ОПАСНЫЕ СИТУАЦИИ, все связанные с ними причины, контекст, установленные НП и т. д.) для оценки вероятности.

При изучении рисунка 5 следует помнить следующее:

- P1 может быть оценена для определенной причины, независимо от ОПАСНОЙ СИТУАЦИИ, которую она может за собой повлечь. Более того, причина может повлечь за собой более одной ОПАСНОЙ СИТУАЦИИ. Следует вести отдельный список причин и связанных с ними значений P1;

- оценка тяжести может быть осуществлена для любых НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ, независимо от ОПАСНОЙ СИТУАЦИИ, послужившей их причиной. Более того, определенные НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ могут возникать вследствие нескольких различных ОПАСНЫХ СИТУАЦИЙ. Следует вести отдельный список распространенных НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и уровней их тяжести;

- P2 зависит от определенной комбинации ОПАСНОЙ СИТУАЦИИ и НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ. В методе, описанном в настоящем стандарте, для каждой ОПАСНОЙ СИТУАЦИИ (ВРЕД-j на рисунке 5) рассматривается одно основное НП. В действительности же рассматриваемая ОПАСНАЯ СИТУАЦИЯ может приводить к различным НП разной тяжести и с разными значениями P2. Из всех возможных идентифицированных НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ выбирается основное НП,

которое при том же значении P1 имеет максимальный РИСК (см. ШАГ 5). В некоторых примерах если значение P2 снижено с помощью мер УПРАВЛЕНИЯ РИСКОМ до несущественного или невозможного, то в последующих итерациях анализа другое НП меньшей тяжести может стать основным. Альтернативой этому подходу будет рассмотрение каждого вида НП по отдельности и выполнение оценки РИСКА для каждого из них. Такой подход является более полным и подробным, но требует более сложной работы с отчетом по АНАЛИЗУ РИСКА;

- полная вероятность возникновения ОПАСНОЙ СИТУАЦИИ является функцией P1a и P1b, а также конкретного P2 для использованного НП.

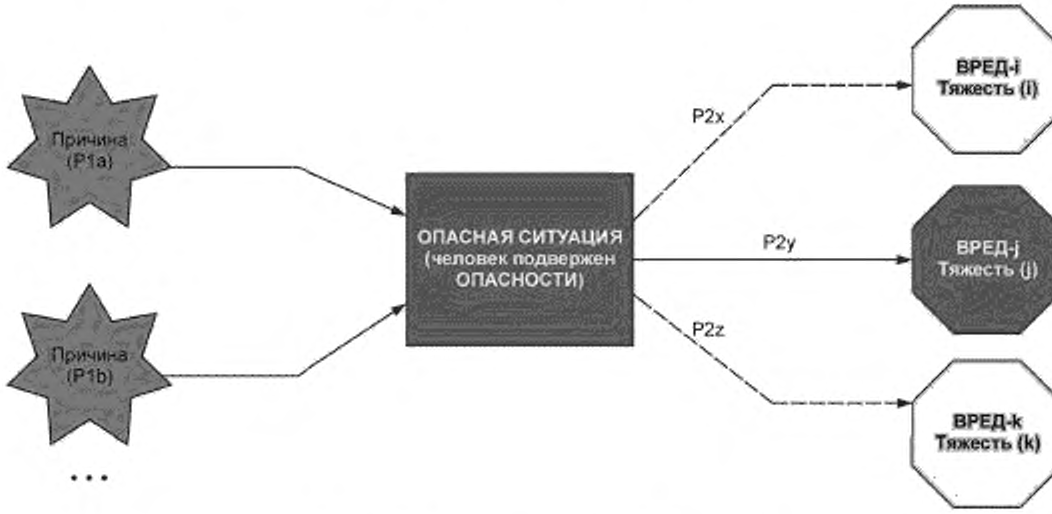


Рисунок 5 — Связь между причиной и ВРЕДОМ

7.4.5 ШАГ 5. ОЦЕНКА РИСКА

На данном этапе для каждой ОПАСНОЙ СИТУАЦИИ идентифицируется основное НП определенной тяжести и выполняется оценка общей вероятности возникновения каждого из этих основных НП.

РИСК является функцией тяжести и вероятности. Например, кратковременная боль будет допустима при более высокой вероятности ее возникновения, чем серьезная болезнь или смерть, для которых тяжесть настолько высока, что для достижения допустимого РИСКА вероятность их должна быть очень низкой. Уровни РИСКА должны быть заданы ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИЕЙ (ОО) заранее для всех возможных комбинаций вероятности и тяжести, а также должно быть выполнено их сравнение с учетом заданных критериев допустимости. Общепринятой практикой является использование матрицы приемлемости РИСКА, см. пример в приложении D. Для каждой ОПАСНОЙ СИТУАЦИИ необходимо применить критерии приемлемости РИСКА, определенные в плане МЕНЕДЖМЕНТА РИСКА, для того чтобы оценить, является ли РИСК приемлемым.

В настоящем стандарте матрица приемлемости РИСКА примера была разделена на три области — высокая, умеренная и низкая степени РИСКА. Высокая степень риска считается недопустимой. Низкая считается допустимой. Умеренный РИСК должен соответствовать политике, определенной в плане МЕНЕДЖМЕНТА РИСКА, который может включать в себя снижение РИСКА, если это практически обосновано, дальнейшие организационные отчеты и т. д. В приложении D рассмотрена матрица приемлемости РИСКА и блок-схема применения ШАГОВ 5 и 6. В настоящем стандарте принято считать, что политика ОО требует дальнейших исследований умеренного РИСКА с целью его снижения, если это возможно.

7.4.6 ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ и выполнение повторной оценки РИСКА (вернуться к ШАГУ 3)

7.4.6.1 Общие положения

Если оценка на ШАГЕ 5 дала высокую степень РИСКА, то необходимо идентифицировать возможности по УПРАВЛЕНИЮ РИСКОМ (выполнить данный шаг). Как правило, возможны несколько способов снижения РИСКА, поэтому необходимо выбрать лучшие меры по УПРАВЛЕНИЮ РИСКОМ.

Если оценка на ШАГЕ 5 дала умеренную степень РИСКА, то, основываясь на предположении, указанном выше, должны быть определены и реализованы дальнейшие возможности УПРАВЛЕНИЯ РИСКОМ (выполнен данный шаг), если это практически достижимо. Если дальнейшее уменьшение рассматриваемых РИСКОВ не представляется практически достижимым или если политикой ОО все же установлено, что в данном случае РИСК допустим, то можно опустить выполнение ШАГОВ 7—9.

Если оценка на ШАГЕ 5 дала низкую степень РИСКА, то в дальнейших возможностях по УПРАВЛЕНИЮ РИСКОМ нет нужды и ШАГИ 6—9 можно опустить.

7.4.6.2 Идентификация мер по УПРАВЛЕНИЮ РИСКОМ

Как было объяснено в 4.6 МЭК 80001-1:2010, меры по УПРАВЛЕНИЮ РИСКОМ способны уменьшить вероятность возникновения ОПАСНОЙ СИТУАЦИИ или же могут уменьшить вероятность возникновения НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ в случае, когда ОПАСНАЯ СИТУАЦИЯ уже возникла. Например, РИСК, возникающий в результате одиночного отказа, может быть снижен устранением этого одиночного отказа (например, за счет резервной линии связи) или уменьшением последствий этого отказа (например, уведомлением о прерванном соединении).

Как установлено в 4.4.4.1 МЭК 80001-1:2010, при оценке мер реализации по УПРАВЛЕНИЮ РИСКОМ следует рассмотреть следующие возможности в том порядке приоритетов, в котором они перечислены.

a) средства управления проектированием (например, надлежащее планирование пропускной способности сети). Предпочтительные меры по управлению РИСКОМ — устранение или снижение возможного РИСКА при проектировании сетевой системы или ее компонентов;

b) защитные меры (например, контроль использования пропускной способности сети и сигнализация о нарушении ограничений). Если РИСК не может быть устранен или уменьшен до допустимого уровня при проектировании, то можно прибегнуть к реализации защитных мер как к альтернативной возможности. Эта возможность менее желательна, так как она обычно требует ответа, что должно изменяться. Данная категория может также включать конкретные клинические или ИТ-ПРОЦЕССЫ;

c) информация для обеспечения КЛЮЧЕВЫХ СВОЙСТВ (например, предупреждения, документация пользователя, обучение). Предоставление информации по РИСКУ считается менее эффективным методом, чем возможности УПРАВЛЕНИЯ РИСКОМ, потому что это основано на установлении РИСКА и реакции на него.

Примеры мер по УПРАВЛЕНИЮ РИСКОМ включены в МЭК 80001-1, а также в раздел 8.

Выбранные меры по УПРАВЛЕНИЮ РИСКОМ необходимо зафиксировать в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ. Если ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ по результатам деятельности МЕНЕДЖМЕНТА РИСКА решает, что установленный тип стандартного изменения может быть осуществлен с допустимым РИСКОМ, подчиняющимся установленным ограничениям, то эта ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ может выпустить РАЗРЕШЕНИЕ НА ИЗМЕНЕНИЕ, которое позволяет осуществлять такие стандартные изменения и устанавливает ограничения на них. В приложении F приведено больше информации о РАЗРЕШЕНИЯХ НА ИЗМЕНЕНИЕ.

7.4.6.3 Выбор мер по УПРАВЛЕНИЮ РИСКОМ

После идентификации возможностей УПРАВЛЕНИЯ РИСКОМ необходимо выбрать средства по УПРАВЛЕНИЮ РИСКОМ, которые требуется реализовать для снижения ОСТАТОЧНОГО РИСКА до допустимых уровней.

В некоторых случаях необходимо провести оценку практической возможности УПРАВЛЕНИЯ РИСКОМ. УПРАВЛЕНИЕ РИСКОМ считается практически невыполнимым, если затрачиваемое время, усилия и расходы не пропорциональны пользе. Процедура оценки пропорциональности и практической возможности может включать в себя, но не ограничиваться:

- качественным анализом преимуществ и трудностей УПРАВЛЕНИЯ РИСКОМ;
- оценкой повышения управляемости МЕДИЦИНСКОЙ ИТ-СЕТИ;
- оцениванием повышения устойчивости МЕДИЦИНСКОЙ ИТ-СЕТИ.

7.4.6.4 Повторная оценка РИСКА

После того как были выбраны меры по УПРАВЛЕНИЮ РИСКОМ, вероятность и основные НП должны быть повторно оценены (возвращение к ШАГАМ 3 и 4), и ОСТАТОЧНЫЙ РИСК, связанный с индивидуальной ОПАСНОЙ СИТУАЦИЕЙ, после УПРАВЛЕНИЯ РИСКОМ должен быть повторно оценен (ШАГ 5).

ОСТАТОЧНЫЙ РИСК — это РИСК, который остается после реализации мер УПРАВЛЕНИЯ РИСКОМ. Это равносильно окончательному уровню РИСКА ОПАСНОЙ СИТУАЦИИ.

На данном этапе выбранная возможность УПРАВЛЕНИЯ РИСКОМ является просто идеей, и поэтому повторная оценка основывается на умозаключении о том, каким может быть ее влияние на РИСК,

к которому она применяется. Опасность заключается в том, что заключения об ожидаемом эффекте от выбранной возможности УПРАВЛЕНИЯ РИСКОМ могут оказаться слишком позитивными. Необходимо записать предположения, сделанные при повторной оценке РИСКА, так как они могут оказаться необходимыми для реализации возможности УПРАВЛЕНИЯ РИСКОМ и/или для КОНТРОЛЯ эффективности этой возможности в условиях эксплуатации. Следует внести все эти предположения в ФАЙЛ МЕНЕДЖМЕНТА РИСКА. Корректность этой начальной повторной оценки будет продемонстрирована на ШАГЕ 9.

7.4.6.5 Анализ соотношения РИСК/польза

Признано, что одним из возможных результатов анализа возможности по УПРАВЛЕНИЮ РИСКОМ может быть отсутствие практических методов снижения РИСКА до допустимых уровней. Как правило, если по результатам оценки ОПАСНАЯ СИТУАЦИЯ признана недопустимой и меры по УПРАВЛЕНИЮ РИСКОМ недостаточны для снижения РИСКА до допустимых уровней, то предлагаемый проект или его изменение должны быть прекращены, а принятое об этом решение зафиксировано в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА. Тем не менее в некоторых случаях большие РИСКИ являются оправданными, если ожидаемая польза от внесенного изменения их не превосходит. В таком случае ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна провести и документально оформить анализ соотношения РИСК/польза, чтобы определить, превосходит ли польза от реализации данного проекта возможные РИСКИ. После того как все возможности по УПРАВЛЕНИЮ РИСКОМ были идентифицированы и выбраны, необходимо перейти к ШАГУ 7.

7.4.7 ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ

Для снижения РИСКА идентифицированные меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы. Реализация не может быть частью работающей системы, если ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА не был успешно завершен. Для оценки эффективности мер по УПРАВЛЕНИЮ РИСКОМ при тестовых испытаниях должны проводиться теоретические анализы или практические исследования.

Если была выбрана и реализована в работающей сети конкретная мера по УПРАВЛЕНИЮ РИСКОМ, то за этим должен следовать ПРОЦЕСС УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ, который необходимо зафиксировать в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ. См. 4.5 МЭК 80001-1:2010.

7.4.8 ШАГ 8. Верификация мер по УПРАВЛЕНИЮ РИСКОМ

7.4.8.1 Общие положения

ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ включает в себя как верификацию реализации мер, так и верификацию их эффективности. Порядок, в котором осуществляются эти верификации, зависит от типа мер по УПРАВЛЕНИЮ РИСКОМ и от того, возможна ли верификация эффективности при тестировании.

7.4.8.2 ВЕРИФИКАЦИЯ эффективности

Эффективность мер по УПРАВЛЕНИЮ РИСКОМ должна быть верифицирована и документально оформлена в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ. Необходимо верифицировать соответствие мер управления ожидаемому эффекту. Например, мера по УПРАВЛЕНИЮ РИСКОМ при отказе канала сети может заключаться в применении резервного канала. ВЕРИФИКАЦИЯ ее эффективности будет включать симуляцию отказа основного канала и верификацию эффективности резервного канала, используемого в качестве меры по УПРАВЛЕНИЮ РИСКОМ. ВЕРИФИКАЦИЯ может происходить при выполнении тестов в условиях испытаний до фактической реализации в работающей системе. Для ВЕРИФИКАЦИИ, которая должна осуществляться в действующей системе, возникнет необходимость во временном окне изменений (см. пояснение ниже). Верификацию необходимо завершить до конца этого окна (до запуска в эксплуатацию).

В некоторых случаях эффективность не может быть ВЕРИФИЦИРОВАНА объективно, и часто достаточно логического обоснования, используя профессиональную подготовку, клинические процедуры и т. п. В таких случаях КОНТРОЛЬ эффективности мер по УПРАВЛЕНИЮ РИСКОМ предоставляет более точный взгляд на эффективность мер по УПРАВЛЕНИЮ РИСКОМ.

ВЕРИФИКАЦИЯ эффективности мер по УПРАВЛЕНИЮ РИСКОМ на данном шаге осуществляется за счет информации и надлежащих методов, доступных на момент выполнения данного шага. После запуска в эксплуатацию и на протяжении всего периода использования МЕДИЦИНСКОЙ ИТ-СЕТИ КОНТРОЛЬ продолжает осуществляться для обеспечения постоянной эффективности мер по УПРАВЛЕНИЮ РИСКОМ. Новые технологические разработки, изменения в фактическом использовании МЕДИЦИНСКОЙ ИТ-СЕТИ, организация пользователя или оценка событий могут продемонстрировать непредвиденные слабости мер по УПРАВЛЕНИЮ РИСКОМ, требующие усовершенствований.

В приложении Е представлены примеры методов оценки эффективности мер по УПРАВЛЕНИЮ РИСКОМ, осуществляемых как часть КОНТРОЛЯ.

Эффективность мер по УПРАВЛЕНИЮ РИСКОМ может быть установлена только при четком понимании того, какой эффект должен достигаться за счет этих мер. Стабильность эффективности на стадии эксплуатации можно контролировать только в том случае, если этот требуемый эффект четко определен и записан вместе с реализованной мерой по УПРАВЛЕНИЮ РИСКОМ.

ВЕРИФИКАЦИЯ реализации

Реализация всех мер по УПРАВЛЕНИЮ РИСКОМ должна быть ВЕРИФИЦИРОВАНА и документально оформлена в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ. ВЕРИФИКАЦИЯ подтверждает, что меры по УПРАВЛЕНИЮ РИСКОМ были реализованы в МЕДИЦИНСКОЙ ИТ-СЕТИ и осуществляется до запуска сети в эксплуатацию. Запуск в эксплуатацию подразумевает использование МЕДИЦИНСКОЙ ИТ-СЕТИ, как правило, для ПАЦИЕНТОВ. Это может означать одно из:

- для новых сетей ВЕРИФИКАЦИЯ завершается до запуска в эксплуатацию или
- в случаях, когда сеть уже используется, определяется «временное окно для изменения», в пределах которого предполагается, что сеть находится в состоянии изменения. Действуют планы возврата, а также, вероятно, временные клинические процедуры (например, контроль у постели больного вместо центрального контроля). ВЕРИФИКАЦИЯ реализации должна осуществляться до конца временного окна для изменения. В приложении G рассмотрены примеры элементов, которые могут быть частью временного окна для изменения.

ВЕРИФИКАЦИИ реализации должен способствовать ПРОЦЕСС УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ.

7.4.9 ШАГ 9. Выполнение оценки новых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ

Существует вероятность появления новых РИСКОВ в результате реализации мер по УПРАВЛЕНИЮ РИСКАМИ.

Примером может служить добавление слишком большого количества средств защиты, приводящее к тому, что практикующий врач не может получить информацию для ПАЦИЕНТА, когда это ему необходимо. В таком случае может потребоваться модифицировать или изменить меры по УПРАВЛЕНИЮ РИСКОМ так, чтобы они скорее служили целям клиники, чем являлись ИТ-решением.

Оценка новых РИСКОВ должна документально оформляться в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ. Любой новый риск должен подвергаться оценке в соответствии с ШАГАМИ 2—9. Это итеративный ПРОЦЕСС, который может состоять из нескольких циклов итерации.

7.4.10 ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

В дополнение к любым ОСТАТОЧНЫМ РИСКАМ, связанным с индивидуальными ОПАСНЫМИ СИТУАЦИЯМИ, ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ требуется определить совокупный ОСТАТОЧНЫЙ РИСК, связанный с МЕДИЦИНСКОЙ ИТ-СЕТЬЮ. Определение ОСТАТОЧНОГО РИСКА включает оценку всех отдельных ОСТАТОЧНЫХ РИСКОВ и определение того, превышает ли всеобщий РИСК сумму РИСКОВ других частей. Например, хотя каждая из двух отдельных ОПАСНЫХ СИТУАЦИЙ может иметь допустимый ОСТАТОЧНЫЙ РИСК, если есть вероятность, что обе ОПАСНЫЕ СИТУАЦИИ возникнут одновременно, то совокупный ОСТАТОЧНЫЙ РИСК может оказаться недопустимым.

ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна определить и документально оформить сводку по ОСТАТОЧНОМУ РИСКУ, содержащую список всех отдельных ОСТАТОЧНЫХ РИСКОВ и совокупный ОСТАТОЧНЫЙ РИСК, остающийся после реализации мер по УПРАВЛЕНИЮ РИСКОМ. Эта сводная информация является реестром ОЦЕНКИ РИСКА.

Как описано в 7.4.6, один тип мер по УПРАВЛЕНИЮ РИСКОМ предназначен для предоставления информации для пользователей системы. Данная информация часто содержит в себе данные об обучении, маркировке или уведомлениях об определенных применениях, способных привести к ОПАСНОЙ СИТУАЦИИ. При оценке совокупного ОСТАТОЧНОГО РИСКА следует учитывать наличие любой другой дополнительной информации, касающейся РИСКА в системе, которую следует донести до пользователей МЕДИЦИНСКОЙ ИТ-СЕТИ, а также нет ли необходимости установить каналы связи для передачи подобной информации.

Не существует никакого предпочтительного метода для оценки допустимости совокупного ОСТАТОЧНОГО РИСКА. ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна установить метод и критерии, которые необходимо соблюдать, в политике МЕНЕДЖМЕНТА РИСКА. Могут быть качественные или количественные подходы. Примером более качественного подхода оценки совокупного ОСТАТОЧНОГО РИСКА может быть определение допустимого максимального числа ОПАСНЫХ СИТУАЦИЙ, которое

сохраняется на среднем уровне РИСКА после реализации мер по УПРАВЛЕНИЮ РИСКОМ. Более количественным подходом может быть прогнозирование суммарной частоты НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ или числа травм, связанных со всеми ОПАСНЫМИ СИТУАЦИЯМИ, возникающими после реализации УПРАВЛЕНИЯ РИСКОМ, и сравнение этого совокупного ОСТАТОЧНОГО РИСКА с предварительно установленным допустимым уровнем.

Если уменьшение совокупного ОСТАТОЧНОГО РИСКА до допустимого уровня не представляется практически достижимым, то необходимо провести и документально оформить анализ соответствия РИСКА/пользы для сравнения совокупного ОСТАТОЧНОГО РИСКА с той пользой, которая может быть получена от внесения запланированного изменения в МЕДИЦИНСКУЮ ИТ-СЕТЬ.

И индивидуальные ОСТАТОЧНЫЕ РИСКИ, и совокупный ОСТАТОЧНЫЙ РИСК необходимо документально оформить в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА МЕДИЦИНСКОЙ ИТ-СЕТИ.

7.5 Рассмотренные шаги и их связь с МЭК 80001-1 и ИСО 14971

Таблица 3 демонстрирует связь между настоящим стандартом, МЭК 80001-1:2010 и ИСО 14971:2007. Разделы и подразделы, не вошедшие в настоящий стандарт, не представлены.

Таблица 3 — Связь между настоящим стандартом, МЭК 80001-1:2010 и ИСО 14971:2007

Раздел/подраздел ИСО 14971		Подраздел МЭК/ТО 80001-1		Шаги
4	АНАЛИЗ РИСКА			
4.1	ПРОЦЕСС АНАЛИЗА РИСКА	—		
4.2	ПРЕДНАЗНАЧЕННОЕ ИСПОЛЬЗОВАНИЕ и идентификация характеристик, связанных с БЕЗОПАСНОСТЬЮ		(Медицинская ИТ-СЕТЬ, определенная и документально оформленная в соответствии с 4.3)	
4.3	Идентификация ОПАСНОСТЕИ	4.4.2		ШАГ 1. Идентификация ОПАСНОСТЕЙ
4.4	Оценка РИСКА(ОВ) для каждой опасной ситуации «Необходимо рассматривать разумно предсказуемые последовательности или комбинации событий, приводящие к возникновению ОПАСНЫХ СИТУАЦИЙ, которые необходимо регистрировать». «Для каждой выявленной ОПАСНОЙ СИТУАЦИИ должна быть получена оценка РИСКА(ОВ)»		«Для каждой выявленной ОПАСНОСТИ ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна дать оценку соответствующих РИСКОВ...»	ШАГ 2. Идентификация причин и возникающих ОПАСНЫХ СИТУАЦИЙ. ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести*. ШАГ 4. Оценка вероятности* возникновения НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ. *Оценивая вероятность и тяжесть НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ, вы оцениваете РИСК. Повторить ШАГИ 1—4, выполняя их как по нисходящему, так и по восходящему принципу. Одна ОПАСНОСТЬ может приводить ко множеству ОПАСНЫХ СИТУАЦИЙ, одна ОПАСНАЯ СИТУАЦИЯ может возникать по множеству причин, одна причина может приводить к множеству ОПАСНЫХ СИТУАЦИЙ
5	ОЦЕНКА РИСКА	4.4.3	ОЦЕНКА РИСКА	ШАГ 5. Оценка РИСКА с учетом заданных критериев допустимости РИСКА
6	УПРАВЛЕНИЕ РИСКОМ	4.4.4	УПРАВЛЕНИЕ РИСКОМ	
6.1	Снижение риска	—		

Окончание таблицы 3

Раздел/подраздел ИСО 14971		Подраздел МЭК/ТО 80001-1		Шаги
6.2	Анализ возможностей УПРАВЛЕНИЯ РИСКОМ	4.4.4.1	Анализ возможностей УПРАВЛЕНИЯ РИСКОМ	ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ(АМИ) и повторная оценка РИСКА (т. е. вернуться к ШАГУ 3)
6.3	Реализация мер по УПРАВЛЕНИЮ РИСКОМ	4.4.4.3	Реализация мер по УПРАВЛЕНИЮ РИСКОМ	ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ
		4.4.4.4	ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ	ШАГ 8. ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ
6.4	Оценка ОСТАТОЧНОГО РИСКА		(Рассмотрено в 4.4.4.1)	
6.5	Анализ соотношения РИСК/польза		(Рассмотрено в 4.4.4.1 и 4.4.5)	(Рассмотрено в ШАГЕ 6 и ШАГЕ 10)
6.6	Риски, возникающие вследствие выполнения мер по УПРАВЛЕНИЮ РИСКОМ	4.4.4.5	Новые риски, возникающие в связи с УПРАВЛЕНИЕМ РИСКОМ	ШАГ 9. Оценка любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ
7	Оценка допустимости совокупного ОСТАТОЧНОГО РИСКА	4.4.5	Оценка ОСТАТОЧНОГО РИСКА и уведомление о риске	ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

8 Практические примеры

8.1 Общие положения

Примеры, приведенные ниже, демонстрируют, как протекает несколько действительно ОПАСНЫХ СИТУАЦИЙ, а также причины для каждого из трех сценариев. Данные примеры не являются исчерпывающими. Скорее, в них представлены определенные общие элементы АНАЛИЗА РИСКА и ПРОЦЕССА управления для одной или двух конкретных ОПАСНЫХ СИТУАЦИЙ и одной или двух связанных с ними причин. Для того чтобы РИСК был оценен, должны быть полностью определены элементы и область применения анализируемой системы.

Кроме того, должно быть известно фактическое использование сети и присоединенных к ней МЕДИЦИНСКИХ ПРИБОРОВ. Примеры, приведенные ниже, начинаются с разъяснения контекста и описания анализируемой сети. Затем для каждого примера выполняются все шаги ПРОЦЕССА, подробно рассмотренные выше. Каждой ОПАСНОСТИ, ОПАСНОЙ СИТУАЦИИ, причине и мере по УПРАВЛЕНИЮ РИСКОМ назначен уникальный идентификатор.

Примеры являются вымышленными, и не стоит воспринимать их как действительные для всех организаций. Примеры данного раздела описаны в рамках следующего формата:

- задается полное описание контекста (случай клинического применения);
- задается анализируемая сеть;
- применяются следующие уникальные идентификаторы:
- ОПАСНОСТИ обозначаются как HAZ01, HAZ02...;
- ОПАСНЫЕ СИТУАЦИИ обозначаются как HS01, HS02...;
- причины обозначаются как C01, C02...;
- меры по УПРАВЛЕНИЮ РИСКОМ обозначаются как RC01, RC02...

8.2 Пример 1. Беспроводной контроль ПАЦИЕНТА во время его транспортировки

8.2.1 Полное описание контекста

Для передачи поступающих в реальном времени данных о ПАЦИЕНТЕ, находящемся в режиме транспортировки, используется беспроводная сеть. Тяжесть состояния больных может широко варьироваться. ПАЦИЕНТА могут перевозить из отделения неотложной помощи, рентгенологического отделения и других диагностических секторов в общую больничную палату или в отделение интенсивной

терапии (ICU). Пациент подключен к активному беспроводному контролирующему прибору типа 802.11b/g. Во время перевозки данные о ПАЦИЕНТЕ в реальном времени передаются из контролирующего прибора на пост медсестры для осуществления наблюдения за ПАЦИЕНТАМИ и в систему электронной медицинской документации больницы для архивирования.

8.2.2 Описание анализируемой сети

Беспроводная локальная сеть 802.11 (WLAN) охватывает всю больницу и использует диапазон 802.11a/b/g (2.4 и 5 ГГц). В этой локальной сети используются восемь сетевых идентификаторов, включая SSID (идентификатор набора служб) гостевого доступа, и в некоторых участках зоны действия сети может находиться большое число беспроводных пользователей. Один из идентификаторов SSID предназначен для контроля ПАЦИЕНТОВ.

Отделение рентгенологии расположено рядом с главной кухней, на которой используются производственные микроволновые печи высокой мощности. В больнице также используются беспроводные телефоны типа DECT (телефон цифровой усовершенствованной беспроводной связи), работающие в диапазоне частот 2,4 ГГц. Для дальнейшего рассмотрения УПРАВЛЕНИЯ РИСКОМ беспроводных сетей см. МЭК 80001-02-3:2012.

8.2.3 10 шагов

ШАГ 1. Идентификация ОПАСНОСТИ

HAZ01. Полная потеря соединения.

HAZ02. Неустойчивая связь.

ШАГ 2. Идентификация причин и возникающих ОПАСНЫХ СИТУАЦИЙ

C01. Внешняя радиопомеха, вызванная микроволновой печью, влечет за собой моментальную потерю связи между устройством-клиентом и WAP (точкой беспроводного доступа).

C02. Внешняя радиопомеха, вызванная DECT-телефонами, влечет за собой временную потерю связи между устройством-клиентом и WAP.

C03. Слишком большое количество устройств-клиентов приводит к перегрузке WAP, которая влечет за собой временную потерю данных.

Идентифицированы следующие ОПАСНЫЕ СИТУАЦИИ:

HS01. Практикующий врач не осведомлен о нуждающемся в лечении ПАЦИЕНТЕ. Задержка начала лечения в связи с потерей данных (сигнал тревоги не дошел до практикующего врача вследствие причин C01,C02 или C03).

ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести

В таблице D.2 предоставлены масштабы тяжести. Следует отметить, что оценка тяжести основана на уровне остроты состояния ПАЦИЕНТА.

НП для HS01. В данном случае в связи с тем, что уровень остроты состояния ПАЦИЕНТОВ может широко варьироваться и во время транспортирования они не могут находиться под местным/непосредственным наблюдением практикующего врача, потеря данных, передающихся в реальном времени, может привести к серьезным последствиям для ПАЦИЕНТА, находящегося в тяжелом состоянии. (Следует отметить, что в зависимости от остроты состояния ПАЦИЕНТОВ могут быть подобраны средства смягчения последствий.) Тяжесть — *катастрофическая*.

ШАГ 4. Оценка вероятности НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

В данном примере выполняется оценка вероятности того, насколько любая из причин, перечисленных выше, влечет за собой определенное выше НП установленной тяжести.

В таблице D.1 приведена шкала вероятностных оценок.

HS01. *Маловероятно*.

ШАГ 5. Оценка РИСКА с учетом заданных критериев допустимости

С помощью таблицы D.3 и основываясь на вероятности и тяжести, определенных на ШАГАХ 3 и 4, начальный уровень РИСКА был определен как высокий.

HS01. (катастрофическая/маловероятно). Уровень РИСКА — *высокий*.

ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ и оценка индивидуального ОСТАТОЧНОГО РИСКА

В данном случае были определены меры по УПРАВЛЕНИЮ РИСКОМ, уменьшающие как P1, так и P2.

Для уменьшения P1 каждая причина была рассмотрена отдельно, и были определены меры по УПРАВЛЕНИЮ РИСКОМ.

Причина 1. Внешняя радиопомеха (микроволновая печь).

RC01. Провести замену старой микроволновой печи, тем самым эффективно уменьшая радиоизлучение, так как новые модели лучше экранированы.

Причина 3. Перегрузка пропускной способности WAP.

RC03. Спроектировать пропускную способность сети так, чтобы предоставить избыточное число WAP-устройств на участке, чтобы одно WAP-устройство обслуживало меньшее количество клиентов.

Для уменьшения Р2 определена следующая мера по УПРАВЛЕНИЮ РИСКОМ.

RC03. Практикующий врач обслуживает ПАЦИЕНТА во время транспортирования. Протокол практикующего врача может быть спроектирован таким образом, что присутствие врача во время транспортирования необходимо только для ПАЦИЕНТОВ с остротой состояния выше заданного уровня. Данная мера по УПРАВЛЕНИЮ РИСКОМ предназначена для снижения вероятности серьезных последствий при эффективном уменьшении возможной тяжести данной травмы.

Следует отметить, что никакие средства смягчения последствий специально не подбирались для низкой вероятности возникновения причины 3 и ее низкого уровня осуществимости (удаления всех DECT-телефонов).

HS01. (новая тяжесть/вероятность — *средняя/практически невероятно*). Уровень РИСКА — *низкий*.

ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ

Меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы для того, чтобы они могли быть ВЕРИФИЦИРОВАНЫ до запуска в эксплуатацию.

RC01. Замена микроволновой печи. Заменить микроволновую печь более новой с меньшим излучением. Включить в требования к закупкам микроволновых печей наличие подходящего экранирования для защиты от внешних радиопомех, чтобы в будущем обеспечить установку ЭМ-совместимых микроволновых печей.

RC02. Избыточный резерв точек WAP. Определить физические/географические участки (например, пункт медсестры и т. п.), на которых наблюдается большое скопление пользователей и плотный беспроводной трафик на единицу площади, и увеличить число точек WAP на данном участке.

RC03. Клиническая процедура. Создается и обновляется политика перевозки пациентов. По завершении деятельности МЕНЕДЖМЕНТА РИСКА в действующей системе будут учреждены меры по УПРАВЛЕНИЮ РИСКОМ. В них должны входить обучение врачей и пригодность персонала.

ШАГ 8. ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ

ВЕРИФИКАЦИЯ RC01

Реализация. Подтвердить включение требований электромагнитной совместимости в документы закупки. Подтвердить, что выбранная микроволновая печь реализует дополнительные требования посредством анализа независимых отчетов об испытании (предпочтительно) или выполненных измерений. Необходимо убедиться, что старые микроволновые печи были удалены.

Эффективность. Необходимо измерить радиоизлучение с помощью анализатора спектра около микроволновой печи. Следует также измерить, как влияют радиопомехи на сети WLAN (если это возможно), для определения уровней такого влияния. Эти измерения должны быть осуществлены до и после замены старой микроволновой печи. Необходимо документально оформить разницу в радиопомехах и провести испытание связи, поместив испытуемый образец вблизи микроволновых печей, чтобы верифицировать устранение нарушения связи.

ВЕРИФИКАЦИЯ RC02

Реализация. Подтвердить плотность скопления точек WAP и доступность к ним в соответствии с обновленной конструкцией перед запуском в эксплуатацию. Следует использовать набор конечных устройств, чтобы сымитировать пиковую нагрузку и подтвердить, что величина пропускной способности соответствует целевому проекту (в данном случае это 50 %).

Эффективность. Верифицировать, что при пиковой нагрузке увеличение числа точек WAP на физическом участке устраняет любые перегрузки WAP. Это необходимо осуществить, используя типы и количество устройств, которые будут использоваться на данном участке, измеряя пиковые нагрузки на точку/точки WAP. Такое измерение может быть осуществлено прибором для измерения эфирного времени, предоставленным третьей стороной, или приборами измерения пропускной способности, встроенными в действующую инфраструктуру. Необходимо верифицировать поддержание связи каждым прибором в соответствии с требующимися характеристиками сети, а также что ни на одной точке WAP пропускная способность не падает ниже 50 % (См. Технический отчет по беспроводным сетям для дальнейшего обсуждения планирования пропускной способности.)

ВЕРИФИКАЦИЯ RC03

Реализация. Верифицировать наличие протокола, а также прохождение персоналом надлежащего обучения и его готовность к запуску системы в эксплуатацию.

Эффективность. Верифицировать эффективность обучения посредством испытания и сертификации.

ШАГ 9. Оценка любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ

По заключениям оценки не было обнаружено никаких новых РИСКОВ, привнесенных добавленными мерами по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

Так как данные примеры представляют только один или два подпроцесса для ПРОЦЕССА заданной МЕДИЦИНСКОЙ ИТ-СЕТИ, концепцию совокупного ОСТАТОЧНОГО РИСКА сложно продемонстрировать. В целях настоящего стандарта следует принять, что совокупный ОСТАТОЧНЫЙ РИСК был определен как допустимый в соответствии с политикой ОО.

8.3 Пример 2. Удаленное отделение интенсивной терапии (ОИТ)/Дистанционное медицинское обслуживание

8.3.1 Полное описание контекста

В данном сценарии используется ГОРОДСКАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ (ГВС) для передачи данных о ПАЦИЕНТЕ в реальном времени из удаленного места, используемого местным практикующим врачом в целях контроля, диагностики и выбора плана лечения. ПАЦИЕНТЫ, за которыми осуществляется контроль, находятся в отделении для пациентов, перенесших кардиохирургию. Тяжесть состояния таких больных, как правило, не такая высокая, как больных в отделении интенсивной терапии. «Местный практикующий врач» в данном случае является врачом телеметрии (техником, медбратом, доктором и т. п.), который географически отделен от удаленного ПАЦИЕНТА. В данном случае место, где находится практикующий врач, соединено с местом, где находится ПАЦИЕНТ, посредством ГВС.

8.3.2 Описание анализируемой сети

Анализируемая сеть включает в себя многоуровневый коммутатор доступа 10/100 с подключенным к нему прибором контроля за ПАЦИЕНТОМ, находящимся в послеоперационном отделении, арендуемого ПРОИЗВОДИТЕЛЯ, с гарантированной полосой пропускания в 12 Гигабайт для всего трафика, поступающего с данного места (включая другие приложения помимо приложений удаленного контроля), и многоуровневый коммутатор доступа 10/100, расположенный на стороне врача. Основываясь на требованиях ПРОИЗВОДИТЕЛЯ к пропускной способности и задержке, предусматривается, что ПРОИЗВОДИТЕЛЬ будет обслуживать трафик, поступающий от приборов контроля, а также трафик, которым будут пользоваться другие приложения в канале. Поставщик ПРОИЗВОДИТЕЛЯ гарантировал минимальный уровень услуг, включающий в себя полосу пропускания, достаточную для всех из этих приложений (их текущее использование).

8.3.3 10 шагов

ШАГ 1. Идентификация ОПАСНОСТИ

Сеть, рассматриваемая в данном примере, предназначена для передачи данных о ПАЦИЕНТЕ от места ПАЦИЕНТА до места практикующего врача в реальном времени. Отказ при выполнении данной передачи будет представлять ОПАСНОСТЬ.

HAZ01. Неустойчивая связь.

HAZ02. Полная потеря связи.

ШАГ 2. Идентификация причин и возникающих ОПАСНЫХ СИТУАЦИЙ

В данном случае, что часто случается, для данной ОПАСНОСТИ в заданном контексте можно идентифицировать множество причин, и они могут приводить к одной или нескольким ОПАСНЫМ СИТУАЦИЯМ.

C01. Незапланированный трафик не в реальном времени, пытающийся занять канал, вызывает перегрузку ГВС.

C02. Выход ГВС из строя, неконтролируемый ОО (отказ средства доступа), вызывает выход из строя всей сети.

Идентифицированы следующие ОПАСНЫЕ СИТУАЦИИ.

HS01. Картинка на дисплее неустойчивая и неполная. Происходит задержка в обеспечении ухода за больными по причине того, что удаленный врач не может провести оценку формы ЭКГ импульса (по причине C01).

HS02. Не получены данные о сигнале тревоги. Происходит задержка в обеспечении ухода за больным по причине того, что врач не уведомлен о ПАЦИЕНТЕ, нуждающемся в лечении (по причине C01).

HS03. Удаленному врачу необходимо выбрать план лечения при отсутствии доступа к данным реального времени о ПАЦИЕНТЕ (по причине C02).

ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести

В таблице D.2 предоставлены масштабы тяжести. Следует отметить, что оценка тяжести основана на уровне остроты состояния ПАЦИЕНТА в данном конкретном случае.

НП для HS01. Короткая задержка начала лечения может привести к таким травмам для ПАЦИЕНТА, как незначительные повреждения органов. Низкая степень тяжести.

НП для HS02. Короткая задержка начала лечения может привести к таким травмам для ПАЦИЕНТА, как незначительные повреждения органов. Низкая степень тяжести.

НП для HS03. Неправильное лечение может привести к хроническим травмам ПАЦИЕНТА. Средняя тяжесть.

ШАГ 4. Оценка вероятности НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

Для оценки вероятности возникновения определенной ОПАСНОЙ СИТУАЦИИ может быть полезно провести оценку вероятности каждой связанной с данной ситуацией причины отдельно и «свести» эти оценки к оцениваемой вероятности ОПАСНОЙ СИТУАЦИИ. Необходимо отметить, что совокупная вероятность включает в себя вероятность возникновения установленных НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ после того, как уже сложилась ОПАСНАЯ СИТУАЦИЯ. Следует использовать всю доступную информацию (определенные ОПАСНЫЕ СИТУАЦИИ, все связанные с ними причины, контекст, определенные НП и т. д.) для предварительной оценки вероятности. В таблице D.1 приведена шкала вероятностных оценок.

HS01. *Вероятна.*

HS02. *Периодически вероятна.*

HS03. *Маловероятна.*

ШАГ 5. Оценка РИСКА с учетом заданных критериев допустимости

Используя таблицу D.3, вычисляется начальный уровень РИСКА, основанный на вероятности и тяжести, определенных на ШАГАХ 3 и 4.

HS01. (Низкая степень/вероятна). Уровень РИСКА — *умеренный.*

HS02. (Низкая степень/периодически вероятна). Уровень РИСКА — *умеренный.*

HS03. (Средняя степень/маловероятно). Уровень РИСКА — *умеренный.*

ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ и оценка индивидуального ОСТАТОЧНОГО РИСКА

RC01. Реализация QoS-политики для того, чтобы высокоприоритетный трафик не нарушался низкоприоритетным трафиком.

RC02. Резервное соединение с удаленным местом.

В данном примере используются только те меры по УПРАВЛЕНИЮ РИСКОМ, которые влияют на вероятность возникновения ОПАСНОЙ СИТУАЦИИ. Таким образом, определенные НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ и связанные с ними тяжести не изменяются. Новые вероятности перечислены ниже.

HS01. *Маловероятно.*

HS02. *Маловероятно.*

HS03. *Практически невероятно.*

Новые уровни РИСКА перечислены ниже.

HS01. (новая тяжесть/вероятность — *низкая степень/маловероятно*). Уровень РИСКА — *низкий.*

HS02. (новая тяжесть/вероятность — *низкая степень/маловероятно*). Уровень РИСКА — *низкий.*

HS03. (новая тяжесть/вероятность — *средняя степень/практически невероятно*). Уровень РИСКА — *низкий.*

ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ

Меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы для того, чтобы они могли быть ВЕРИФИЦИРОВАНЫ до запуска в эксплуатацию.

RC01. В случае политики QoS данная мера может быть реализована на небольшой демонстрационной сети в лаборатории, или же ОО может включить информацию о проектировании и испытании данной политики в СОГЛАШЕНИЕ ОБ ОТВЕТСТВЕННОСТИ вместе с подрядчиком ИТ, предоставляющим сетевое оборудование.

RC02. Реализация резервного канала должна быть согласована с провайдером.

ШАГ 8. ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ

ВЕРИФИКАЦИЯ RC01

Эффективность. Новая конфигурация QoS будет испытана в лаборатории перед реализацией в действующей системе в целях верификации ожидаемых рабочих характеристик.

Реализация. В данном примере УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ предназначено обеспечить завершение реализации и ее введение в действующую МЕДИЦИНСКУЮ ИТ-СЕТЬ.

ВЕРИФИКАЦИЯ RC02

Эффективность. В целях верификации ожидаемых характеристик работоспособности до реализации в действующей системе выполняется симулирование этого нового резервного канала и осуществляется его испытание в лаборатории, где особое внимание уделяется аварийному переключению. Если представляется возможным, следует выполнить испытание в реальной сети в рамках управляемого временного окна для изменения.

Реализация. В данном примере УПРАВЛЕНИЕ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ предназначено обеспечить завершение реализации и ее введение в действующую МЕДИЦИНСКУЮ ИТ-СЕТЬ.

ШАГ 9. Оценка любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ

По заключениям оценивания не было обнаружено никаких новых РИСКОВ, привнесенных добавленными мерами по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

Так как данные примеры представляют только один или два подпроцесса для ПРОЦЕССА заданной МЕДИЦИНСКОЙ ИТ-СЕТИ, концепцию совокупного ОСТАТОЧНОГО РИСКА сложно продемонстрировать. В целях настоящего стандарта следует принять, что совокупный ОСТАТОЧНЫЙ РИСК был определен как допустимый в соответствии с политикой ОО.

8.4 Пример 3. Палата послеанестезиологической помощи (PACU)

8.4.1 Полное описание контекста

Палата послеанестезиологической помощи представляет собой отделение в линейке предоставления услуг реанимации (интенсивной терапии). ПАЦИЕНТЫ данного отделения варьируются от детей младшего возраста до людей, страдающих заболеваниями пожилого возраста. Немедленный послеоперационный уход и контроль осуществляются за ПАЦИЕНТАМИ, которым предписана общая или контролируемая анестезиологическая помощь и которые только что подвергались инвазивной процедуре, вплоть до и включая хирургическую операцию. Острота состояний ПАЦИЕНТОВ варьируется от нетяжело больных до ПАЦИЕНТОВ в сложном критическом состоянии, требующих множества способов воздействия инвазивного контроля и лечения, включающего в себя искусственную вентиляцию легких. Услуги предоставляются для 1000—1200 ПАЦИЕНТОВ в месяц, и отделение работает 24 часа в сутки.

Палата послеанестезиологической помощи имеет открытую планировку. Пункт медсестры имеет линию обзора, охватывающую все постели отделения. Практикующий врач находится в непосредственной близости от ПАЦИЕНТОВ на протяжении всего времени.

8.4.2 Описание анализируемой сети

Существующее оборудование контроля ПАЦИЕНТОВ окончательно состарилось и уже не поддерживается производителем (окончание срока службы), а также не используется ни на каких других участках оказания интенсивной терапии. По этой причине финансовым комитетом был одобрен план замены оборудования.

Установленные 14 приборов контроля ПАЦИЕНТОВ PACU будут заменены 14 новыми приборами контроля ПАЦИЕНТОВ, соединенными с Центральным информационным центром (ЦИЦ). Новые приборы контроля и ЦИЦ соединены посредством проводной сети, использующей кабельную систему CAT 5 (см. рисунок 6). Данные показаний сигналов ПАЦИЕНТА в реальном времени будут передаваться в ЦИЦ для активации центральной аварийной сигнализации, распечатки и для записи данных в историю болезни. Новые приборы контроля за ПАЦИЕНТОМ будут взаимодействовать с системой кардиологической информации больницы для передачи ЭКГ в 12 отведениях, получаемых от 14 прикроватных приборов контроля. Соединение между новыми приборами контроля за ПАЦИЕНТОМ и системой кардиологической информации будет выполнено специальными многомодовыми волоконно-оптическими линиями связи, соединяющими сетевой коммутатор, предназначенный для PACU, с выделенным маршрутизатором системы кардиологической информации.

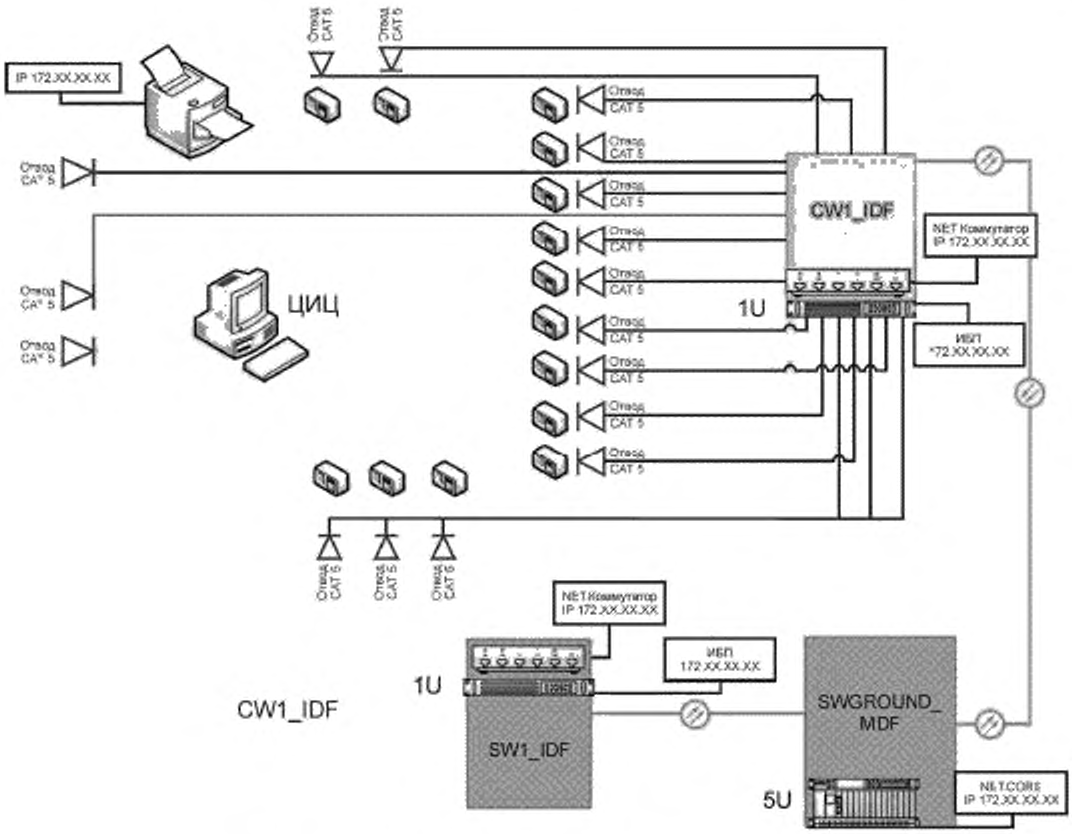


Рисунок 6 — Схема палаты послеанестезиологической помощи (PACU)

8.4.3 10 Шагов

ШАГ 1. Идентификация ОПАСНОСТИ

HAZ01. Полная потеря связи (см. рисунок 8).

ШАГ 2. Идентификация причин и возникающих ОПАСНЫХ СИТУАЦИЙ

C01. Сетевой коммутатор не был правильно сконфигурирован.

C02. Отказ аппаратуры сетевого коммутатора.

C03. Потеря питания в сетевом коммутаторе.

Идентифицированы следующие ОПАСНЫЕ СИТУАЦИИ:

HS01. Задержка или необеспечение ухода за больным из-за потери данных реального времени о ПАЦИЕНТЕ и о сигналах тревоги (по причине C01, C02 и C03).

HS02. Задержка или необеспечение ухода за больным из-за потери накопленных данных о ПАЦИЕНТЕ, включая отчеты по ЭКГ в 12 отведениях, данные устройства, записывающего на ленту, и лазерной печати (по причине C01, C02 и C03).

ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести

В палате послеанестезиологической помощи ПАЦИЕНТЫ находятся в поле зрения лечащих врачей, и они слышат сигналы тревоги прикроватных приборов контроля. Накопленные данные не несут такой же критической важности, как, например, в других отделениях, таких как реанимационное отделение. Независимые портативные приборы физиологического контроля могут применяться для распечатки данных на ленту в случае отказа всей сети. Портативные электрокардиографы могут применяться для отправки ЭКГ ПАЦИЕНТОВ в систему кардиологической информации посредством аналоговой телефонной линии.

В таблице D.2 предоставлены масштабы тяжести. Следует отметить, что оценка тяжести основана на уровне остроты состояния ПАЦИЕНТА в данном конкретном случае.

НП для HS01. В данном случае по причине того, что лечащий врач находится в поле зрения ПАЦИЕНТОВ, предполагается, что потеря данных реального времени для ЦИЦ приведет к НП не более тяжким, чем временная или незначительная травма.

Степень тяжести — *средняя*.

НП для HS02. В данном случае по причине того, что потерянные данные не являются ни данными реального времени, ни накапливаемыми данными, предполагается, что степень тяжести НП будет не более высокой, чем временный дискомфорт. Степень тяжести — *низкая*.

ШАГ 4. Оценка вероятности НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

В таблице D.1 приведена шкала вероятностных оценок.

HS01. *Маловероятно*.

HS02. *Маловероятно*.

ШАГ 5. Оценка РИСКА с учетом заданных критериев допустимости

Используя таблицу D.3, следует вычислить начальный уровень РИСКА, основанный на вероятности и тяжести, определенных на ШАГАХ 3 и 4.

HS01. (Средняя степень/маловероятно). Уровень РИСКА — *средний*.

HS02. (Низкая степень/маловероятно). Уровень РИСКА — *низкий*.

ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ и оценка индивидуального ОСТАТОЧНОГО РИСКА

В данном случае каждая причина была рассмотрена отдельно и были определены меры по УПРАВЛЕНИЮ РИСКОМ.

Причина 1. Потеря связи из-за неправильной конфигурации коммутатора.

RC01. Использовать практику управления сетевым коммутатором. Принять соглашение о присвоении уникальных имен биомедицинским (жизненно важным) сетевым коммутаторам, которые позволят отличать сетевой коммутатор от обычных коммутаторов ИТ-данных.

RC02. Физически идентифицировать сетевой коммутатор с помощью окрашенных в разные цвета соединительных кабелей, указывающих на четкое и явное отличие от прочих обычных коммутаторов ИТ-данных.

Причина 2. Отказ аппаратуры сетевого коммутатора.

RC03. Следует хранить предварительно настроенный сетевой коммутатор в отделении биомедицинской инженерии, который может послужить физической заменой дефектному сетевому коммутатору. Такой подход серьезно минимизирует простои системы.

Причина 3. Потеря питания сетевого коммутатора.

RC04. Следует подключить сетевой коммутатор к управляемому источнику бесперебойного электропитания (UPS). Если происходит сбой подачи питания сетевому шкафу, то отделу биомедицинской инженерии и ИТ-поддержке отправляется электронное письмо, указывающее на потерю питания и на тот факт, что сетевой коммутатор работает за счет питания от батареи.

RC01, RC02 и RC04 уменьшают вероятность начального возникновения ОПАСНОЙ СИТУАЦИИ (P1). RC03 вступает в силу после возникновения ОПАСНОЙ СИТУАЦИИ, таким образом она уменьшает вероятность того, что ОПАСНАЯ СИТУАЦИЯ повлечет за собой НП (P2). Вместе эти меры уменьшают вероятность до *практически невероятного* уровня.

HS01. (новая тяжесть/вероятность — *средняя степень/практически невероятно*). Уровень РИСКА — *низкий*.

HS02. (новая тяжесть /вероятность — *низкая степень/практически невероятно*). Уровень РИСКА — *низкий*.

ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ

Меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы для того, чтобы они могли быть ВЕРИФИЦИРОВАНЫ до запуска в эксплуатацию.

RC01. Управление сетевым коммутатором. Сетевому коммутатору, использующемуся для контроля ПАЦИЕНТОВ, было назначено имя «Unity_Biomed», чтобы указать, что данное устройство является компонентом контроля ПАЦИЕНТА.

RC02. Окрашенные в разные цвета соединительные кабели. Соединительные кабели, окрашенные в уникальные цвета «розовый и желтый», используются как кабели данных, идущих от прибора контроля ПАЦИЕНТА к сетевому коммутатору. Розовые и желтые соединительные кабели используются только для оборудования контроля ПАЦИЕНТА. Розовый цвет обозначает критически важные данные реального времени. Желтый цвет обозначит обмен информацией (IX) не в реальном времени, такой как запросы на печать и полное раскрытие информации.

RC03. Запасной коммутатор. Запасной предварительно настроенный сетевой коммутатор, находящийся в биомедицинском отделении, который может быть использован в случае, если в системе контроля ПАЦИЕНТА коммутатор отказал.

RC04. Источник бесперебойного питания. Сетевой коммутатор подключен к управляемому источнику бесперебойного питания.

В данном примере старая сеть может продолжать использоваться в условиях эксплуатации, пока устанавливаются новая сеть и приборы контроля. Это предоставляет возможность реализовать все меры по УПРАВЛЕНИЮ РИСКОМ перед ее запуском в эксплуатацию. (Необходимо отметить, что если реализация должна быть осуществлена в действующей сети, то может быть использовано временное окно для изменения.)

ШАГ 8. ВЕРИФИКАЦИЯ мер по УПРАВЛЕНИЮ РИСКОМ

ВЕРИФИКАЦИЯ RC01

Реализация. Доказано, что сетевые коммутаторы обладают правильно сконфигурированными именами, соответствующими определенному соглашению о присвоении имен.

Эффективность. В данном случае утверждается, что активно управляемая сеть имеет меньше шансов на отказ, чем неуправляемая. ВЕРИФИКАЦИЯ эффективности мер по УПРАВЛЕНИЮ РИСКОМ может заключаться в логическом обосновании причин такого утверждения.

ВЕРИФИКАЦИЯ RC02

Реализация. Проверкой было подтверждено, что соединительные кабели сетевых коммутаторов имеют соответствующие цвета.

Эффективность. В данном случае утверждается, что физические идентификаторы сети и окрашенные в разные цвета кабели уменьшают РИСК неправильной конфигурации. ВЕРИФИКАЦИЯ эффективности мер по УПРАВЛЕНИЮ РИСКОМ может заключаться в логическом обосновании причин такого утверждения (см. рисунок 7).

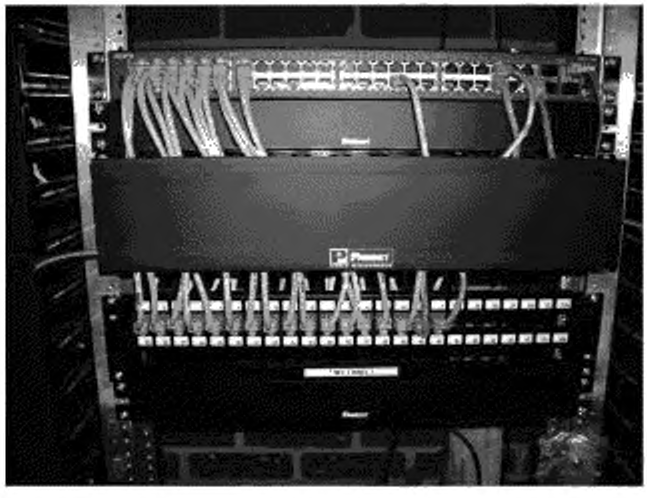


Рисунок 7 — Пример использования окрашенных в разные цвета кабелей

ВЕРИФИКАЦИЯ RC03

Реализация. Необходимо подтвердить, что в инвентаре биомедицинского отдела хранится запасной коммутатор.

Эффективность. Необходимо создать симуляцию условий отказа коммутатора и замерить время, которое займет замена данного коммутатора на запасной.

ВЕРИФИКАЦИЯ RC04

Реализация. Необходимо создать симуляцию потери питания и подтвердить, что источник бесперебойного питания подключен, а также биомедицинский и ИТ-персонал уведомлен.

Эффективность. Необходимо создать симуляцию потери питания и подтвердить подключение бесперебойного источника питания, а также отсутствие потери связи (см. рисунок 8).

ШАГ 9. Оценка любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ

По заключениям оценивания не было обнаружено никаких новых РИСКОВ, привнесенных добавленными мерами по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

Так как данные примеры представляют только один или два подпроцесса для ПРОЦЕССА заданной МЕДИЦИНСКОЙ ИТ-СЕТИ, концепцию совокупного ОСТАТОЧНОГО РИСКА сложно продемонстрировать. В целях настоящего стандарта следует принять, что совокупный ОСТАТОЧНЫЙ РИСК был определен как допустимый в соответствии с политикой ОО.

№	ОПАСНОСТЬ	Причина(ы), способствующие факторы	ОПАСНАЯ СИТУАЦИЯ	НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ	Начальный РИСК			Меры ослабления РИСКА/ УПРАВЛЕНИЯ РИСКОМ, обеспеченные проектом, защитные меры, или клинический ПРОЦЕСС, или информация по БЕЗОПАСНОСТИ	Ссылка на спецификации, политику или отчеты об испытаниях ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ, а также к другим пунктам настоящего стандарта (ко всем, которые могут использоваться для прослеживания)	ОСТАТОЧНЫЙ РИСК		
					Тяжесть	Вероятность	РИСК (уровень)			Тяжесть	Вероятность	РИСК
1	HA201. Полная потеря связи в сети	C01.Сетевой коммутатор неправильно сконфигурирован	HS01.Задержка или необеспечение ухода за больным из-за потери данных реального времени о ПАЦИЕНТЕ и о сигналах тревоги (по причине C01, C02 и C03)	Задержка обеспечения ухода за пациентом в палате послеанестезиологической помощи ПАЦИЕНТЫ находятся в поле зрения лечащих врачей, и они слышат сигналы тревоги прикроватных приборов контроля Накопленные данные не несут такой же критической важности, как, например, в других отделениях, таких как реанимационное отделение Независимые портативные приборы физиологического контроля могут применяться для распечатки данных на ленту в случае отказа всей сети. Портативные электрокардиографы могут применяться для отправки ЭКГ ПАЦИЕНТОВ в систему кардиологической информации посредством аналоговой телефонной линии	Средняя степень	Маловероятно	Умеренный	RC01. Управление сетевым коммутатором Сетевому коммутатору, используемому для контроля ПАЦИЕНТОВ, было назначено имя «Unity_Biomed», чтобы указать что данное устройство является компонентом контроля ПАЦИЕНТА RC02 Окрашенные в разные цвета соединительные кабели. Соединительные кабели, окрашенные в уникальные цвета «розовый и желтый», используются как кабели данных, идущих от прибора контроля ПАЦИЕНТА к сетевому коммутатору Розовые и желтые соединительные кабели используются только для оборудования контроля ПАЦИЕНТА. Розовый цвет обозначает критически важные данные реального времени Желтый цвет обозначает обмен информацией (IX) не в реальном времени такой как запросы на печать и полное раскрытие информации	Ознакомьтесь с политикой клиники для чрезвычайных ситуаций в палате послеанестезиологической помощи	Средняя степень	Практически невероятно	Низкий
		C02 Отказ аппаратуры сетевого коммутатора	HS02 Задержка или необеспечение ухода за больным из-за потери накопленных данных о ПАЦИЕНТЕ, включая отчеты по ЭКГ в 12 отведениях, данные устройства, записывающего на ленту, и лазерной печати (по причине C01, C02 и C03)		Низкая степень	Маловероятно	Низкий	RC03 Запасной предварительно настроенный сетевой коммутатор, находящийся в биомедицинском отделении, который может быть установлен	Укажите имя и дату ВЕРИФИКАЦИИ в файле УПРАВЛЕНИЯ РИСКОМ	Низкая степень	Практически невероятно	Низкий
		C03 Потеря питания в сетевом коммутаторе						RC04 Сетевой коммутатор подключен к управляемому источнику бесперебойного питания	Электронное письмо от устройства о подтверждении испытания. Часть файла УПРАВЛЕНИЯ РИСКОМ			

Рисунок 8 — Образец сводного реестра ОЦЕНКИ РИСКА для примера палаты послеанестезиологической помощи (PACU)

8.5 Пример 4. Ультразвук. Уязвимость в операционной системе (ОС)

8.5.1 Полное описание контекста

Разработчик ОС выпускает исправление для своей операционной системы, которое устраняет потенциальную уязвимость (идентифицированный вирус-червь) в ультразвуковой системе. Если ультразвуковая система не защищена, то это может повлиять на обеспечение ухода за ПАЦИЕНТАМИ (снижение скорости, непригодные функции). ПРОИЗВОДИТЕЛЮ ультразвукового устройства требуется время для верификации и подтверждения соответствия выпущенного исправления перед тем, как его можно будет применить в МЕДИЦИНСКОМ ПРИБОРЕ. Вирус-червь был обнаружен в приборе, подключенном к сети внутри ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Данная сеть используется для получения информации о ПАЦИЕНТАХ и запланированных процедурах из информационной системы больницы (например, сервера, хранящего список методов формирования цифровых изображений и обмена ими в медицине DICOM). Сеть предоставляет средства для архивирования, перемещая результаты исследования эхограмм из ультразвуковой системы в систему передачи и архивирования изображений (PACS). Последней стадией данной процедуры является отправка отчета об успешном завершении исследования из сети в информационную систему больницы. В качестве компонента в сеть может быть добавлена рабочая станция, которая впоследствии может применяться для извлечения эхограмм из сервера PACS для дополнительной обработки, такой как осуществление измерений и отправка отчетов об ультразвуковой системе, что позволяет создать эффективный рабочий процесс для ПАЦИЕНТОВ и рентгенологов. После того как вирус-червь проник в ультразвуковую систему, он может использовать уязвимые места в ОС других устройств, соединенных с ИТ-СЕТЬЮ, принадлежащей ОО. ОО осознает, что РИСКИ, связанные с уязвимостью в ультразвуковой системе, которые не были устранены, должны быть управляемыми.

8.5.2 Описание анализируемой сети

Ethernet-сеть охватывает всю больницу и поддерживает скорость 100 МВ/Гигабит в секунду. Сервер DHCP [протокола динамической конфигурации главного узла (хоста) сети] способен автоматически управлять конфигурацией IP-АДРЕСОВ. Ультразвуковая система представляет собой мобильный МЕДИЦИНСКИЙ ПРИБОР, который перемещается между палатой зондирования, палатой неотложной медицинской помощи и другими палатами в больнице. В сети присутствуют виртуальные ЛС (локальные сети), предназначенные для создания анклавов (защищенных сетей), в которых используются МЕДИЦИНСКИЕ ПРИБОРЫ, и для отделения МЕДИЦИНСКИХ ПРИБОРОВ от стандартных стационарных компьютеров. Все устройства, подключенные к PACS, находятся в одной виртуальной ЛС.

8.5.3 10 шагов

ШАГ 1. Идентификация ОПАСНОСТИ

HAZ01. Несанкционированный доступ к данным (к информации о ПАЦИЕНТЕ или об организации).

HAZ02. Нарушена функция МЕДИЦИНСКОГО ПРИБОРА (потеря функциональной пригодности системы).

HAZ03. Потеря доступа (доступ к данным, необходимым для процедур, ограничен или закрыт).

ШАГ 2. Идентификация причин и возникающих ОПАСНЫХ СИТУАЦИЙ

C01. Раскрытие данных о ПАЦИЕНТЕ. Вредоносное программное обеспечение, способное извлекать персональную, поддающуюся идентификации, информацию (PII — личные данные, такие как номер социального страхования, номер медицинской карты, дату рождения...) и экспортировать ее из системы в случае обнаружения.

C02. Снижение производительности системы. Вредоносное или невредоносное программное обеспечение загружено и установлено в систему. Системные ресурсы затрачиваются на инструменты раскрытия паролей, переполнение сети, сканирование или обмен информацией в сети.

C03. Раскрытие личных данных. Из-за этой уязвимости ультразвуковое устройство может стать источником угроз для других устройств, подключенных к ИТ-СЕТИ.

Идентифицированы следующие ОПАСНЫЕ СИТУАЦИИ:

HS01. (Защищенность данных) Без ведома лечащего врача или рентгенолога вирус или вирус-червь устанавливает программу перехвата вводимой с клавиатуры информации (кейлогер) или же автоматически начинает извлекать персональную, поддающуюся идентификации, информацию и отправляет регистрационное имя пользователя и PII в несанкционированное место (по причине C01).

HS02. (БЕЗОПАСНОСТЬ) Во время процедуры сканирования (для родовспоможения, кардиологии, желудочно-кишечного тракта) расход аппаратных ресурсов на вредоносное программное обеспечение

нарушает выполнение работы, что приводит к отказу процедуры формирования изображения и подвергает риску процесс лечения (например, становится невозможным управление иглой амниоцентеза) (по причине С02).

HS03. (Эффективность) Потеря доступа. Отказ в доступе к серверу со списком методов в связи с серьезным переполнением сети, или система не может получить доступ к серверу PACS для сохранения полученных данных изображений для использования в отключенной от сети реанимационной тележке и других медицинских процедурах. При отказе системы планирования лечащий врач/техник должен прибегнуть к ручным методам (по причине С02).

HS04. (Защищенность и эффективность) Без ведома лечащего врача и персонала больницы множество устройств оказалось подвержено уязвимости, которая ведет к возникновению HS01 и HS03 в других устройствах в сетевом анклаве (по причине С03).

ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести

В таблице D.2 предоставлены масштабы тяжести. Следует отметить, что оценка тяжести основана на уровне остроты состояния ПАЦИЕНТА в данном конкретном случае.

НП для HS01. Нарушение неприкосновенности частной жизни, раскрытие ДАННЫХ о ЗДОРОВЬЕ ПАЦИЕНТА, несанкционированное раскрытие медицинских данных и уведомление о нарушении для ОТВЕТСТВЕННОЙ ОРГАНИЗАЦИИ. Необратимое раскрытие ДАННЫХ о ЗДОРОВЬЕ ПАЦИЕНТА может привести к несанкционированному использованию данных ПАЦИЕНТА. Степень тяжести — *низкая*.

НП для HS02. Отмененная процедура или задержанное лечение. Отказ при локализации иглой может быть обнаружен, и процедуры будут отменены. Степень тяжести — *средняя*.

НП для HS03. Лечащий врач должен прибегнуть к ручным методам, что затрудняет выполнение операции. Степень тяжести — *низкая*.

НП для HS04. Уязвимость сказалась на множестве других МЕДИЦИНСКИХ ПРИБОРОВ. Степень тяжести — *высокая*.

ШАГ 4. Оценка вероятности НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

Для оценки вероятности должны быть учтены существующие меры по УПРАВЛЕНИЮ РИСКОМ, уже заложенные в МЕДИЦИНСКИЙ ПРИБОР. При учете данных мер управления вероятность НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ оценивается так, как это показано ниже. Меры по УПРАВЛЕНИЮ РИСКОМ варьируются от прибора к прибору и будут влиять на ранжирование вероятности в зависимости от установленных средств управления.

- Ультразвуковой прибор имеет аппаратно реализованную ОС. На устройстве отсутствуют интернет-браузеры, службы ограничиваются наличием только тех, что требуются для ПРЕДНАМЕРЕННОГО ИСПОЛЬЗОВАНИЯ; присутствуют средства управления доступом.

- Необходимо открыть порты для использования. Ультразвуковой прибор обладает программным брандмауэром, который блокирует все порты, кроме 104, использующегося для ИНТЕРОПЕРАБЕЛЬНОСТИ DICOM.

- В виртуальной ЛС не было обнаружено вирусов-червей, что свидетельствует о том, что данный анклав виртуальной ЛС выдерживает текущее испытание.

В таблице D.1 приведена шкала вероятностных оценок.

HS01. *Маловероятно.*

HS02. *Практически невероятно.*

HS03. *Маловероятно.*

HS04. *Периодически вероятно.*

ШАГ 5. Оценка РИСКА с учетом заданных критериев допустимости

Используя таблицу D.3, вычислить начальный уровень РИСКА, основанный на вероятности и тяжести, определенных на ШАГАХ 3 и 4.

HS01. (низкая степень/маловероятно). Уровень РИСКА — *низкий*.

HS02. (средняя степень/практически невероятно). Уровень РИСКА — *низкий*.

HS03. (низкая степень/маловероятно). Уровень РИСКА — *низкий*.

HS04. (высокая степень/периодически вероятно). Уровень РИСКА — *умеренный*.

ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ и оценка индивидуального ОСТАТОЧНОГО РИСКА

Существуют легко осуществимые меры по УПРАВЛЕНИЮ РИСКОМ, которые могут быть применены на сетевом уровне.

RC01. Использовать резервирование DHCP для определенного диапазона ультразвуковых аппаратов таким образом, чтобы контроль сетевого трафика мог инициировать сигналы тревоги.

RC02. Использовать сетевые брандмауэры для защиты виртуальных ЛС от нежелательного трафика.

RC03. Установить исправление для ультразвуковой системы.

RC04. Отсоединить ультразвуковую систему от сети.

Все вышеперечисленные меры по УПРАВЛЕНИЮ РИСКОМ уменьшают Р1. В данном примере вероятности уже были невысокими, но RC01 и RC02 считаются лучшими методами. RC03 (применение исправлений для ОС или антивирусного приложения к ультразвуковой системе) не была выбрана, так как последствия применения этой меры для приборов неизвестны или же она может привести к неполноценной конфигурации, которая в свою очередь может повлечь за собой HS02, что делает ее неподходящей.

RC04 (отсоединение ультразвуковой системы от сети) не была выбрана. Данная мера понижает БЕЗОПАСНОСТЬ из-за увеличения вероятности возникновения ошибок, связанной с месяцами ручной обработки данных, которая ведет к повышению вероятности возникновения неполных и неправильно распределенных записей о ПАЦИЕНТЕ. Последние в свою очередь ведут к возможному неправильному лечению.

Новые уровни РИСКА:

HS01. *Низкий.*

HS02. *Низкий.*

HS03. *Низкий (не изменился).*

HS04. *Умеренный (не изменился).*

ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ

Меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы для того, чтобы они могли быть ВЕРИФИЦИРОВАНЫ до запуска в эксплуатацию.

RC01. Резервирование DHCP может быть реализовано в системе, которая не подвергается клиническому применению. Данная система может использоваться при ВЕРИФИКАЦИИ УПРАВЛЕНИЯ РИСКОМ.

RC02. Брандмауэры могут быть испытаны на маленьких образцовых сетях в лаборатории или во время окна времени для изменения в действующей сети.

ШАГ 8. Верификация мер по УПРАВЛЕНИЮ РИСКОМ

ВЕРИФИКАЦИЯ RC01

Реализация. Следует подтвердить, что ультразвуковая система получает правильный адрес, и воспользоваться симуляцией клинической ситуации для подтверждения связи.

Эффективность. В данном случае утверждается, что вредоносный трафик был заблокирован и не достиг МЕДИЦИНСКОГО ПРИБОРА. ВЕРИФИКАЦИЯ эффективности мер по УПРАВЛЕНИЮ РИСКОМ может заключаться в логическом обосновании такого утверждения.

ВЕРИФИКАЦИЯ RC02

Реализация. Следует создать симуляцию нежелательного трафика и подтвердить, что брандмауэр его не пропускает.

Эффективность. В данном случае утверждается, что вредоносный трафик был заблокирован и не достиг МЕДИЦИНСКОГО ПРИБОРА. ВЕРИФИКАЦИЯ эффективности мер по УПРАВЛЕНИЮ РИСКОМ может заключаться в логическом обосновании такого утверждения.

ШАГ 9. Оценка любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ

По заключениям оценивания не было обнаружено никаких новых РИСКОВ, привнесенных добавленными мерами по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

Так как данные примеры представляют только один или два подпроцесса для ПРОЦЕССА заданной МЕДИЦИНСКОЙ ИТ-СЕТИ, концепцию совокупного ОСТАТОЧНОГО РИСКА сложно продемонстрировать.

Согласно МЭК 80001-1:2010, «настолько, насколько УПРАВЛЕНИЕ РИСКОМ требует уступок по ОСНОВНЫМ СВОЙСТВАМ, ОСНОВНЫЕ СВОЙСТВА должны рассматриваться в порядке приоритета БЕЗОПАСНОСТЬ, ЭФФЕКТИВНОСТЬ и ЗАЩИЩЕННОСТЬ ДАННЫХ И СИСТЕМ». В данном примере показатели РИСКА для БЕЗОПАСНОСТИ и защищенности были улучшены за счет реализации двух типов средств УПРАВЛЕНИЯ РИСКОМ. Допустимый, но в то же время нежелательный РИСК для HS04 не может быть улучшен, так как идентифицированные средства УПРАВЛЕНИЯ РИСКОМ увеличивают РИСК для БЕЗОПАСНОСТИ ПАЦИЕНТА, что является недопустимым, согласно политике ОО. Совокупный РИСК соответствует политике ОО и потому является допустимым.

Приложение А
(справочное)

Распространенные ОПАСНОСТИ, ОПАСНЫЕ СИТУАЦИИ и их причины, которые следует учесть при работе с МЕДИЦИНСКИМИ ИТ-СЕТЯМИ

А.1 Типичные ОПАСНОСТИ в МЕДИЦИНСКИХ ИТ-СЕТЯХ

Ниже перечислены ОПАСНОСТИ, которые следует учитывать при выполнении АНАЛИЗА РИСКА в МЕДИЦИНСКОЙ ИТ-СЕТИ. Они структурированы иерархически, что помогает организовать как деятельность по ОЦЕНКЕ РИСКА, так и процесс документального оформления.

Также важно учитывать, что любая из перечисленных ниже ОПАСНОСТЕЙ может сказаться на одном из трех ОСНОВНЫХ СВОЙСТВ:

1) потеря работоспособности (нарушенная доступность):

a) значительная потеря работоспособности:

i) потеря данных (потеря связи):

a. временная связь;

b. полная потеря связи;

ii) потеря работоспособности МЕДИЦИНСКОГО ПРИБОРА:

a. неправильные данные (нарушенная целостность):

b. неправильные данные (расхождение в данных ПАЦИЕНТОВ);

b) ухудшение работоспособности:

i) неправильное или нецелесообразное распределение данных во времени;

ii) неправильный или нецелесообразный обмен данными или ИНТЕРОПЕРАБЕЛЬНОСТЬ;

iii) непреднамеренные взаимодействия между терминалами;

iv) ухудшение работоспособности МЕДИЦИНСКОГО УСТРОЙСТВА;

2) потеря конфиденциальности:

a) несанкционированный доступ к данным.

Организации могут рассмотреть возможность соотнести ОПАСНОСТИ, с которыми они сталкиваются, с нежелательными явлениями, разобранными в других спецификациях, таких как ИСО 19218.

А.2 Типы ОПАСНЫХ СИТУАЦИЙ

Необходимо отметить, что после того как ОПАСНАЯ СИТУАЦИЯ была определена, появляется возможность предсказать возможные НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ и их тяжесть. Эта деталь может быть добавлена в описание ОПАСНОЙ СИТУАЦИИ (т. е. величина задержки в минутах) и/или описана в контексте, связанном с анализируемой сетью:

- задержка в обеспечении ухода за пациентом;
- отсутствие обеспечения ухода за пациентом;
- предоставление ненадлежащего ухода или лечения;
- нарушение неприкосновенности частной жизни или конфиденциальности (раскрытие ДАННЫХ О ЗДОРОВЬЕ ПАЦИЕНТА);
- неправильная или неполная информация в правовом отчете или истории болезни;
- отказ в предоставлении лабораторных данных или дозирования лекарств;
- отказ отображения на экране медикаментов, администрируемых системой;
- отсутствие возможности принять ПАЦИЕНТА в кабинете неотложной помощи.

А.3 Распространенные причины в МЕДИЦИНСКИХ ИТ-СЕТЯХ

- Перегруженный канал.
- Неправильная конфигурация качества услуги.
- Провал беспроводного сигнала.
- Конфликт IP-адресов.
- Слишком агрессивная защита предотвращает соединение.
- Неисправные кабели.
- Отказ сетевого оборудования.
- Отказ программного обеспечения сети.
- Неправильная конфигурация (преднамеренная).
- Неправильная конфигурация (непреднамеренная).
- Потеря питания.
- Непреднамеренное отсоединение кабеля от коммутаторного щита.
- Непреднамеренное отсоединение кабеля в палате ПАЦИЕНТА.
- Вирус.

- Слишком строгая политика обеспечения защиты.
- Пользовательские ошибки.
- Несоответствующие процедуры.
- Неправильное выполнение процедур.
- Несоответствующее обучение.
- Ошибка конфигурации сети.
- ЭМП.
- Присоединение к сети зараженного компьютера.
- Проникновение в сеть вируса, пришедшего из внешней/соседней сети.
- Дистанционное обслуживание.
- Неудачное или неполное обновление.
- Враждебная «атака» на МЕДИЦИНСКУЮ ИТ-СЕТЬ.
- Непреднамеренная утечка информации.

Ограниченная функциональность прибора при передаче данных, вызванная обновлением программного обеспечения или технических средств.

А.4 Связь между требующимися характеристиками сети и ОПАСНОСТЯМИ

Перечисленные в приведенной ниже таблице характеристики могут быть определены для прибора, который требуется подключить к МЕДИЦИНСКОЙ ИТ-СЕТИ. В 3.5 МЭК 80001-1:2010 они именуются «требующимися характеристиками». Каждая такая характеристика может быть связана с ОПАСНОСТЬЮ, как это показано в таблице А.1.

Таблица А.1 — Опасности в привязке к предполагаемым требующимся характеристикам сети

Предполагаемые требующиеся характеристики сети	ОПАСНОСТИ, связанные с характеристиками
Сеть должна обеспечить связь (доставку пакетов данных с определенной скоростью)	Потеря данных (потеря связи)
Сеть должна доставлять трафик только адресату	Неправильный или несоответствующий обмен данными или неожиданное получение данных
Соответствие — сеть не должна искажать данные	Неправильные данные
Задержка <= x	Неправильная или несоответствующая синхронизация данных
Дрожание <= y	
Защищенность. Сеть не должна пропускать вредоносный трафик к устройству	Потеря работоспособности (более конкретная ОПАСНОСТЬ зависит от устройства)
Защищенность. Сеть должна защищать уязвимые данные	Несанкционированный доступ к данным
Примечание — Перечисленные ОПАСНОСТИ основаны на МЭК 60601-1:2005, пункты 14.6.1, H.7.2.	

А.5 Связь между ОПАСНОСТЯМИ, предсказуемыми последовательностями и причинами

Таблица А.2 помогает понять связь между ОПАСНОСТЯМИ и причинами.

Таблица А.2 — Связь между ОПАСНОСТЯМИ, предсказуемыми последовательностями и причинами

ОПАСНОСТЬ	Более конкретная ОПАСНОСТЬ (ПРОИЗВОДИТЕЛЬ использует ее в качестве причины)	Причина
Потеря данных	Временная связь (отброшенные пакеты)	Перегруженный канал Неправильная конфигурация QoS Выпадение беспроводного сигнала Конфликт IP-адресов Слишком агрессивная защита предотвращает соединение Провал сигнала радиочастоты (РЧ) Неисправные кабели

Окончание таблицы А.2

ОПАСНОСТЬ	Более конкретная ОПАСНОСТЬ (ПРОИЗВОДИТЕЛЬ использует ее в качестве причины)	Причина
Потеря данных	Полная потеря связности	Отказ технических средств сети Отказ программного обеспечения сети Неправильная конфигурация (преднамеренная или непреднамеренная) Потеря питания Непреднамеренное отсоединение кабеля от коммутаторного щита Непреднамеренное отсоединение кабеля в палате ПАЦИЕНТА Вирус Слишком строга политика обеспечения защиты Пользовательские ошибки Организационные несоответствия
Неправильный или несоответствующий обмен данными или неожиданное получение данных		Конфликт IP-адресов Отказ технических средств сети Отказ программного обеспечения сети Отказ конфигурации сети
Неправильные данные		ЭМП Неисправные кабели
Неправильная или несоответствующая синхронизация данных	Задержка > x	Перегруженный канал Неправильная конфигурация QoS
	Дрожание < y	Перегруженный канал Неправильная конфигурация QoS
Потеря работоспособности (прибора)		Присоединение зараженного компьютера к сети Проникновение в сеть вируса, пришедшего из внешней/соседней сети
Несанкционированный доступ к данным		Демонстрация личных данных на экране в публичном месте Вредоносный перехват беспроводных данных Вредоносный перехват проводных данных в сетевом шкафу
Пользовательские ошибки		Несоответствующее обучение Сложные потоки работ Установка несоответствующих каналов коммуникаций между отделениями

А.6 ОПАСНОСТИ, причины, предсказуемые последовательности и ОПАСНЫЕ СИТУАЦИИ

Таблица А.3 помогает понять связь между ОПАСНОСТЯМИ, причинами, прогнозируемыми последовательностями и ОПАСНЫМИ СИТУАЦИЯМИ.

Таблица А.3 — Связь между ОПАСНОСТЯМИ, причинами, прогнозируемыми последовательностями и ОПАСНЫМИ СИТУАЦИЯМИ

ОПАСНОСТЬ	Предсказуемая последовательность	ОПАСНАЯ СИТУАЦИЯ
1.0 ОПАСНОСТИ потери работоспособности		
Потеря данных	Неправильная конфигурация компонента сети (причина) Потеря связи Данные об аварийных сигналах не получены	Лечащий врач не уведомлен о сигнале тревоги от ПАЦИЕНТА

Окончание таблицы А.3

ОПАСНОСТЬ	Предсказуемая последовательность	ОПАСНАЯ СИТУАЦИЯ
Потеря данных	Плохо спроектированная сеть (причина) Перегруженный канал Связь с перебоями Искажение формы сигнала в реальном времени	Лечащий врач не способен поставить пациенту правильный диагноз
Подраздел 7.3		
Связь с перебоями	Незапланированный трафик не в режиме реального времени пытается воспользоваться каналом (причина) Перегруженный канал ГВС Временная потеря пакетов	Картинка на дисплее неустойчивая и неполная. Задержка в обеспечении ухода за больными по причине того, что удаленный врач не может провести оценку формы ЭКГ импульса
Связь с перебоями	Незапланированный трафик не в режиме реального времени пытается воспользоваться каналом (причина) Перегруженный канал ГВС Временная потеря пакетов	Не получены данные о сигнале тревоги. Задержка в обеспечении ухода за больным по причине того, что врач не уведомлен о ПАЦИЕНТЕ, нуждающемся в лечении
Полная потеря связи	Выход ГВС из строя, неконтролируемый ОО (отказ средства доступа)	Удаленному врачу необходимо выбрать план лечения при отсутствии доступа к данным реального времени о ПАЦИЕНТЕ. Предоставление ненадлежащего ухода или лечения

Приложение В
(справочное)

Список вопросов, которые следует рассмотреть во время идентификации ОПАСНОСТЕЙ МЕДИЦИНСКОЙ ИТ-СЕТИ

Дополняя приложение С ИСО 14971:2007 при рассмотрении возможных причин и ОПАСНОСТЕЙ, следует учитывать следующие вопросы:

a) Случаи разумно предсказуемого неправильного использования

Является ли соединением с сетью несоответствующего с ПРЕДНАЗНАЧЕННЫМ ИСПОЛЬЗОВАНИЕМ каждого входящего в нее МЕДИЦИНСКОГО ПРИБОРА?

b) Неправильный поток данных к или от каждого МЕДИЦИНСКОГО УСТРОЙСТВА в МЕДИЦИНСКОЙ ИТ-СЕТИ

Для чего используются данные, передаваемые по сети, и с какими задачами они связаны?

c) Чрезмерное использование/загрузка МЕДИЦИНСКОЙ ИТ-СЕТИ сетевыми узлами

Какое число сетевых узлов планируется использовать и каков предполагаемый коэффициент их загрузки? Достаточно ли имеющихся ресурсов для удовлетворения нужд ИТ-СЕТИ и подключенных к ней приборов?

d) Ошибки пользователя

Какие навыки требуются от ОПЕРАТОРА для его эффективной работы с системой?

e) Несоответствующее УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ

Приводит ли периодическое сервисное обслуживание к изменению характеристик (например, после удаления доступа, обновлений программного обеспечения и оборудования)? Обеспечивает ли ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ анализ и разрешение модификаций каждого МЕДИЦИНСКОГО ПРИБОРА?

f) Информация в неправильном месте

Поступают ли данные в подходящее и ожидаемое место? Сопровождаются ли эти данные другими данными, не имеющими отношения к делу, которые могут сбить с толку ОПЕРАТОРА или затруднить понимание желаемых данных? При поступлении данных указан ли соответствующим образом их источник?

Приложение С
(справочное)

Уровни МЕДИЦИНСКИХ ИТ-СЕТЕЙ, на которых могут встречаться ошибки

С.1 Обзор

МЕДИЦИНСКАЯ ИТ-СЕТЬ может рассматриваться как состоящая на двух общих уровнях (см. таблицу С.1):

1) подключенные устройства — это те системы, которые используют сеть;

2) инфраструктура сети — это сетевые компоненты и связанные с ними топология и конфигурация (ЛС, WAN, сеть поставщика, сотовая связь и т. д.).

Каждый из данных уровней может, в свою очередь, быть разделен на подсистемы и системные уровни (см. таблицу С.1):

1) подсистема — это индивидуальный компонент или совокупность компонентов (аппаратных/программных);

2) система — это подсистемы, работающие вместе.

Таблица С.1 — Уровни МЕДИЦИНСКОЙ ИТ-СЕТИ

			Примеры
Подсистемы	Подключенные устройства	Система	Взаимодействия устройства с устройством. Конфигурации устройств
		Подсистема	Серверы, главные узлы (хосты), оконечные устройства (например, прибор контроля ПАЦИЕНТА)
	Инфраструктура сети	Система	Все компоненты сети, работающие вместе
		Подсистема	Коммутаторы, маршрутизаторы, точки доступа. Система предотвращения проникновений (IPS). Система обнаружения проникновений (IDS). Брандмауэры. Радиоэлектронное оборудование. Сотовые компоненты

С.2 Ошибки и сбои

Данные уровни можно также разделить по функциональности (делает ли система то, что от нее требуется) и по рабочим характеристикам (может ли она продолжать корректно функционировать под нагрузкой и в экстремальных/граничных условиях).

С точки зрения ОО рассуждения о том, где во всей МЕДИЦИНСКОЙ ИТ-СЕТИ могут возникать ошибки и сбои, затрагивают две категории сбоев:

a) Сбои, не поддающиеся управлению со стороны ОО. Это ошибки, которые уже существовали в подсистеме, когда она была предоставлена для ОО, будь эта система коммутатором, маршрутизатором, сервером или МЕДИЦИНСКИМ ПРИБОРОМ. Данная категория также включает в себя сбои служб связи, предоставляемых для ОО (т. е. в выделенной линии или при подключении к интернету).

b) Сбои, управляемые ОО. Подсистемы, предоставленные поставщиком ИТ-услуг или ПРОИЗВОДИТЕЛЕМ, функционируют и имеют рабочие характеристики в соответствии со спецификацией, но топология, конфигурация и рабочие процессы, установленные в ОО, не поддерживаются. Хорошим примером является перегрузка восходящего канала связи.

Таблица С.2 демонстрирует данные уровни, а также то, где могут встречаться сбои двух вышеописанных разновидностей.

Таблица С.2 — Пример уровней МЕДИЦИНСКОЙ ИТ-СЕТИ

Где могут встречаться ошибки или сбои?						
Суперсистема	Подключенные устройства	Система	Взаимодействия устройства с устройством. Конфигурации устройств	Конфигурация	Устройства сконфигурированы для предполагаемого применения или рабочего процесса?	Отказы на данном уровне являются ошибками конфигурации устройства, т. е. соотношение скорость/дуплекс или IP-АДРЕС, или запланированное хранение на серверах с нехваткой места
				Рабочие характеристики	Корректно ли взаимодействуют устройства под нагрузкой и в граничных условиях при любой допустимой конфигурации?	На данном уровне ПРОИЗВОДИТЕЛИ верифицируют устройства на заявленное соответствие (собственные устройства или устройства других ПРОИЗВОДИТЕЛЕЙ). ОО ответственны за верификацию новых взаимодействий
				Функциональность	Корректно ли взаимодействуют устройства?	
		Подсистема	Серверы, хосты, оконечные устройства (например, прибор контроля ПАЦИЕНТА)	Рабочие характеристики	Корректно ли работают устройства под нагрузкой и в граничных условиях при любой допустимой конфигурации?	На данном уровне ПРОИЗВОДИТЕЛИ осуществляют верификацию и уведомляют пользователей об ОСТАТОЧНОМ РИСКЕ
				Функциональность	Корректно ли работают устройства?	
	Инфраструктура сети	Система	Все компоненты сети, работающие вместе	Конфигурация	Корректно ли сконфигурированы компоненты (локальные конфигурации, т. е. конфигурации портов коммутатора, и конфигурации системы, т. е. конфигурации маршрутизации и коммутации)?	На данных уровнях отказы происходят по причинам, связанным с проектированием сети и из-за отказов конфигурации, т. е. из-за недостаточной полосы пропускания для заданной нагрузки, конфигурации QoS, топологии и т. д. Все это требует от ОО внесения исправлений
				Топология	Правильно ли соединены компоненты (конструкция сети)?	
				Рабочие характеристики	Т. е. осуществимы ли маршрутизация и конвертирование под нагрузкой и в граничных условиях?	На данном уровне отказы уже существуют в сетевом устройстве в том виде, как оно было поставлено вендором. Это требует либо внесения исправлений вендором или поставщиком услуг, или временного решения от ОО. Компоненты сети не обязательно являются регламентированными МЕДИЦИНСКИМИ ПРИБОРАМИ и могут не соответствовать стандартам медицинских приборов и быть неиспытанными. Может потребоваться испытание приборов для использования в МЕДИЦИНСКОЙ ИТ-СЕТИ
				Функциональность	Т. е. осуществимы ли таблицы маршрутизации, связующие деревья?	
		Подсистема	Коммутаторы, маршрутизаторы, система предотвращения проникновений (IPS), система обнаружения проникновений (IDS), брандмауэры, радиоэлектронное оборудование, сотовые компоненты	Рабочие характеристики	Работает ли в соответствии с техническими характеристиками под нагрузкой и в граничных условиях?	
				Функциональность	Пересылка пакетов осуществляется корректно?	

Приложение D
(справочное)

Шкалы вероятности, тяжести и допустимости РИСКА, используемые в примерах настоящего стандарта

Таблица D.1 — Шкала вероятностных оценок, используемая в настоящем стандарте

Часто вероятно (Frequent)	НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ возникают часто или же происходят каждый раз
Вероятно (Probable)	Возникновение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ очень вероятно
Периодически вероятно (Occasional)	Возникновение любых НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ вероятно в определенной степени
Маловероятно (Remote)	Возникновение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ маловероятно
Практически невероятно (Improbable)	Возникновение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ практически невероятно

Таблица D.2 — Шкала тяжести

Масштаб	БЕЗОПАСНОСТЬ РИСК нанесения ВРЕДА	ЭФФЕКТИВНОСТЬ	ЗАЩИЩЕННОСТЬ ДАННЫХ
Катастрофическая степень (catastrophic)	Тяжелая травма, смерть	Запланированная операция больше не представляется возможной	Может привести к полному разглашению конфиденциальной информации
Высокая степень (high)	Непоправимое поражение функции тела или непоправимое повреждение структуры тела	Запланированная операция прервана или задержана	Может привести к разглашению большого объема конфиденциальной информации
Средняя степень (medium)	Временная и незначительная травма, требуется медицинское вмешательство	От неудобства до прерывания операции	Раскрытие конфиденциальной информации может создать неловкое положение. Исправление потребует определенной затраты ресурсов
Низкая степень (low)	Временный дискомфорт, устранимый без медицинского вмешательства	Незначительное влияние на операцию или неудобство	Раскрытие конфиденциальной информации может оказать слабое влияние на организацию или отдельные лица. Исправление требует минимум усилий
Пренебрежимо малая степень (negligible)	Незначительный и кратковременный дискомфорт	Не сказывается на операции или имеет незначительное на нее влияние	Если угроза реализована и используется уязвимость, то она имеет пренебрежительно малый эффект

Таблица D.3 — Шкала уровней РИСКА

	НЕПРЕДНАМЕРЕННЫЕ ПОСЛЕДСТВИЯ для защищенности, ЭФФЕКТИВНОСТИ и ЗАЩИЩЕННОСТИ ДАННЫХ И СИСТЕМЫ	Увеличение вероятности →				
		Практически невероятно	Маловероятно	Периодически вероятно	Вероятно	Часто вероятно
Увеличение степени тяжести ↑	Катастрофическая	Умеренный	Высокий	Высокий	Высокий	Высокий
	Высокая степень	Умеренный	Умеренный	Высокий	Высокий	Высокий
	Средняя степень	Низкий	Умеренный	Умеренный	Высокий	Высокий
	Низкая степень	Низкий	Низкий	Умеренный	Умеренный	Высокий
	Пренебрежительно малая	Низкий	Низкий	Низкий	Умеренный	Умеренный

Высокий	РИСК для целей является недопустимым, РИСК должен быть уменьшен перед использованием МЕДИЦИНСКОЙ ИТ-СЕТИ посредством уменьшения вероятности или за счет снижения степени тяжести
Умеренный	Допустимость РИСКА требует дальнейшего рассмотрения. РИСК влияет на цели в определенной мере, но может быть допущен, если будет уравновешен пользой ОО должна предварительно утвердить политику для РИСКОВ данного уровня в плане МЕНЕДЖМЕНТА РИСКА. Политика может включать в себя проверки особой командой (ИТ, клинических специалистов) участие контролирующих органов, логическое обоснование, утверждение документа ВЫСШИМ РУКОВОДСТВОМ, демонстрацию того что РИСК был сокращен настолько, насколько это практически возможно, и т д
Низкий	РИСК допустим РИСК незначительно влияет на цели дополнительные меры по управлению не требуются

Примечание — В настоящем стандарте данная таблица относится ко всем трем ОСНОВНЫМ СВОЙСТВАМ.

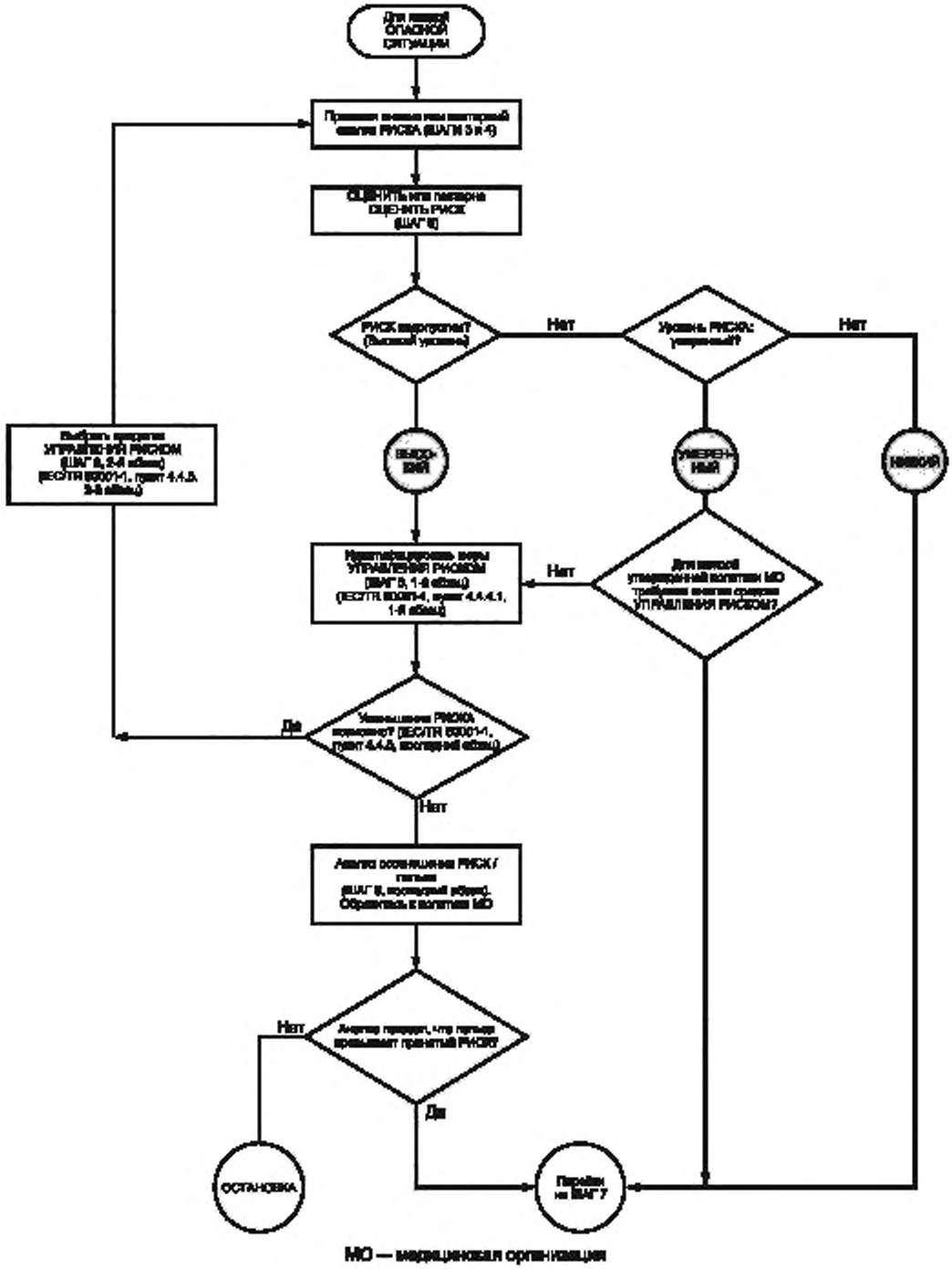


Рисунок D.1 — Применение ШАГОВ 5 и 6 с учетом трех уровней допустимости РИСКА

Приложение Е
(справочное)

КОНТРОЛЬ эффективности ослабления РИСКА

Е.1 Обзор

КОНТРОЛЬ представляет собой непрерывный обзор всей деятельности МЕНЕДЖМЕНТА РИСКА и возможностей УПРАВЛЕНИЯ РИСКОМ, установленных для достижения допустимого РИСКА использования (на стадии эксплуатации) МЕДИЦИНСКОЙ ИТ-СЕТИ(ЕЙ). Он предоставляет свидетельство того, что совокупный РИСК для ОСНОВНЫХ СВОЙСТВ МЕДИЦИНСКОЙ ИТ-СЕТИ является допустимым. Результат действий КОНТРОЛЯ может привести к:

- восстановлению ухудшенных рабочих характеристик ОСНОВНЫХ СВОЙСТВ (сигнал для УПРАВЛЕНИЯ СОБЫТИЯМИ);
- улучшению мер УПРАВЛЕНИЯ РИСКОМ (запрос на изменение);
- внесению изменений в ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА, критерии допустимости или политику.

Надлежащий КОНТРОЛЬ требует анализ:

- эффективности установленных мер по УПРАВЛЕНИЮ РИСКОМ (см. Е.2);
- эффективности проектирования и выполнения ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА (см. Е.3).

Е.2 Верификация эффективности мер по УПРАВЛЕНИЮ РИСКОМ

КОНТРОЛЬ затрагивает три возможности УПРАВЛЕНИЯ РИСКОМ (см. МЭК 80001-1:2010, пункт 4.4.2.4.1 «Анализ возможностей УПРАВЛЕНИЯ РИСКОМ»). Они представлены (в порядке предпочтения) ниже:

a) управление основным свойством, предусмотренное при проектировании (например, фильтрация пакетов на границе сети);

b) защитные меры (например, добавление сигнализации);

c) информация для обеспечения ОСНОВНЫХ СВОЙСТВ (например, предупреждения, документация пользователя, обучение).

Е.3 Верификация эффективности управления основным свойством, предусмотренного при проектировании

КОНТРОЛЬ мер по УПРАВЛЕНИЮ РИСКОМ, основанный на КОНТРОЛЕ, заложенном в проекте МЕДИЦИНСКОЙ ИТ-СЕТИ, требует поиска любых еще не обнаруженных РИСКОВ в компонентах или в конфигурации МЕДИЦИНСКОЙ ИТ-СЕТИ, чем напоминает послепродажный контроль.

a) ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ (ОО) воспринимает МЕДИЦИНСКИЕ ПРИБОР(Ы) и компоненты ИТ-СЕТИ как черные ящики.

i) В соответствии с регламентом юрисдикции ПРОИЗВОДИТЕЛИ МЕДИЦИНСКИХ ПРИБОРОВ могут осуществлять послепродажный контроль (PMS), обнаруживая любую проблему, связанную с проектированием, изготовлением или конфигурацией, и информировать ОТВЕТСТВЕННУЮ ОРГАНИЗАЦИЮ о требующихся или предлагаемых действиях по решению данной проблемы (например, отзыв или уведомление безопасности).

ii) ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна соответствующим образом реагировать на любое уведомление от ПРОИЗВОДИТЕЛЯ.

iii) ОТВЕТСТВЕННАЯ ОРГАНИЗАЦИЯ должна информировать ПРОИЗВОДИТЕЛЯ о любых проблемах с их МЕДИЦИНСКИМ ПРИБОРОМ, или компонентом ИТ-СЕТИ, или конфигурацией, связанной с приборами, компонентами или конфигурацией, для того чтобы ПРОИЗВОДИТЕЛЬ мог осуществлять послепродажный контроль.

Примечание — Процедуры устанавливаются как часть ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА, и они лучше интегрируются с УПРАВЛЕНИЕМ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕМ СОБЫТИЯМИ.

b) Элементы конфигурации. КОНТРОЛЬ эффективности мер по УПРАВЛЕНИЮ РИСКОМ, который основан на конфигурации, может быть достигнут за счет:

i) контроля (критических) элементов конфигурации или контроля рабочей характеристики системы, которая основана на этих элементах конфигурации МЕДИЦИНСКОЙ ИТ-СЕТИ. Как правило, такой контроль осуществляется, используя сетевые средства, например, контроль QoS, обнаружение проникновения. Единичное уведомление, поступившее от данных средств, является событием и должно быть перенаправлено в УПРАВЛЕНИЕ СОБЫТИЯМИ;

ii) анализа жалоб или проблем пользователя, которые обрабатывались процедурой УПРАВЛЕНИЯ СОБЫТИЯМИ. Это может указать на ухудшение ОСНОВНЫХ СВОЙСТВ и/или неправильное использование процедур пользователя МЕДИЦИНСКОЙ ИТ-СЕТИ;

iii) периодического анализа событий для обнаружения тенденций или других признаков, указывающих на складывающийся РИСК для ОСНОВНЫХ СВОЙСТВ. Типичными признаками этого являются:

1) увеличение или уменьшение частоты возникновения событий;

2) возникновение событий, связанных с другими событиями или изменениями.

Частота периодического анализа должна быть установлена как параметр ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА.

Данные процедуры устанавливаются как часть ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА, и их лучше всего использовать вместе с УПРАВЛЕНИЕМ ИЗМЕНЕНИЯМИ И ВЕРСИЯМИ и УПРАВЛЕНИЕМ СОБЫТИЯМИ.

Е.4 Верификация эффективности мер защиты

КОНТРОЛЬ эффективности мер защиты, таких как сигналы тревоги, как правило, требует:

a) КОНТРОЛЯ (технической) эксплуатации мер защиты посредством:

i) КОНТРОЛЯ надлежащего выполнения мер по УПРАВЛЕНИЮ РИСКОМ [например, отправки сигнала об отказе в соединении, если это соединение является (частью) меры по УПРАВЛЕНИЮ РИСКОМ]. Предполагаемый результат и требующееся действие, следующее за сигналом, должны быть утверждены как часть ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА (при ОЦЕНКЕ РИСКА);

ii) испытания функции сигнала тревоги (например, при запуске перед использованием или при еженедельном испытании). Частота выполнения таких испытаний должна быть утверждена как часть ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА (в ОЦЕНКЕ РИСКА);

b) КОНТРОЛЯ эффективного использования мер защиты;

c) учета влияния человеческого фактора пользователей систем, которые предупреждают и сигнализируют о необходимости действия. Например, неподходящий интерфейс пользователя, нецелесообразные инструкции или окружение пользователя могут негативно сказаться на эффективности мер по УПРАВЛЕНИЮ РИСКОМ.

Периодический анализ удобства использования и учета человеческих факторов мер защиты, как правило, достигается аудитом использования мер защиты. Частота выполнения данных испытаний должна быть утверждена как часть ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА (при ОЦЕНКЕ РИСКА). Как правило, инструменты аудита могут включать в себя анкетирование, интервью и наблюдения. В приложении В приведен список причин и вопросов, указывающих на (возможные) ошибки пользователя.

Е.5 Верификация эффективности информации об ОСНОВНЫХ СВОЙСТВАХ для ослабления РИСКА

Анализ эффективности информации для ослабления РИСКА требует контроля использования данной информации. См. Е.4, перечисление b).

Е.6 ВЕРИФИКАЦИЯ проектирования и выполнения ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА

Целью является верификация способности установленной политики и системы МЕНЕДЖМЕНТА РИСКА точно оценить и обеспечить в течение продолжительного времени ОСТАТОЧНЫЙ РИСК на допустимых уровнях.

КОНТРОЛЬ осуществляется проверкой соответствия с МЭК 80001-1 и периодическими аудитами выполнения ПРОЦЕССА МЕНЕДЖМЕНТА РИСКА.

a) Соответствие с МЭК 80001-1 проверяется в процессе анализа ФАЙЛА МЕНЕДЖМЕНТА РИСКА.

b) Частота проведения аудитов должна устанавливаться средствами ОЦЕНКИ РИСКА.

i) В процессе аудита проверяется:

1) соответствие ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА стандарту МЭК 80001-1 и местным требованиям;

2) соответствие выполняемых действий, входящих в МЕНЕДЖМЕНТ РИСКА, установленным ПРОЦЕССАМ и протоколам, описанным в ФАЙЛЕ МЕНЕДЖМЕНТА РИСКА.

Примечание — Типичные инструменты аудита включают в себя анкетирование, интервью и наблюдения.

Приложение F
(справочное)

АНАЛИЗ РИСКА для небольших изменений в МЕДИЦИНСКОЙ ИТ-СЕТИ

Рисунок F.1 демонстрирует, как может осуществляться ОЦЕНКА РИСКА для небольших изменений в МЕДИЦИНСКОЙ ИТ-СЕТИ.

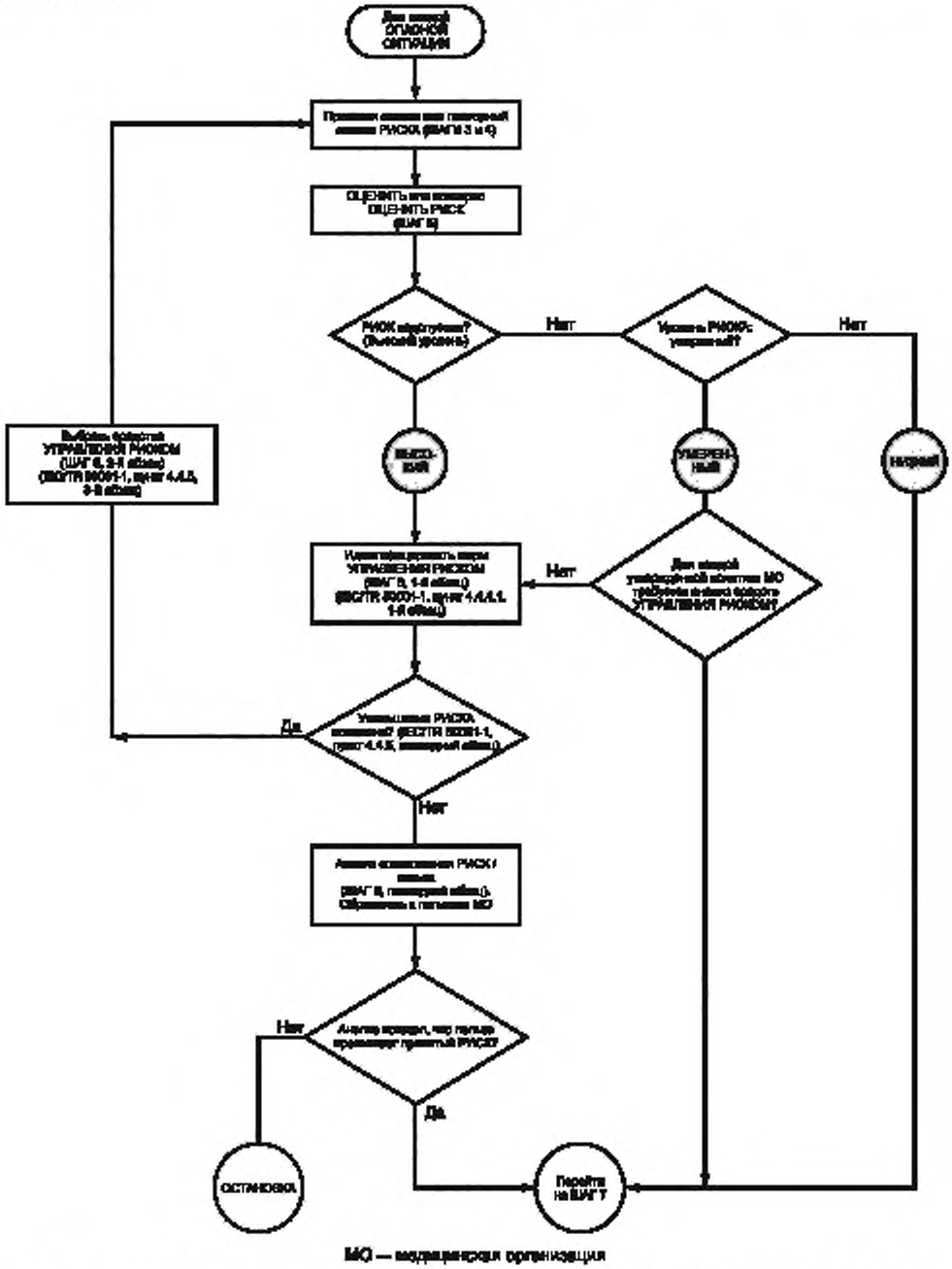


Рисунок F.1 — Обзор АНАЛИЗА РИСКА для небольших изменений в МЕДИЦИНСКОЙ ИТ-СЕТИ

Приложение G
(справочное)

Пример формы временного окна для изменения

Имя инициатора запроса:	Имя менеджера инициатора запроса:
Отделение / Группа:	Тип изменения. Аппаратное Программное
Затронутые Система(ы):	Затронутые Этажи/Здания
Затронутые Отделение(я).	Оказывает ли влияние на клиническую безопасность или безопасность пациента? Да ☐ Нет ☐
Приблизительное число затронутых пользователей:	Данное изменение прежде осуществлялось? Да ☐ Нет ☐
Одобрение затронутых пользователей получено? Да ☐ Нет ☐	Данное изменение прежде успешно проходило испытания? Да ☐ Нет ☐
Если изменение прежде испытывалось. Кем?	На каких системах?
Описание предложенного изменения / Обоснование	
Назначенные специалист(ы) по внедрению:	Контактные данные специалиста(ов) по внедрению:
Дата изменения (число месяц год):	Время изменения:
Запрашиваемое время остановки работы (в минутах) __5 __10 __15 __20 __25 __30 __40 __50 __60 __60+	
Вендор(ы)/Имя:	Контактные данные вендора(ов):
Местонахождение подробного плана реализации	
Шаги плана реализации	
Подготовительные шаги Шаги выполнения Шаги после выполнения Верификация	
Запрашиваемое время возврата (в минутах): __5 __10 __15 __20 __25 __30 __40 __50 __60 __60+	
Менеджер возврата:	Время принятия решения о возврате (часы:минуты):
Местонахождение подробного плана возврата. (План возврата — это те шаги, которые необходимо выполнить в случае, если обновление или изменение сети не удалось осуществить. Данные шаги «возвратят» изменения и вернут сеть или систему в состояние, в котором она находилась до изменений)	
Шаги плана возврата	
Подготовительные шаги Шаги выполнения Шаги после выполнения Верификация	
Контроль окна времени для верификации (Мин/Часы):	
Контактные данные выполняющего верификацию:	Контактный номер телефона выполняющего верификацию.

Приложение Н
(справочное)

Шаблон для примеров

Полное описание контекста
Описание анализируемой сети
10 Шагов

ШАГ 1. Идентификация ОПАСНОСТЕЙ

[при необходимости добавить детали/пояснения]

HAZ01.

HAZ02.

ШАГ 2. Идентификация причин и возникающих ОПАСНЫХ СИТУАЦИЙ

[при необходимости добавить детали/пояснения]

C01.

C02.

Идентифицированы следующие ОПАСНЫЕ СИТУАЦИИ:

HS01. (по причине Cn).

HS02. (по причине Cn).

HS03. (по причине Cn).

ШАГ 3. Определение НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ и оценка их возможной тяжести

Следует учесть, что оценка тяжести основывается на знании уровня тяжести состояния типичного ПАЦИЕНТА в данном контексте.

НП для HS01. Степень тяжести *ло*[1)].

НП для HS02. Степень тяжести *ло*.

НП для HS03. Степень тяжести *ло*.

ШАГ 4. Оценка вероятности возникновения НЕПРЕДНАМЕРЕННЫХ ПОСЛЕДСТВИЙ

HS01. *По*

HS02. *По*

HS03. *По*

ШАГ 5. Оценка РИСКА с учетом заданных критериев допустимости РИСКА

Необходимо вычислить начальный уровень РИСКА, основанный на вероятности и тяжести, определенных на ШАГАХ 3 и 4.

HS01 (*по*/*по*). Уровень РИСКА. *По*.

HS02 (*по*/*по*). Уровень РИСКА. *По*.

HS03 (*по*/*по*). Уровень РИСКА. *По*.

ШАГ 6. Идентификация и документальное оформление предложенных мер по УПРАВЛЕНИЮ РИСКОМ и оценка индивидуального РИСКА

RC01.

RC02.

[Необходимо пояснить, если вероятности или степень тяжести или и то и другое были уменьшены с помощью мер по управлению]

HS01. *По*.

HS02. *По*.

HS03. *По*.

ШАГ 7. Реализация мер по УПРАВЛЕНИЮ РИСКОМ

Меры по УПРАВЛЕНИЮ РИСКОМ должны быть реализованы для того, чтобы они могли быть ВЕРИФИЦИРОВАНЫ до запуска в эксплуатацию. [Необходимо пояснить, как данные меры могут быть реализованы]

ШАГ 8. Верификация мер по УПРАВЛЕНИЮ РИСКОМ

ВЕРИФИКАЦИЯ RC01.

Эффективность.

Реализация.

ВЕРИФИКАЦИЯ RC02.

Эффективность.

Реализация.

[1)] Аббревиатура *ло* в данном приложении означает «подлежит последующему определению».

ШАГ 9. Оценка любых РИСКОВ, возникающих в связи с УПРАВЛЕНИЕМ РИСКОМ

По заключениям оценки не было обнаружено никаких новых РИСКОВ, привнесенных добавленными мерами по УПРАВЛЕНИЮ РИСКОМ.

ШАГ 10. Оценка совокупного ОСТАТОЧНОГО РИСКА и формирование отчета о нем

Так как данные примеры представляют только один или два подпроцесса для ПРОЦЕССА заданной МЕДИЦИНСКОЙ ИТ-СЕТИ, концепцию совокупного ОСТАТОЧНОГО РИСКА сложно продемонстрировать. В целях настоящего стандарта следует принять, что совокупный ОСТАТОЧНЫЙ РИСК был определен как допустимый в соответствии с политикой ОО.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 80001-1:2010	IDT	ГОСТ Р МЭК 80001-1—2015 «Информатизация здоровья. Менеджмент рисков в информационно-вычислительных сетях с медицинскими приборами. Часть 1. Роли, ответственности и действия»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичный стандарт.		

Библиография

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

[2] IEC 60601-1-2:2007 Medical electrical equipment — Part 1-2: General requirements for basic safety and essential performance — Collateral standard. Electromagnetic compatibility — Requirements and tests

[3] IEC 80001-2-2:2012 Application of risk management for IT-networks incorporating medical devices — Part 2-2: Guidance for the communication of medical device security needs, risks and controls

[4] IEC 80001-2-3:2012 Application of risk management for IT-networks incorporating medical devices — Part 2-3: Guidance for wireless networks

[5] ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements

[6] ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management

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

[8] ISO 19218-2 Medical devices — Hierarchical coding structure for adverse events — Part 2: Evaluation codes

[9] ISO 27799:2008 Health informatics — Information security management in health using ISO/IEC 27002

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

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

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.М. Поляченко*
Компьютерная верстка *Д.В. Кардановской*

Сдано в набор 22.01.2019. Подписано в печать 30.01.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 6,20.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11
gost.e-ecolog.ru @mail.ru

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

gost.e-ecolog.ru