ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56837— 2015/ ISO/TR 11633-1: 2009

Информатизация здоровья

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УДАЛЕННОГО ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ МЕДИЦИНСКИХ ПРИБОРОВ И МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Часть 1

Требования и анализ рисков

ISO/TR 11633-1:2009
Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 1: Requirements and risk analysis
(IDT)

Издание официальное

Москва
Стандартинформ
2016

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Центральный научно-исследовательский институт организации и информатизации здравоохранения Министерства здравоохранения Российской Федерации» (ЦНИИОИЗ Минздрава) и Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации «Фирма «ИНТЕРСТАНДАРТ» на основе собственного аутентичного перевода на русский язык международного 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. № 2225-ст

4 Настоящий стандарт идентичен международному документу ISO/TR 11633-1:2009 «Информатизация здоровья. Менеджмент информационной безопасности удаленного технического обслуживания медицинских приборов и медицинских информационных систем. Часть 1. Требования и анализ рисков» (ISO/TR 11633-1:2009 «Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 1: Requirements and risk analysis», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного документа для приведения в соответствие с ГОСТ Р 1.5–2004 (пункт 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0–2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Стандартинформ, 2016

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

Содержание

1 Область применения 1
2 Термины и определения 1
3 Сокращения 2
4 Описание защиты служб удаленного технического обслуживания 3
4.1 Содержание защиты служб удаленного технического обслуживания 3
4.2 Требования к защите служб удаленного технического обслуживания 4
4.3 Роли центра удаленного технического обслуживания и медицинской организации 5
5 Варианты использования служб удаленного технического обслуживания 6
5.1 Введение 6
5.2 Устранение неисправностей при перебоях в работе 6
5.3 Регулярное техническое обслуживание 8
5.4 Обновление программного обеспечения 8
6 Анализ рисков 9
6.1 Общие положения 9
6.2 Критерии анализа риска 9
Приложение А (справочное) Пример результата анализа риска служб удаленного технического обслуживания 11
Библиография 16

Введение

Прогресс и распространение современных технологий в информационной и коммуникационной сферах, а также хорошо организованная структура, основанная на этих технологиях, внесли большие изменения в современное общество. В здравоохранении ранее закрытые информационные системы в каждом учреждении здравоохранения теперь объединены сетями, и на сегодняшний день технологии позволяют обеспечить взаимное использование медицинской информации, собранной в каждой информационной системе. Обмен подобной информацией по коммуникационным сетям реализуется не только между учреждениями здравоохранения, но и между учреждениями здравоохранения и поставщиками медицинского оборудования или медицинских информационных систем. Благодаря так называемым «сервисам удаленного технического обслуживания» (СУО) становится возможным снизить временные потери и расходы.

Однако оказалось, что такая связь учреждений здравоохранения с внешними организациями обладает не только преимуществами, но также несет в себе риск, связанный с конфиденциальностью, целостностью и доступностью информации и систем, то есть риски, которые раньше даже не учитывались.

На основе информации, предлагаемой в настоящем стандарте, учреждения здравоохранения и провайдеры СУО смогут обеспечить следующее:

- уточнить риски, возникающие при использовании СУО, если внешние условия участка запрашивающего поставщика (ЦУО) и места медицинского учреждения, которому предоставляется техническое обслуживание (HCF), могут быть выбраны из каталога, приведенного в приложении А;
- понять основы выбора и применения технических и нетехнических «средств управления», которые применяют в их учреждении для предотвращения рисков, описанных в настоящем стандарте;
- направить запрос от бизнес-партнеров на предмет принятия конкретных мер противодействия, так как настоящий документ может идентифицировать соответствующие риски для защиты;
- уточнить границы ответственности между владельцем медицинского учреждения и провайдером СУО;
- планировать программу по сохранению или передаче риска, т. к. остаточные риски уточняются при выборе соответствующих «средств управления».

Применяя оценки риска и используя «средства управления» в соответствии с настоящим стандартом, владельцы медицинского учреждения и провайдеры СУО смогут воспользоваться следующими преимуществами:

- будет достаточно выполнить оценку риска для тех организационных сфер, где настоящий стандарт не применим, а, следовательно, усилия по оценке риска могут быть значительно снижены;
- будет легко продемонстрировать третьей стороне то, что меры СУО по пресечению нарушения защиты прошли подтверждение на соответствие;
- при предоставлении СУО на двух или более участках провайдер может последовательно и эффективно применять меры противодействия.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УДАЛЕННОГО ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ МЕДИЦИНСКИХ ПРИБОРОВ И МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Часть 1

Требования и анализ рисков

Health informatics. Information security management for remote maintenance of medical devices and medical information systems. Part 1. Requirements and risk analysis

Дата введения — 2016—11—01

1 Область применения

Предметом настоящего стандарта являются услуги удаленного технического обслуживания (СУО), предоставляемые поставщиками медицинского оборудования или информационными медицинскими системами (провайдерами СУО) для информационных систем в медицинских учреждениях. Кроме этого в данном стандарте предоставлен пример выполнения анализа риска, необходимого для защиты информационных активов обеих сторон (в первую очередь, самой информационной системы и персональных медицинских данных), безопасным и эффективным (в экономическом смысле) способом.

Настоящий стандарт включает в себя:

- каталог сценариев использования для СУО;
- каталог информационных активов в медицинских учреждениях и провайдеров СУО;
- пример анализа риска, основанный на вариантах использования

2 Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями:

2.1 **подотчетность** (accountability): Свойство, обеспечивающее однозначное прослеживание действий любого логического объекта.

[ИСО/МЭК 13335-1:2004, определение 2.1]

2.2 **актив** (asset): Все, что представляет ценность для организации.

Примечания

1 Термин заимствован из ИСО/МЭК 13335-1.

2 В контексте защиты медицинской информации информационные активы включают:

a) медицинскую информацию;
b) IT-сервисы;
c) аппаратные средства;
d) программное обеспечение;
e) коммуникационные средства;
f) средства информации;
g) IT-средства;
h) медицинские приборы, которые записывают данные или формируют отчеты данных.

2.3 **доверие** (assurance): Результат серии процессов установления соответствия, посредством которых организация достигает уверенности в статусе менеджмента защиты информации.

Издание официальное

2.4 **доступность** (availability): Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

[ИСО/МЭК 13335-1:2004, определение 2.4]

2.5 **оценка соответствия** (compliance assessment): Процессы, которыми организация подтверждает, что средства управления защитой информации остаются работоспособными и эффективными.

Примечание — Соответствие закону, в частности, относится к средствам управления защитой, установленным для соблюдения требований соответствующего законодательства, например, директивы Европейского союза по защите персональных данных.

2.6 **конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованных лиц, логического объекта или процесса.

[ИСО/МЭК 13335-1:2004, определение 2.6]

2.7 **целостность данных** (data integrity): Свойство, гарантирующее, что данные не будут изменены или уничтожены неправомочным образом.

[ИСО/МЭК 9797-1:1999, определение 3.1.1]

2.8 **управление информацией** (information governance): Процессы, благодаря которым организация получает уверенность в том, что риски, связанные с ее информацией, а значит, работоспособность и целостность организации эффективно выявляются и контролируются.

2.9 **информационная безопасность** (information security): Поддержание конфиденциальности, целостности и доступности информации.

Примечание — Другие свойства, в частности подотчетность пользователей, а также аутентичность, отказоустойчивость и надежность, часто упоминаются как аспекты информационной безопасности, но также могут рассматриваться как производные от трех основных свойств в определении.

2.10 **риск** (risk): Сочетание вероятности события и его последствия.

[Руководство ИСО/МЭК 73:2002, определение 3.1.1].

2.11 **оценка рисков** (risk assessment): Общий процесс анализа и оценивания риска.

[Руководство ИСО/МЭК 73:2002, определение 3.3.1]

2.12 **менеджмент рисков** (risk management): Скоординированные действия, направляющие и контролирующие организацию работ, связанных с риском.

Примечание — Менеджмент риска обычно включает в себя оценку риска, обработку риска, степень допустимого риска и информирование о рисках.

[Руководство ИСО/МЭК 73:2002, определение 3.1.7]

2.13 **обработка рисков** (risk treatment): Процесс выбора и применения мер для изменения (обычно для снижения) риска.

Примечание — Адаптировано из Руководства ИСО/МЭК 73:2002.

2.14 **целостность системы** (system integrity): Свойство системы выполнять предусмотренную для нее функцию в нормальном режиме, свободном от преднамеренного или случайного несанкционированного воздействия на систему.

2.15 **угроза** (threat): Потенциальная причина нежелательного инцидента, который может нанести ущерб системе или организации.

Примечание — Адаптировано из ИСО/МЭК 13335-1.

2.16 **уязвимость** (vulnerability): Слабость одного или нескольких активов, которая может быть использована угрозой.

Примечание — Адаптировано из ИСО/МЭК 13335-1.

3 Сокращения

МУ — медицинское учреждение (HCF — Healthcare facility);

ПХИ — программа хищения информации (ISP — Information-stealing programme);

ПМИ — персональная медицинская информация (PHI — Personal health information);

СУО — службы удаленного технического обслуживания (RMS — Remote maintenance services);

ЦУО — центр удаленного технического обслуживания (RSC — Remote maintenance service centre);
ЗУО — защита удаленного обслуживания (RSS — Remote maintenance service security);
VPN — виртуальная частная сеть (VPN — virtual private network).

4 Описание защиты служб удаленного технического обслуживания

4.1 Содержание защиты служб удаленного технического обслуживания

4.1.1 Общие положения

Службы удаленного обслуживания (СУО) предназначены для трех целей:
- обеспечение надлежащей реакции во время сбоя медицинского оборудования;
- регулярное техническое обслуживание;
- обновление программного обеспечения.

В настоящем стандарте рассматривается система, состоящая из целевых приборов и внутренней сети в медицинском учреждении, внешней сети, соединяющей медицинское учреждение и центр служб удаленного технического обслуживания (ЦУО), а также внутренней сети и оборудования или служб в самом ЦУО (см. рисунок 1).

В настоящем стандарте описываются типы и текущее состояние мер защиты.

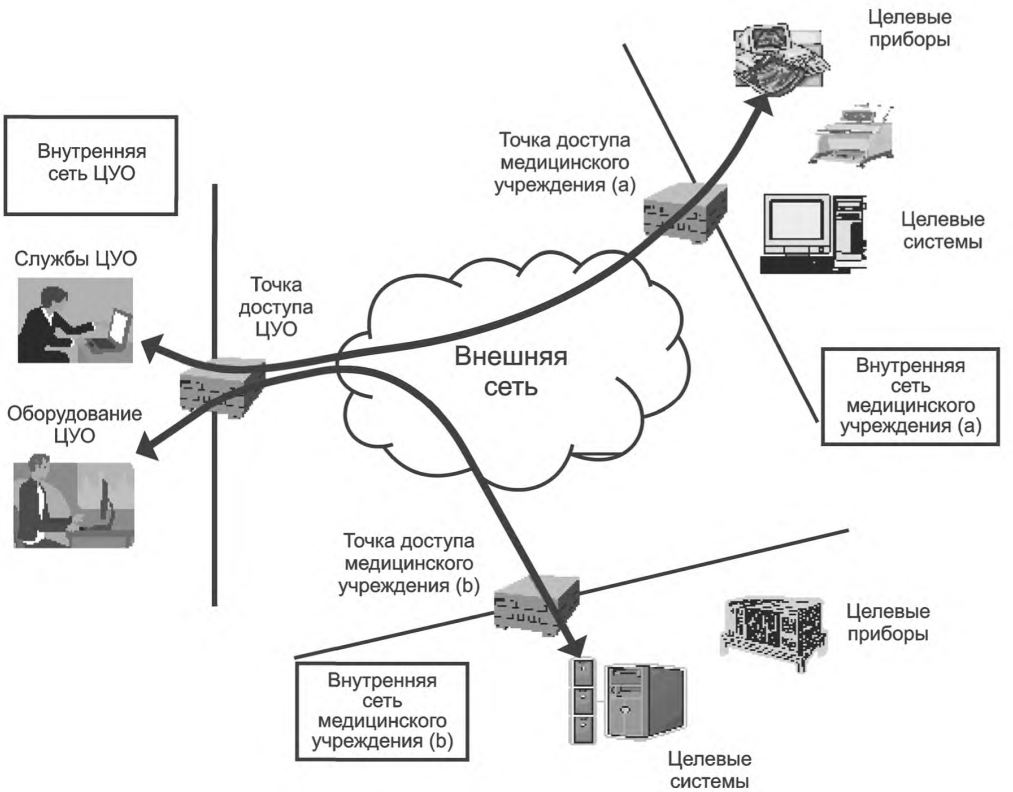


Рисунок 1 — Предполагаемые СУО

4.1.2 Виды служб удаленного технического обслуживания и меры технической защиты

4.1.2.1 СУО, использующие коммутируемую телефонную сеть общего доступа

В медицинском учреждении устанавливают устройство с функцией сервера коммутируемого доступа. Это устройство соединяется с коммутируемой телефонной сетью общего доступа при помощи модема и т. д., и ожидает получения доступа от удаленного оборудования ЦУО. Телекоммуникационное оборудование, обладающее функциями коммутируемых маршрутизаторов, находится в широком использовании.

При использовании коммутируемой телефонной сети общего доступа телекоммуникационные линии обладают следующими свойствами:

- маршрут прямой коммуникации между медицинским учреждением и ЦУО может быть защищен;
- перехватывание информации представляется затрудненным в связи с тем, что коммутируемая телефонная сеть общего доступа полностью работает в цифровом режиме.

Благодаря этим свойствам защита поддерживается посредством следующих технических мер:

a) определение номера вызывающего абонента — использование функции сертификата обратного звонка или функции сертификата идентификации звонящего;

b) сертификация пользователя — использование одноразового пароля и шифрования пароля;

c) обзор журнала аудита связи — определение нелегального доступа к компьютеру.

4.1.2.2 СУО, использующие Интернет

В медицинском учреждении располагается устройство подключения к Интернету с фиксированным глобальным IP-адресом. ЦУО готовит среду подключения к Интернету и сам подключается к медицинскому учреждению через Интернет.

Настоящий стандарт определяет больший набор технологий для коммуникации и проверки подлинности пользователя между медицинским учреждением и ЦУО, т. к. по сути это обычное Интернет соединение, а не прямое соединение через коммутируемую телефонную сеть общего доступа.

Настоящий стандарт демонстрирует следующие примеры:

- установка брандмауэра;
- применение таких инструментов, как антивирусное программное обеспечение;
- связь при помощи VPN для кодирования канала связи;
- использование множества методов проверки подлинности пользователей, таких как одноразовые пароли, кодировка паролей и использование цифровых сертификатов.

4.2 Требования к защите служб удаленного технического обслуживания

4.2.1 Меры обеспечения защиты при удаленном техническом обслуживании

Обычно для защищенной работы системы и для защиты конфиденциальности личной информации используются регламентирующие правила. Настоящий стандарт представляет следующие примеры регламентов:

a) регламент для оператора ЦУО;

b) регламентирующие меры, исключающие работу неавторизованных удаленных терминалов ЦУО;

c) регламент на увеличение числа удаленных терминалов ЦУО и их перемещение;

d) регламент о доступе с мобильных терминалов.

4.2.2 Контракты между медицинским учреждением и центром удаленного обслуживания

Следующие регламентирующие нормы могут применять в случае непредвиденных сбоев:

a) регламентирующие правила для разграничения ответственности между медицинским учреждением и ЦУО;

b) заключение контрактов о конфиденциальности информации.

Существует несколько средств для обеспечения мер защиты СУО. Каждый провайдер СУО поддерживает защиту, используя эти средства в соответствии с первоначальными регламентирующими нормами.

Однако настоящий стандарт предусматривает, что в будущем для медицинских учреждений расходы на защиту увеличатся, а поддержание уровня защиты станет более сложным, т. к. используемые методы будут изменяться в зависимости от провайдера СУО.

4.2.3 Защита персональной информации и службы удаленного технического обслуживания

4.2.3.1 Защита конфиденциальности медицинской информации в медицинских организациях

В соответствии с законодательными актами о защите конфиденциальности управление конфиденциальностью персональной информации переходит от врачей к установлению права управления информацией и защитой ее конфиденциальности самими пациентами.

Медицинские организации обязаны управлять персональной информацией, разъяснять пациенту риски, которым подвергается конфиденциальность персональной информации, а также гарантировать, что медицинские работники не используют информацию о здоровье в целях, выходящих за пределы тех целей, ради которых она была собрана.

В связи с тем что медицинская информация является особо важным типом персональной информации, с ней следует обращаться бережно и осторожно.

4.2.3.2 Ответственность и меры защиты персональной информации

Законы США об установлении правил обмена личной медицинской информацией и ее защите от неразрешенного использования (HIPAA) требуют, чтобы медицинские организации назначали лицо, ответственное за менеджмент информации в системе, и определяют ответственность медицинской организации за утечку персональной информации за ее пределы независимо от причин утечки.

В Японии руководство по защите персональной информации в сфере здравоохранения устанавливает ответственность медицинских организаций за защиту персональной информации и требует от ответственного лица по защите персональных данных в организации здравоохранения выполнения его обязанности. Таким образом, медицинские организации обязаны самостоятельно заниматься менеджментом информации в системе.

Однако настоящий стандарт рассматривает случаи, когда медицинские организации полностью передают менеджмент систем медицинской информации поставщикам СУО для медицинских приборов и провайдерам систем медицинской информации. Ответственным лицам в медицинской организации может быть сложно надлежащим образом разрешать непростые проблемы, связанные с управлением информацией в медицинских организациях, если управление информацией было полностью передано поставщикам СУО.

Однако в случае инцидентов, ведущих к утечке информации и т. д., может возникнуть проблема, связанная с тем, кто должен нести ответственность — поставщик СУО или поставщик медицинских услуг. Для разрешения таких ситуаций настоящий стандарт указывает на то, что предпочтительнее пересмотреть систему менеджмента информации медицинской организации, чтобы убедиться в ее соответствии любым подведомственным актам по защите конфиденциальности персональной информации.

4.2.3.3 СУО и защита конфиденциальности медицинской информации

Для защиты персональной информации надлежащим образом медицинские организации должны обеспечить меры защиты, соответствующие ответственности медицинской организации, как описано в предыдущем подпункте.

В настоящее время медицинские организации в основном предоставляют правила управления медицинского центра, устанавливают меры надлежащего управления и реализуют меры защиты информационных систем и технические средства защиты персональной информации.

В частности, в качестве мер обеспечения защиты сети, многие медицинские организации реализуют такие меры, как «соединение с внешней сетью не разрешено», «использовать VPN» и т. д., а также защиту против внешних хакерских атак из Интернета. Однако, даже если контрмеры медицинской организации против внешнего вмешательства представляются идеальными, СУО являются единственным каналом, который позволяет доступ извне.

Доступ сотрудника, обслуживающего поставщика СУО, в систему через СУО принимается как необходимая служба для быстрого восстановления функции.

СУО имеет преимущества как перед медицинскими организациями, так и перед поставщиками СУО, и поэтому является необходимой службой, даже когда документы по защите конфиденциальности медицинской информации уже были приняты и опубликованы.

Для применения защиты и ответственности при использовании СУО медицинские организации должны хорошо понимать СУО, заключить соответствующий контракт и применить технические меры обеспечения защиты и оперативные меры. Важно четко разграничить ответственность между медицинской организацией и поставщиками СУО, построить прошедший необходимую оценку механизм безопасности, чтобы обеспечить соответствие подобных разграничений защите конфиденциальности медицинской информации. Как медицинская организация, так и поставщики СУО должны четко понимать свои обязательства и выбирать соответствующие СУО по взаимному соглашению.

4.3 Роли центра удаленного технического обслуживания и медицинской организации

Если медицинское учреждение по контракту обслуживания с поставщиками СУО доверило поставщику СУО обеспечение для ее защиты, то меры защиты применяются в соответствии с процедурами и ответственностью каждого поставщика СУО.

Возникают следующие проблемы:

- не существует положений о том, что третья сторона может удостовериться в том, что поставщик СУО предоставляет достаточные меры обеспечения защиты;
- медицинское учреждение не рассматривало меры управления как технологические меры, использующиеся вместе с мерами обеспечения защиты;
- медицинское учреждение недостаточно изучило последовательность событий после инцидента;

- медицинское учреждение не изучило широко распространенные угрозы, такие как компьютерные вирусы.

Документы по защите конфиденциальности требуют от медицинского учреждения взять на себя ответственность за защиту индивидуальной медицинской информации. Медицинское учреждение также должно взять на себя ответственность за обеспечение защиты служб удаленного обслуживания. Следовательно, настоящий стандарт объясняет функции медицинского учреждения и поставщиков СУО. Реализация защиты в СУО является функцией поставщиков служб удаленного обслуживания, так как только поставщик СУО может реализовать функцию службы удаленного обслуживания для медицинской информационной системы. Поставщики СУО должны учитывать, что применение различных технологий защиты препятствует распространению служб удаленного обслуживания.

При подготовке точек доступа для каждой СУО поставщики могут усложнить управление защитой. Такое усложненное управление способствует нарушениям системы защиты. Следовательно, каждый поставщик СУО должен адаптировать и реализовать стандартизированную и широко используемую технологию обеспечения защиты.

Меры, используемые для менеджмента защиты информации, так же важны, как и технологические меры. Они необходимы как для медицинского учреждения, так и для ЦУО. Оба этих учреждения должны документально отразить текущую систему менеджмента защиты информации, ориентируясь на международный стандарт, например ИСО/МЭК 27001, который поддерживает реализацию политики защиты. После этого они должны сравнить и сопоставить ее с политиками защиты; необходимо также уточнить минимальный стандарт защиты для СУО. Медицинское учреждение принимает решение и использует меры, основываясь на своей собственной политике защиты, и затем изучает и оценивает эту политику защиты, а также обстоятельства применения мер обеспечения защиты в СУО, указанных поставщиками СУО. После этого медицинское учреждение приходит к соглашению с поставщиками СУО о соответствии их работы и обеспечении конфиденциальности. В результате защита СУО гарантирована.

5 Варианты использования служб удаленного технического обслуживания

5.1 Введение

Настоящий стандарт выделяет три типичных варианта использования СУО, рассматриваемых в качестве модели для своей работы.

a) Устранение неисправностей при перебоях в работе

В случае перебоев в работе оборудования в медицинском учреждении и в ходе ответа на запрос из медицинского учреждения, производятся операции по техническому обслуживанию, осуществляемые с помощью доступа к целевым приборам из центра удаленного обслуживания.

b) Регулярное техническое обслуживание

Операции по регулярному обслуживанию выполняются из ЦУО после получения разрешения из медицинского учреждения. Это может привести к периодическому доступу к целевым приборам в медицинском учреждении.

c) Обновление программного обеспечения

Выполняется обновление программного обеспечения целевых приборов в медицинском учреждении при получений доступа к ним из ЦУО.

5.2 Устранение неисправностей при перебоях в работе

Порядок работы в случае устранения неисправностей при перебоях продемонстрирован на рисунке 2.

Данный порядок работы включает следующие шаги:

a) медицинское учреждение уведомляет ЦУО о возникновении проблемы (может быть в форме автоматического уведомления по электронной почте)»;

b) ЦУО запрашивает медицинское учреждение о подключении к сети для службы удаленного обслуживания;

c) ЦУО выполняет запуск подключения к сети;

d) технические специалисты центра удаленного обслуживания выполняют инспектирование, обработку и подтверждение через сетевое подключение:

1) используется программа автоматического инспектирования;
2) собирается соответствующая информация о целевом оборудовании:
   i) журнал регистрации работы,
   ii) данные в виде изображений,
   iii) конфигурационные файлы / информация о конфигурации системы,
   iv) содержание базы данных;
3) исследование проблемы;
4) если проблема возникла в программном обеспечении, то выполняется модификация или обновление целевого оборудования:
   i) модификация конфигурационных файлов,
   ii) обновление программного обеспечения,
   iii) восстановление данных;
5) если проблема связана с аппаратными средствами, то передается сообщение техническому персоналу о необходимости замены поврежденных компонентов;
6) выполняется инспектирования после ремонта;

e) ЦУО сообщает о результатах работы медицинскому учреждению;

f) ЦУО отключает соединение с сетью для служб удаленного технического обслуживания;

g) ЦУО запрашивает медицинское учреждение об отключении сетевого подключения СУО;

h) если ЦУО пересылал персональную медицинскую информацию, то центр удаленного обслуживания удаляет все копии персональной медицинской информации.

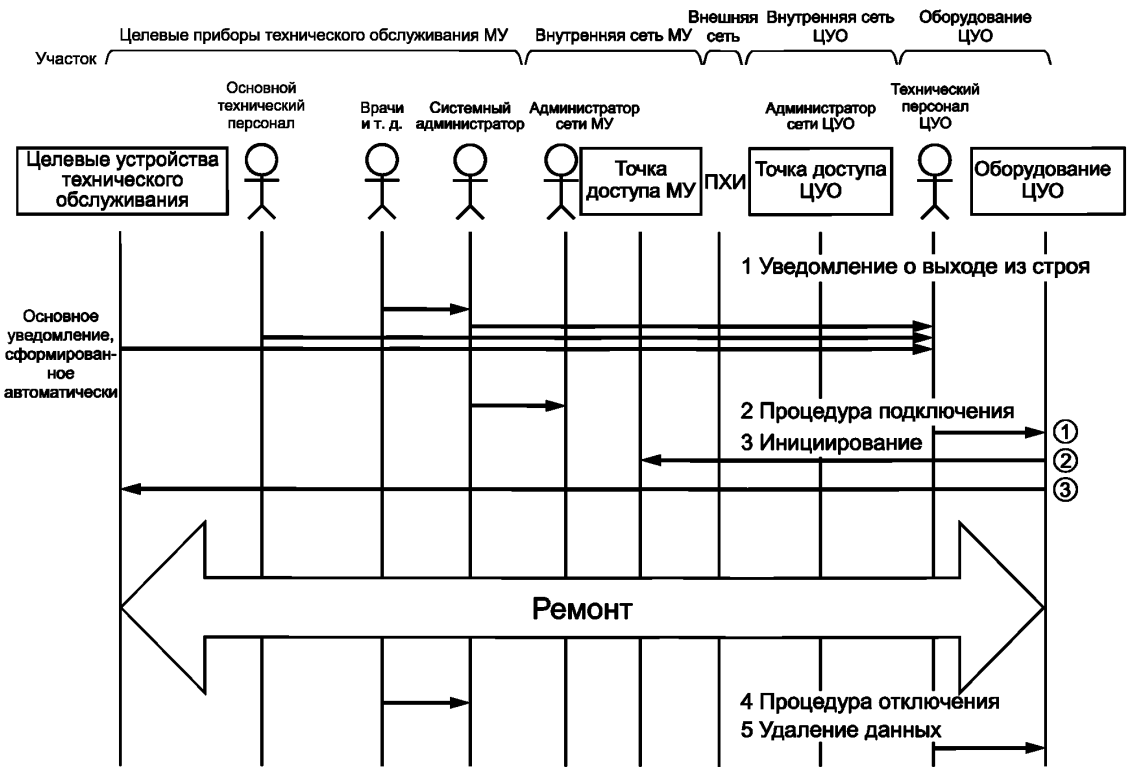


Рисунок 2 — Порядок работы в случае устранения неисправностей

5.3 Регулярное техническое обслуживание

Порядок работы в случае регулярного технического обслуживания продемонстрирован на рисунке 3.

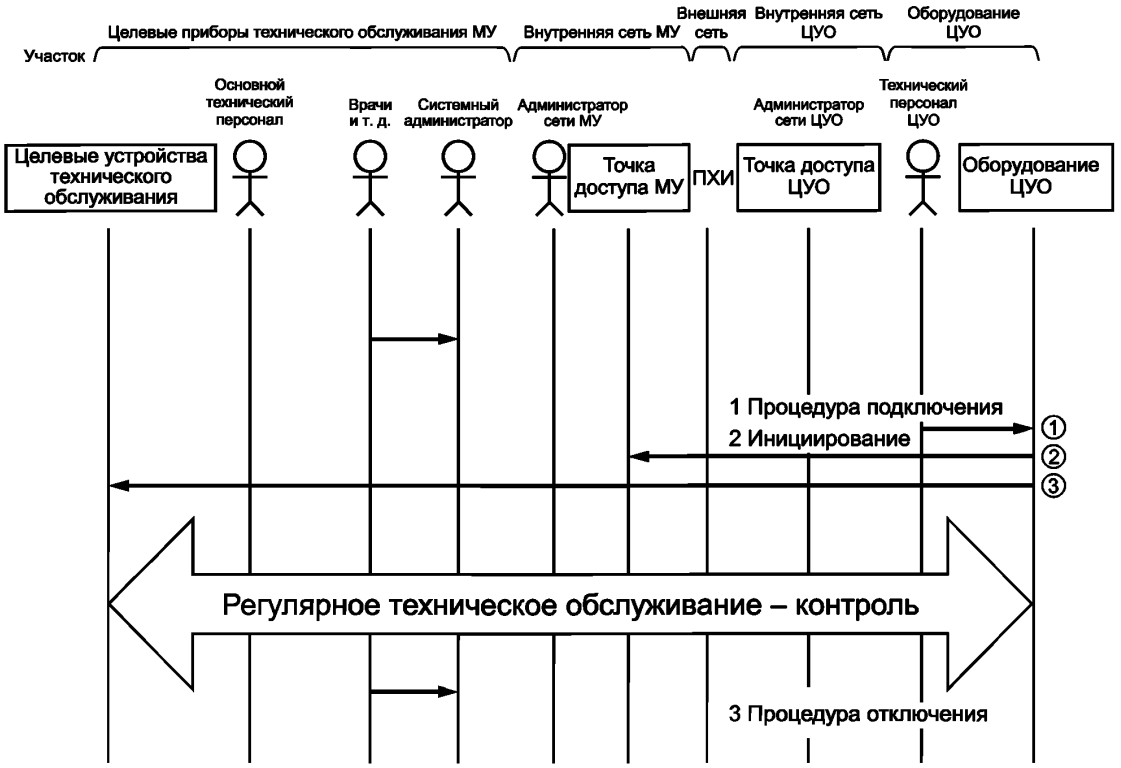


Рисунок 3 — Порядок работы в случае регулярного технического обслуживания

Данный порядок работы включает следующие шаги:

a) ЦУО запрашивает медицинское учреждение о подключении к сети для службы удаленного технического обслуживания;

b) ЦУО выполняет запуск подключения к сети;

c) технические специалисты ЦУО выполняют инспектирование через сетевое подключение:

1) используется программа автоматического инспектирования;
2) проверяются журналы;
3) проверяется качество изображения (точность);
4) собирается рабочая информация;

d) ЦУО сообщает о результатах работы медицинскому учреждению;

e) ЦУО отключает соединение с сетью для СУО;

f) ЦУО запрашивает медицинское учреждение об отключении соединения с сетью служб удаленного обслуживания;

g) если ЦУО пересылал персональную медицинскую информацию, то центр удаленного обслуживания удаляет все копии персональной медицинской информации.

5.4 Обновление программного обеспечения

Порядок работы в случае обновления программного обеспечения продемонстрирован на рисунке 4.



Рисунок 4 — Порядок работы в случае обновления программного обеспечения

Данный порядок работы включает следующие шаги:

a) ЦУО запрашивает медицинское учреждение о подключении к сети для СУО;

b) ЦУО выполняет запуск подключения к сети;

c) технический персонал ЦУО обновляет программное обеспечение через сетевое подключение:

1) выполняется замена программного обеспечения;

2) выполняется изменение конфигураций;

3) выполняется подтверждение выполняемой функции;

d) ЦУО сообщает о результатах работы медицинскому учреждению;

e) ЦУО отключает соединение с сетью служб удаленного технического обслуживания;

f) ЦУО запрашивает медицинское учреждение об отключении соединения с сетью служб удаленного технического обслуживания;

g) Если ЦУО переслал персональную медицинскую информацию, то ЦУО удаляет все копии персональной медицинской информации.

6 Анализ рисков

6.1 Общие положения

В настоящем разделе представлен анализ рисков для вариантов использования, рассмотренных в разделе 5.

6.2 Критерии анализа риска

6.2.1 Политика

Политика требует: назначенный медицинской организацией администратор информации должен постоянно анализировать защиту и риски в медицинской организации, применяя правила HIPAA (Закон

США об установлении правил обмена личной медицинской информацией и ее защите от неразрешенного использования). Это необходимо для прогнозирования риска и для обеспечения защиты при обмене информацией с внешними организациями.

Результаты такого анализа должны храниться в медицинском учреждении в качестве дополнительного документа или руководящих указаний к контракту с ЦУО. Руководство должно выполнять такой анализ для каждой дополнительной организации здравоохранения.

6.2.2 Классификация участка

Оборудование ЦУО.

Внутренняя сеть ЦУО.

Внешняя сеть.

Внутренняя сеть медицинского учреждения.

Целевые приборы медицинского учреждения.

6.2.3 Профиль защиты

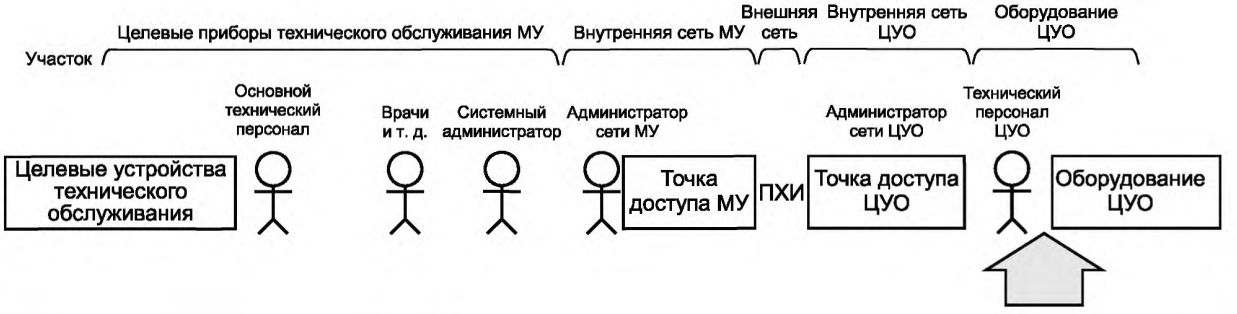
Профилю защиты для обеспечения:

- конфиденциальности необходима защита: от тактик взламывания/незаконного присвоения, неавторизованного входа/обмана и подбора пароля;
- целостности необходима защита: от фальсификации, подмены, подлога и от воспрепятствования отказа партнеров по связи;
- доступности необходима защита: от отказа оборудования, аварии, перебоя в обслуживании из-за прерывания подачи питания/отказа в обслуживании.

Приложение А
(справочное)

Пример результата анализа риска служб удаленного технического обслуживания

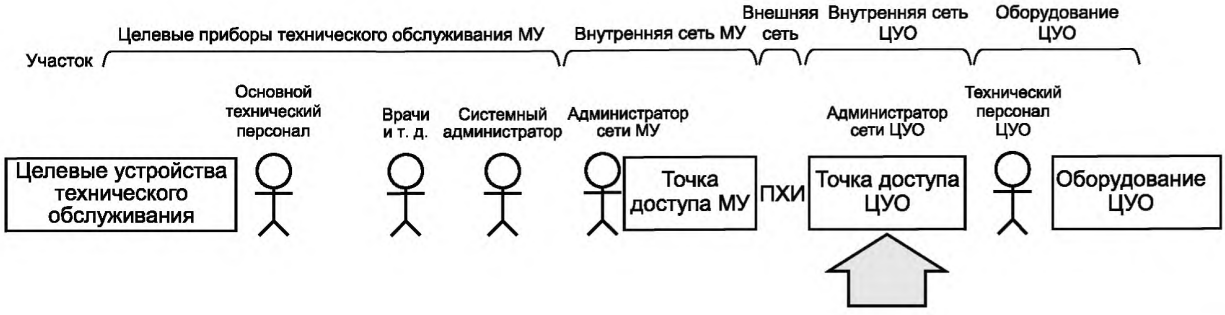
А.1 Активы и угрозы (оборудование центра удаленного обслуживания)



Активы	№	Угроза (К — конфиденциальность, Ц — целостность, Д — доступность)
Персональная медицинская информация (ПМИ) на карте памяти, диске и экране	11	Незащищенность данных [К] из-за ошибки удаления на участке [К], подсматривания [К]/кражи [К], неавторизованного доступа к оборудованию ЦУО [К] / обмана [К]
	12	Незащищенность данных [К] из-за кражи при передаче [К], неавторизованного доступа к оборудованию ЦУО [К] / обмана [К]
Записи и распечатки ПМИ	13	Незащищенность данных [К] из-за подсматривания в бумажные записи о ремонте [К], выноса [К]
Резервные носители ПМИ	14	Незащищенность данных [К] при выносе носителей информации на ремонт [К]
Программное обеспечение, обрабатывающее ПМИ	15	Незащищенность данных [К] из-за черного хода/установки программ, похищающих информацию [К]
Оборудование, обрабатывающее ПМИ	16	Незащищенность данных [К] из-за выноса [К], несанкционированного вмешательства [К], утечки электромагнитного излучения [К]
	17	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]
Оборудование, обрабатывающее ПМИ[a)]	18	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]
Операторы, обрабатывающие ПМИ	19	Незащищенность данных из-за подкупа [К], отказа службы [Д] из-за неверного ввода информации [Ц]/отказа при удалении [Д]
Алгоритм шифрования, ключи и метод распределения ключей	1а	Незащищенность данных [К] из-за расшифровки зашифрованных данных [К]

[a)] Указывает на средства аварийной защиты/силовое оборудование. Однако сетевое оборудование не включено.

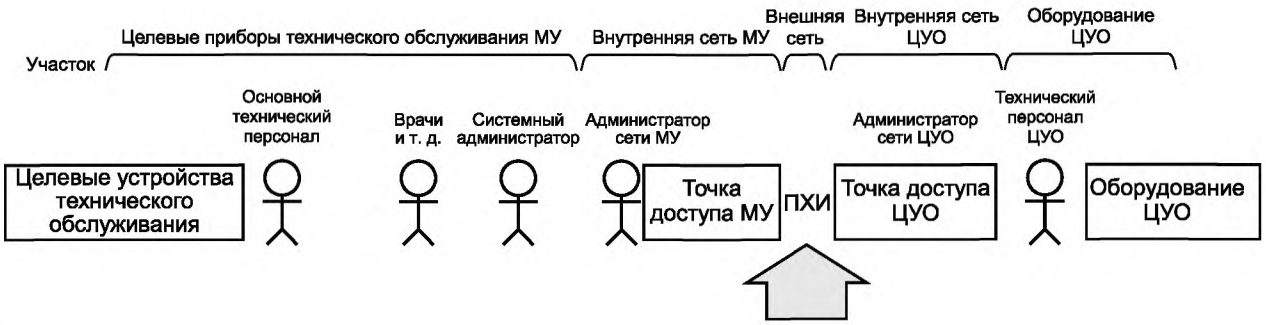
А.2 Активы и угрозы (внутренняя сеть ЦУО)



Активы	№	Угроза (К — конфиденциальность, Ц — целостность, Д — доступность)	
		без контрмер по VPN	с контрмерами по VPN
ПМИ во внутренней сети ЦУО	21	Незащищенность данных [К] из-за отслеживания пути [К], неавторизованного доступа к сетевому оборудованию ЦУО [К] / обмана [К], прослушивания [К]	Угрозы, не отмеченные знаком [Д], можно не учитывать
Записи и распечатки коммуникационного следа вышеуказанной информации	22	Незащищенность данных [К] из-за подсматривания в протокол контроля [К], выноса [К]	
Среда резервного копирования коммуникационного следа вышеуказанной информации	23	Незащищенность данных [К] из-за выноса монитора при копировании носителей информации [К]	
Программное обеспечение сетевого оборудования	24	Незащищенность данных [К] из-за черного хода/установки программ, похищающих информацию [Ц]	
Сетевое оборудование	25	Незащищенность данных [К] из-за выноса [К], несанкционированного вмешательства [К], влияния электромагнитного излучения [К]	
	26	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]	
Системы защиты окружающей среды сетевого оборудования[a)]	27	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д], разрыва кабеля [Д]	
Операторы сетевого оборудования	28	Незащищенность из-за подкупа [К], угрозы [К] неверной настройки [К]	
Алгоритм шифрования, ключи и метод распределения ключей	29	Незащищенность данных [К] из-за расшифровки зашифрованных данных [К]	

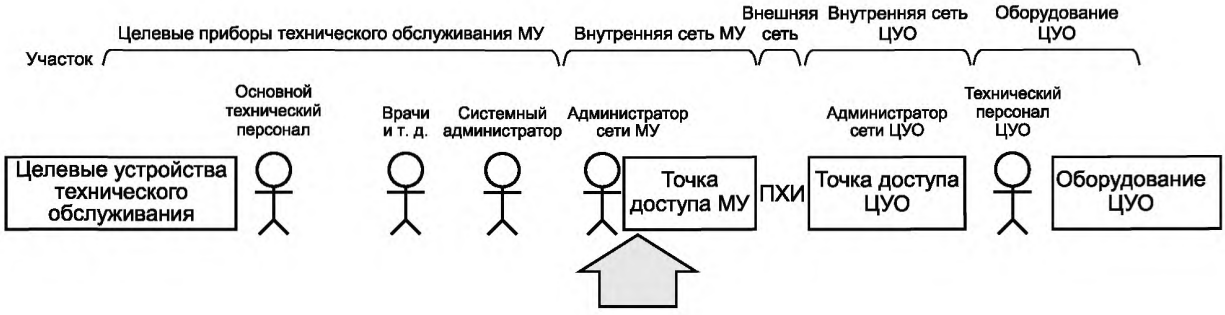
[a)] Обозначает источники питания/средства аварийной защиты.

А.3 Активы и угрозы (внешняя сеть)



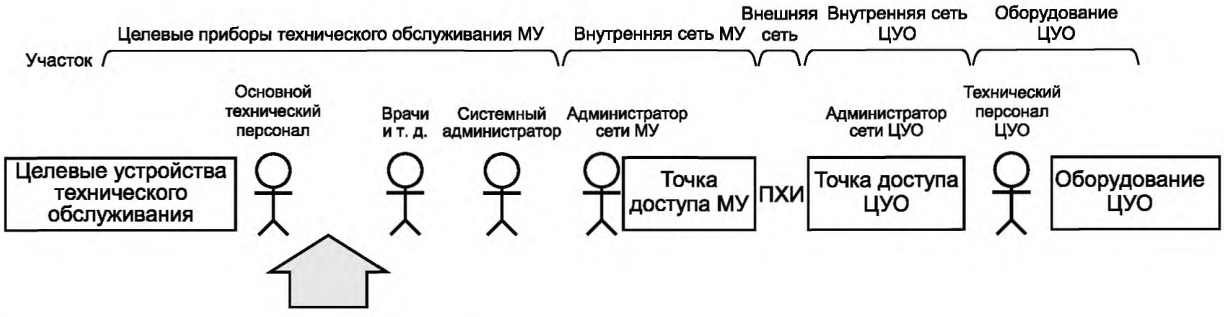
Активы	№	Угроза (К — конфиденциальность, Ц — целостность, Д — доступность) Предполагается наличие контрмер на VPN. Все угрозы, за исключением (Д) доступности, можно не принимать в расчет
ПМИ во внешней сети	31	Незначительная
Записи и распечатки коммуникационного следа вышеуказанной информации	32	Незначительная
Средства резервного копирования коммуникационного следа вышеуказанной информации	33	Незначительная
Программное обеспечение сетевого оборудования	34	Незначительная
Сетевое оборудование	35	Незначительная
	36	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]
Системы защиты окружающей среды сетевого оборудования[a)]	37	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д], разрыва кабеля [Д]
Операторы сетевого оборудования	38	Незначительная
Алгоритм шифрования, ключи и метод распределения ключей	39	Незащищенность данных [К] из-за расшифровки зашифрованных данных [К]
[a)] Обозначает источники питания/средства аварийной защиты.		

А.4 Активы и угрозы (внутренняя сеть медицинского учреждения)



Активы	№	Угроза (К — конфиденциальность, Ц — целостность, Д — доступность)
ПМИ во внутренней сети медицинского учреждения	41	Незащищенность данных [К] из-за отслеживания пути [К], неавторизованного доступа к сетевому оборудованию медицинского учреждения [К]/обмана [К], прослушивания [К]
Записи и распечатки коммуникационного следа вышеуказанной информации	42	Незащищенность данных [К] из-за подсматривания в протокол контроля [К], выноса [К]
Средства резервного копирования коммуникационного следа вышеуказанной информации	43	Незащищенность данных [К] из-за выноса монитора при копировании носителей информации [К]
Программное обеспечение сетевого оборудования	44	Незащищенность данных [К] из-за черного хода / установки программ, похищающих информацию [Ц]
Сетевое оборудование	45	Незащищенность данных [К] из-за выноса [К], несанкционированного вмешательства [К], влияния электромагнитного излучения [К]
	46	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]
Системы защиты окружающей среды сетевого оборудования[a)]	47	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д], разрыва кабеля [Д]
Операторы сетевого оборудования	48	Незащищенность из-за подкупа [К], угрозы [К], неверной настройки [К]
[a)] Обозначает источники питания/средства аварийной защиты.		

А.5 Активы и угрозы (обслуживание целевых приборов медицинских учреждений)



Активы	№	Угроза (К — конфиденциальность, Ц — целостность, Д — доступность)
ПМИ на карте памяти, диске и экране	51	Незащищенность данных [К] и их фальсификации из-за ошибки удаления на участке [К], подсматривания [К] / кражи [К], неавторизованного доступа к целевым устройствам обслуживания [К] / обмана [К], замены [Ц]
	52	Незащищенность данных [К] и их фальсификации [Ц] из-за кражи в пути передачи [К], неавторизованного доступа к целевым устройствам обслуживания [К]/ обмана [К], замены [Ц]
Записи и распечатки ПМИ[a)]	53	Незащищенность данных [К] и их фальсификации [Ц] посредством подглядывания в ведомости для работы [К], выноса [К], замены [Ц]
Резервные носители ПМИ[b)]	54	Незащищенность данных [К] и их фальсификации [Ц] из-за подсматривания в протокол работы [К], замены [Ц]
Программное обеспечение, обрабатывающее ПМИ	55	Незащищенность данных [К] из-за черного хода / установки программ, похищающих информацию [К]
Оборудование, обрабатывающее ПМИ	56	Незащищенность данных [К] и их фальсификации [Ц] из-за замены [Ц], выноса [К], несанкционированного вмешательства [К], влияния электромагнитного излучения [К]
	57	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]
Системы защиты окружающей среды оборудования, обрабатывающего ПМИ[c)]	58	Невозможность предоставления услуги [Д] из-за отказа [Д], аварии [Д], повреждения [Д]
Операторы, обрабатывающие ПМИ	59	Незащищенность данных из-за подкупа [К], неверного ввода информации [Ц], отказа службы [Д] при неверном удалении [Д]

[a)] Вносимые документы и носители информации не включены.
[b)] Как и для большинства больниц, контроль входа в помещения не предполагается.
[c)] Обозначает источники питания/средства аварийной защиты.

Библиография

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

[2] ISO/IEC 9797-1:1999, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher

[3] ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

[4] SO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements

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

УДК 004:61:006.354 ОКС 35.240.80 П85 ОКСТУ 4002

Ключевые слова: здравоохранение, информатизация здоровья, информационная защита, менеджмент защиты, удаленное обслуживание, медицинские устройства, медицинские информационные системы, анализ рисков

Редактор *А.Ф. Колчин*
Технический редактор *В.Ю. Фотиева*
Корректор *Ю.М. Прокофьева*
Компьютерная верстка *К.Л. Чубанова*

Сдано в набор 24.05.2016. Подписано в печать 30.05.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,80. Тираж 29 экз. Зак. 1402.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru