



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р
56838—
2015
ISO/TR 11633-2:2009

Информатизация здоровья

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

Часть 2

**Внедрение системы менеджмента
информационной безопасности**

ISO/TR 11633-2:2009

Health informatics — Information security management for remote maintenance
of medical devices and medical information systems —
Part 2: Implementation of an information security management system
(IDT)

Издание официальное



Москва
Стандартинформ
2016

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 англоязычной версии 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. № 2226-ст

4 Настоящий стандарт идентичен международному документу ISO/TR 11633-2:2009 «Информатизация здоровья. Менеджмент информационной безопасности удаленного технического обслуживания медицинских приборов и медицинских информационных систем. Часть 2. Внедрение системы менеджмента информационной безопасности» («Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 2: Implementation of an information security management system», IDT).

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

© Стандартиформ, 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

II

Содержание

1 Область применения	1
2 Термины и определения	1
3 Сокращения	3
4 Система менеджмента информационной безопасности для служб удаленного технического обслуживания	3
4.1 Общие положения	3
4.2 Область применения обеспечения соответствия	4
4.3 Политика безопасности	5
4.4 Оценка рисков	5
4.5 Риски, которыми предстоит управлять	6
4.6 Идентификация рисков, которые не описаны в настоящем стандарте	7
4.7 Обработка рисков	7
5 Меры управления безопасностью для СУО	7
6 Принятие остаточных рисков	8
7 Аудит безопасности	8
7.1 Аудит безопасности для служб удаленного технического обслуживания	8
7.2 Рекомендации по аудиту безопасности, проводимому сторонними организациями	8
Приложение А (справочное) Пример оценки риска в службах удаленного технического обслуживания	9
Библиография	115

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 настоящее время 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, «службам 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 риски, связанные 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 места расположения, запрашиваемого поставщиком (ЦУО), и места расположения 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 применяются в их учреждении для предотвращения рисков, описанных в настоящем стандарте;
- запросить от бизнес партнеров предоставить конкретные меры противодействия, так как настоящий документ может идентифицировать соответствующие риски безопасности;
- уточнить границы ответственности между владельцем медицинского учреждения и провайдером СУО;
- планировать программу по сохранению или снижению риска, т. к. остаточные риски уточняются при выборе подходящих «средств управления».

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

- необходимо будет только 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 безопасности, прошли подтверждение на соответствие;
- при предоставлении СУО в двух или более местах, провайдер может последовательно и эффективно применять меры противодействия.

Информатизация здоровья

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

Часть 2

Внедрение системы менеджмента информационной безопасности

Health informatics. Information security management for remote maintenance of medical devices and systems.
Part 2. Implementation of an information security management system

Дата введения — 2016—11—01

1 Область применения

В настоящем стандарте представлены примеры выбранных и применяемых для защиты служб удаленного технического обслуживания (СУО) «средств управления», определяемых в системе менеджмента информационной безопасности (СМИБ) на основе результатов анализа риска, описанного в ИСО/ТО 11633-1. Настоящий стандарт не рассматривает решение проблем коммуникаций и использование методов шифрования.

Настоящий стандарт включает в себя:

- каталог типов безопасных сред в медицинских учреждениях и у поставщиков СУО;
- пример комбинаций угроз и уязвимостей, идентифицированных при определенных условиях для «вариантов использования»
- пример оценивания и эффективности «средств управления», определяемых в системе менеджмента информационной безопасности (СМИБ).

2 Термины и определения

В настоящем документе используются 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 адаптирован из ИСО/МЭК 13335-1.

2 В контексте информационной безопасности в медицине, 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 информационной безопасности.

2.4 доступность (availability): Свойство быть доступным и годным к использованию по запросу авторизованного субъекта.

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

2.5 оценка соответствия (compliance assessment): Процессы, которыми организация подтверждает, что средства управления информационной безопасностью остаются рабочими и эффективными.

Примечание — Соответствие закону в частности относится к средствам управления безопасностью, установленным для соблюдения требований соответствующего законодательства, как например, Директивы Европейского Союза по защите персональных данных.

2.6 конфиденциальность (confidentiality): Свойство, заключающееся в том, что информация не может быть доступной или же не может быть раскрыта для неавторизованных лиц, объектов или процессов.

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

2.7 целостность данных (data integrity): Свойство, гарантирующее, что данные не будут изменены или уничтожены неправомерным 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 последствий.

[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): Согласованные виды деятельности по руководству и управлению организацией в отношении рисков.

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 для хищения информации (ISP — Information-stealing programme);
 ПМИ — Медицинская персональная 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 службы удаленного технического обслуживания (RSS — Remote maintenance service security);
 ВЧП — Виртуальная частная сеть (VPN — Virtual private network).

4 Система менеджмента информационной безопасности для служб удаленного технического обслуживания

4.1 Общие положения

Система менеджмента информационной безопасности (СМИБ) — это механизм, который циклически реализует последовательность процессов планирования / выполнения / проверки / воздействия, осуществляющихся в рамках политики защиты. Эта последовательность процессов означает, что организация планирует надлежащие меры обеспечения защиты (планирование), осуществляет эти меры обеспечения защиты (выполнение), контролирует эти меры (проверка) и вносит в них изменения при необходимости (управление воздействием). СМИБ уже соответствует стандарту ИСО/МЭК 27001, следовательно, при конструировании и эксплуатации СМИБ целесообразно ссылаться на ИСО/МЭК 27001. Это помогает также убедить пациентов, организации по оценке медицинского обслуживания и других лиц в эффективности мер обеспечения безопасности.

Основные шаги по созданию СМИБ продемонстрированы на рисунке 1.

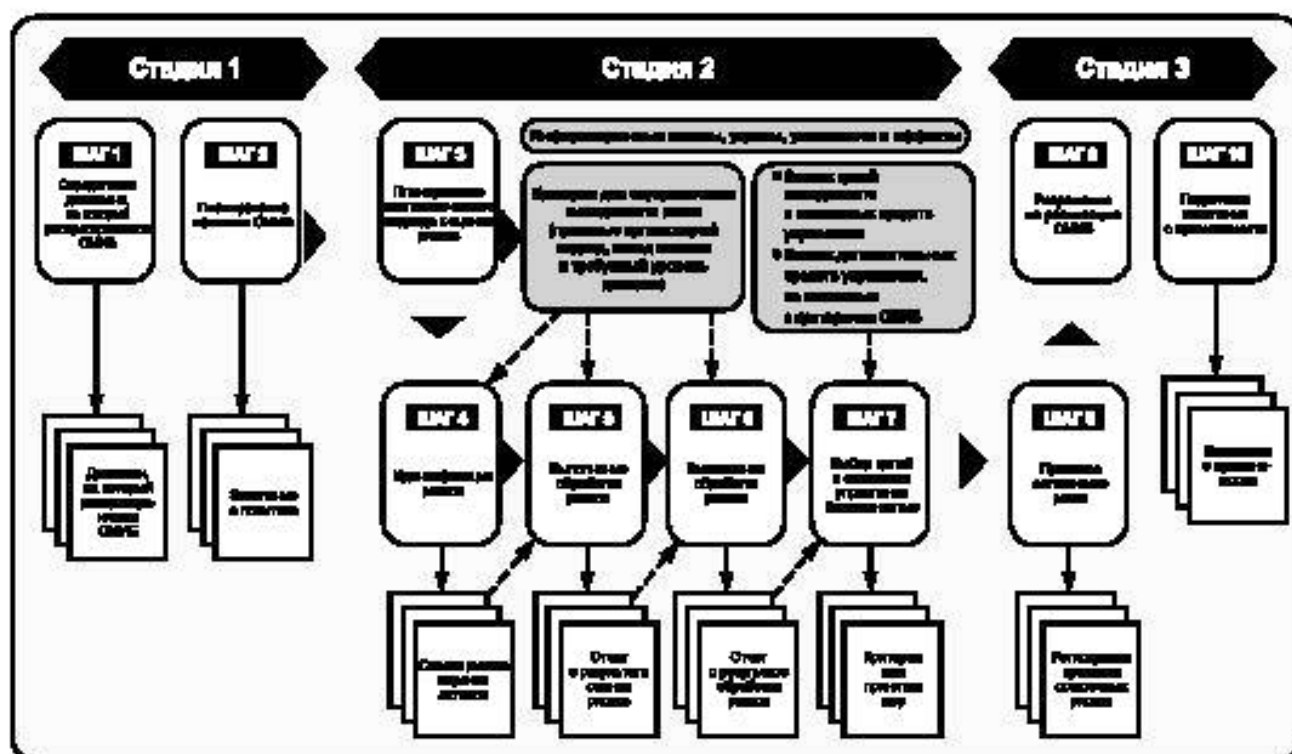


Рисунок 1 — Шаги реализации СМИБ

Ниже описаны меры обеспечения безопасности для охраны персональной информации в СУО в соответствии с концепцией СМИБ.

Медицинская организация и поставщик СУО должны создать соответствующую СМИБ. Кроме того, медицинская организация должна идеально выполнять работу по настройке менеджмента информационной безопасности для всех поставщиков СУО для защиты персональной информации. СУО соединяет сети поставщика СУО и медицинской организации. После соединения этих сетей возникают риски появления новых слабых мест в защите. В случае СУО может возникнуть иная проблема, связанная с созданием системы в отдельной организации, так как СУО действует между медицинской организацией и центром удаленного технического обслуживания (ЦУО), то есть между двумя независимыми друг от друга организациями. А значит, это будет проблемой, как для медицинской организации, так и для ЦОУ, если меры обеспечения безопасности с самого начала не рассматриваются как неотъемлемая часть СУО. В связи с этим использование СМИБ (с тщательно проверенным методом) может рассматриваться, как наилучший способ эффективно реализовать безопасность СУО.

В соответствии с большим количеством законов о защите персональной информации, медицинская организация принимает на себя ответственность и обязанности хранителя персональной информации. В случае СУО, медицинская организация должна запросить от поставщика служб удаленного технического обслуживания соответствующие меры для защиты персональной информации, т. к. поставщику дается доступ к настройкам целевого прибора в медицинском учреждении из центра удаленного технического обслуживания через сеть. Медицинская организация должна самостоятельно настроить все системы менеджмента информационной безопасности поставщиков СУО, которые поставляют СУО, и подтвердить, что в защите нет слабых мест. Дополнительно медицинская организация должна подтвердить, что уровень безопасности каждого поставщика СУО поддерживается на должном уровне.

Для настройки СМИБ необходимо выполнять документирование и удовлетворять следующим пунктам:

- политике обеспечения защиты;
- стандарту мер обеспечения безопасности;
- схеме политики защиты;
- набору технических решений;
- правилу выполнения операции;
- стандартам аудита безопасности;
- аудиту безопасности и журналу аудита.

Медицинская организация должна включить перечисленные пункты в контракт по предоставлению технического обслуживания или в соглашение между медицинской организацией и поставщиком СУО, которые ЦОУ применяет для обеспечения надлежащих мер в центре удаленного технического обслуживания. В результате медицинская организация распределит ответственность и обязанности по защите персональной информации в ходе технического обслуживания на поставщика СУО по контракту или соглашению. Медицинская организация должна создавать соответствующую СМИБ, одновременно прописывая в контракте на техническое обслуживание или контракте консигнации обязанность поставщика СУО осуществлять надзор в качестве последней инстанции, ответственной за менеджмент персональной информацией.

Анализ рисков и меры описаны в настоящем стандарте в соответствии с подходом СМИБ. Поэтому считается, что формирование безопасности службы удаленного технического обслуживания (ЗУО) с помощью данного подхода сможет обеспечить преимущества, как медицинской организации, так и центру удаленного технического обслуживания. Если содержание данной оценки риска не полное, то требуется дополнительная оценка риска только для недостающих частей.

4.2 Область применения обеспечения соответствия

Согласно рабочей модели, описанной в разделе 6 ИСО/ТО 11633-1, СМИБ охватывает следующие элементы:

- целевой прибор для технического обслуживания в медицинском учреждении (HCF);
- внутреннюю сеть медицинской организации;
- маршрут от точки доступа СУО в медицинской организации к ЦОУ;
- внутреннюю сеть ЦОУ;
- управление оборудованием в ЦОУ.

В связи с тем, что следующие риски существуют, независимо от наличия СУО, они исключаются из рассматриваемой в настоящем разделе области применения СМИБ:

- угрозы, связанные с доступностью к оборудованию и программному обеспечению, которое работает с защищенной медицинской информацией (PHI);
- угрозы, связанные с компьютерными вирусами;
- угрозы, связанные с персоналом, который имеет отношение к внедрению, обучению и практике.

4.3 Политика безопасности

В соответствии с пунктом 5.1.1 ИСО/МЭК 27002:2005 в базовую политику должно быть включено следующее:

- a) определение информационной безопасности, ее общих целей, области применения и важности безопасности как механизма содействия обмену информацией;
- b) заявление о намерении руководства поддерживать цели и принципы информационной безопасности в соответствии с бизнес-стратегией и целями организации;
- c) подход для формирования задач управления информационной безопасностью и средств управления для решения этих задач, включая структуру оценки рисков и менеджмент рисков;
- d) краткое разъяснение политик безопасности, принципов, стандартов и требований соответствия, имеющих определенную важность для организации, включая:

- соответствие юридическим, нормативным и контрактным требованиям,
- обучение защите, инструктаж, требования осведомленности,
- управление непрерывностью бизнеса,
- последствия нарушения политики обеспечения защиты информации;

определение общей и конкретной ответственности за менеджмент информационной безопасности, включая отчетность об инцидентах нарушения информационной безопасности;

ссылки на документацию, которая может поддерживать политику безопасности, например, более подробные описания политики безопасности и процедур для конкретных информационных систем или правил безопасности, которым должны следовать пользователи.

После применения этих условий к защите службы удаленного технического обслуживания (ЗУО), необходимо обеспечить доступность системы, обеспечить целостность, читаемость и сохранение персональной информации пациента.

Необходимо, чтобы в базовой политике защиты службы удаленного технического обслуживания были указаны используемые в ней технические и систематические меры, а также меры по использованию человеческих ресурсов и физические меры безопасности.

Следующая информация предназначена для более крупного интегрированного медицинского учреждения (МУ). Возможно, что ЦОУ обеспечивает службы удаленного технического обслуживания в двух или более подразделениях крупного медицинского учреждения. В таком случае необходима политика объединенного управления. Если масштаб медицинского учреждения и организация работы отличаются от крупного интегрированного медицинского учреждения, то важно реализовывать защиту в организации в соответствии с фактической ситуацией.

4.4 Оценка рисков

В оценке риска выполняется анализ информационных активов по отношению к следующим вопросам:

- какие угрозы существуют;
- насколько возможно возникновение каждой угрозы и как часто они могут возникать;
- насколько сильно влияние угрозы при ее реализации.

Методы анализа можно разделить на следующие четыре общих подхода:

a) Базовый подход.

Базовый подход анализа риска основан на стандартах и руководствах, используемых в целевых областях применения. Меры безопасности в данном подходе основываются на стандарте оценки риска, заранее созданном для этой отрасли.

Несмотря на то, что данный подход дает преимущество во времени и по затратам, так как отсутствует необходимость оценки самого риска, интерпретация рисков, описанных в стандартах, для рисков в конкретной организации может быть проблематичной.

b) Детальный анализ рисков.

Выполнение детальной оценки риска включает анализ риска для элементов системы, а также необходимость выбора соответствующего плана менеджмента. Для такой оценки риска требуется значительный бюджет и время, включая обеспечение необходимых человеческих ресурсов.

с) Смешанный подход.

Данный подход сочетает базовый подход с подетальным анализом рисков и обладает преимуществами обоих.

д) Неформальный подход.

Данный подход применяет анализ риска, использующий знания и опыт персонала организации. Для третьей стороны сложно оценить результат анализа рисков, потому что данный метод не является структурированным.

СУО связана с медицинской организацией и центром удаленного технического обслуживания, следовательно, анализ рисков должен быть согласован с обеими сторонами. В настоящем стандарте смоделирован типичный вариант использования, а также выполнена оценка риска для этой модели. Анализ рисков выполнен по базовому подходу а) и смешанному подходу в) и далее используются результаты этой оценки риска, которые представлены в таблице А.1. Таблица А.1 позволяет выбрать соответствующую цель управления информационной безопасностью и план управления для ее достижения, которые представлены в ИСО/МЭК 27001, по результатам анализа риска, выполненного в соответствии с ИСО/ТО 11633-1. Таблица А.1 соответствует ИСО/МЭК 27001 и состоит из 11 областей управления информационной безопасностью и 133 планов управления для реализации целей информационной безопасности.

Меры, предписанные в настоящем стандарте, устанавливают процедуры, которые должны соблюдаться, как минимум при работе СУО. Медицинская организация, которая также является администратором персональной информации, должна оценить, соответствует ли центр удаленного технического обслуживания настоящему стандарту, и запросить принятие необходимых мер, если это не так. Более того, если уровень безопасности медицинской организации ниже уровня, указанного в настоящем стандарте, то необходимо выполнить соответствующие меры. Каждый поставщик СУО должен применять необходимые меры, чтобы соответствовать требованиям, описанным в настоящем стандарте.

4.5 Риски, которыми предстоит управлять

В данном подразделе рассматривается несколько примеров по предотвращению рисков, связанных с защитой персональной информации, которые наиболее типичны для СУО. Важно, чтобы меры против этих рисков были достаточными. Обсуждаемый риск приводится только в качестве примера. Важно также уметь управлять и другими типами рисков.

а) Медицинская организация осуществляет управление обработкой персональной информации, выполняемой ЦОУ

В этом случае проблемой, требующей особого внимания, является утечка информации третьим лицам. Необходимо уделять внимание информации, отображаемой на экранах компьютеров на рабочих местах, и информации, распечатываемой на бумажном носителе, а также угрозе хакерского проникновения в систему. Основные риски следующие:

- просмотр с экранов лицами, не работающими в центре удаленного технического обслуживания;
- утечка в пользу третьих лиц;
- утечка из журналов при анализе данных, с бумажного носителя или кэш-памяти и т. д.;
- утечка в сети.

б) Центр удаленного технического обслуживания получает доступ к оборудованию медицинской организации для технического обслуживания по решению административного органа.

В этом случае проблемами, требующими особого внимания, являются ошибка оператора и несоответствующий доступ к компьютеру (запуск не разрешенных операций). Главными рисками являются:

- уничтожение данных в целевом приборе в связи с ошибкой оператора;
- уничтожение данных в целевом приборе в связи с вредоносной и злоумышленной деятельностью;
- утечка и уничтожение наиболее важной информации с помощью проникновения внутрь в процессе технического обслуживания прибора.

с) Центр удаленного обслуживания обновляет программное обеспечение.

В этом случае, необходима особая осторожность, чтобы не установить на целевые приборы вредоносное программное обеспечение и компьютерные вирусы и т.п. Главными рисками являются:

- утечка и уничтожение данных в целевом приборе из-за вредоносного программного обеспечения;
- утечка и уничтожение важной информации при вторжении компьютерного вируса.

4.6 Идентификация рисков, которые не описаны в настоящем стандарте

В настоящем стандарте оценка риска производится в соответствии с типовой моделью, следовательно, остальные случаи не рассматриваются.

Если бизнес-модель отличается от модели, которая рассматривается в настоящем стандарте, то результаты оценки риска, полученные в соответствии с настоящим стандартом, могут быть неправомерно использованы. Есть также возможность, что не все случаи могут быть охвачены. Если охват всех случаев не возможен, то необходимо провести подробный анализ рисков, используя объединенный подход оценки риска, который не описан в настоящем стандарте.

Метод оценки риска при подробном анализе риска рассмотрен в ИСО/ТО 11633-1. Применяя методы ИСО/ТО 11633-1, результаты оценки риска, отличающейся бизнес-модели, могут легко быть интегрированы с результатами оценки риска, выполненного в соответствии с настоящим стандартом.

4.7 Обработка рисков

Обработка риска определяется как обеспечение приемлемого риска в соответствии с результатами оценки риска. Варианты работы с рисками продемонстрированы в таблице 1. При необходимости эти варианты могут комбинироваться и применяться.

Обычно в процессе управления риском выбирается сочетание этих мер после общей оценки серьезности риска или простоты реализации таких мер. Особенно важно применять управление риском(ами), предусмотренное законами и регламентами по защите конфиденциальности информации. В этом случае, необходимо обязательно управлять риском надежно, потому что такие меры, как сохранение или передача рисков, не всегда являются отвечающими требованиям, или адаптировать избегание риска и, согласно закону, совсем не обрабатывать объект персональной информации в СУО.

В настоящем стандарте рекомендуется управлять риском на основе СМИБ. Конкретные меры детально даются в приложении А.

Таблица 1 — Обработка риска

Управление рисками	Передача рисков
Меры (план управления) адаптированы для надежного сокращения ущерба. Предотвращение риска. Применяются меры для снижения угроз и уязвимостей. Сведение к минимуму ущерба. Применяются меры для снижения ущерба при реализации возникшего риска.	Меры по передаче сторонним организациям по контракту и т. д. Страхование. Использование страхования от ущерба и других типов страхования, передавая, таким образом, риск. Аутсорсинг. Информационные активы и меры информационной безопасности доверяются третьей стороне.
Сохранение риска	Избегание риска
Подход, который воспринимает риск как принадлежащий организации. Финансирование. Означает накопление резерва и т. д. Никаких мер не предпринимается.	Подход, когда подходящие меры не найдены. Прекращение деятельности. Деятельность останавливается. Уничтожение информационных активов. Объект управления утерян.

5 Меры управления безопасностью для СУО

Возможность утечки персональной информации из СУО, например информации о больном, требует, чтобы центр удаленного технического обслуживания оказал помощь медицинской организации для обеспечения защиты СУО.

Чтобы принять соответствующие меры защиты для обеспечения безопасности СУО, медицинская организация и центр удаленного технического обслуживания (ЦОУ) должны выбрать средства управления безопасностью, основываясь на результатах оценки риска. Вне зависимости от того, контролируется ли ЦОУ медицинской организацией, ЦОУ должен убедиться в том, что СУО соответствуют требованиям безопасности.

В приложении А более детально показано, как перейти к целям и соответствующим средствам управления для их реализации, обеспечивающим менеджмент безопасности, в случае работы СУО для

медицинской организации и центра удаленного технического обслуживания. Ожидается, что информация в таблице А.1 снизит время оценки риска при подготовке СУО.

Даже если СУО уже эксплуатируется, то рекомендуется проводить аудит, используя таблицу А.1, чтобы убедиться, что оценка риска была адекватной.

6 Принятие остаточных рисков

Остаточными рисками называют такие риски в медицинском учреждении, когда оно преднамеренно не принимает достаточных контрмер или когда у медицинского учреждения возникают трудности с идентификацией этих рисков, или риски, снижение которых потребуют больших затрат, если медицинское учреждение пожелает применить все контрмеры, определяемые оценкой риска. Когда риск остается, даже если медицинское учреждение выполняет управление рисками, сохранение или передачу риска, то руководству необходимо решить, принять или нет эти остаточные риски в результате выполнения управления рисками. Если руководство медицинского учреждения принимает эти остаточные риски, то это значит, что медицинское учреждение принимает СУО, созданную в соответствии с оценкой риска на основании СМИБ.

Медицинское учреждение принимает остаточные риски для всего контракта СУО, а ЦОУ реализует СУО, с учетом этих остаточных рисков. В соответствии с результатом анализа риска в СУО, продемонстрированным в приложении А, в частности в центре удаленного технического обслуживания, сохраняется возможность утечки персональной информации, включая медицинскую персональную информацию. Медицинское учреждение должно выявлять эти опасности, учитывать руководящие документы, выпущенные правительством, а также проводить аудит соответствующих мер безопасности, принятых в действующем СУО.

7 Аудит безопасности

7.1 Аудит безопасности для служб удаленного технического обслуживания

Целью аудита безопасности является подтверждение эффективности реализации менеджмента риска для обеспечения защиты и подтверждение выполнения надлежащего управления защитой на основе этой оценки риска. Аудит безопасности всесторонне оценивает соответствие стандарту менеджмента информационной безопасности, но также возможно выполнить аудит самой службы удаленного технического обслуживания. При аудите безопасности СУО аудитор проверяет и оценивает, если это возможно, поддерживается и выполняется ли управление защитой на основе оценки риска.

Более того, как для медицинского учреждения, так и для центра удаленного технического обслуживания аудит является эффективным способом, оценки стандартов безопасности, так как результат таких аудитов становится действующим оценочным материалом для улучшения надежности СУО.

7.2 Рекомендации по аудиту безопасности, проводимому сторонними организациями

При проведении медицинским учреждением аудита информационной безопасности, как внутреннего аудита, могут возникнуть следующие проблемы:

- сложно понять из оценки риска, существуют ли риски утечки информации;
- не будут удовлетворены требования объективности и независимости;
- в связи с необходимостью профессиональных знаний, обучение команды аудиторов требует времени;
- сложно составить отчет об аудите в связи с риском разглашения.

Как указано выше, аудит медицинского учреждения должен выполняться внешней организацией и аудитором с высоким уровнем технических знаний, чтобы объективно оценить службы удаленного технического обслуживания. Выполнение внешнего аудита на основе соответствующей процедуры аудита облегчает сертификацию информационной безопасности такой системы, как СМИБ. Наконец, медицинское учреждение может улучшить общественную репутацию. Рекомендуется также проводить внешний аудит для снижения любых расхождений информации о надежности в отчетах аудита безопасности медицинского учреждения и центра удаленного технического обслуживания.

Приложение А
(справочное)**Пример оценки риска в службах удаленного технического обслуживания**

В настоящем приложении приводится пример оценки риска СУО. Пример показан в таблице А.1. Нумерация строк в таблице А.1 такая же, как у соответствующих разделов ИСО/МЭК 27001.

Комментарии к таблице А.1 представлены сразу после окончания данной таблицы.

Таблица А.1 — Пример оценки риска СУО

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Уязвимость	Актив	Пример угрозы (К — конфиденциальность, Ц — целостность, Д — доступность)	Пример средства управления	У	В	П	О
А.5 По- литика информа- ционной безопас- ности	А.5.1 Направля- ющая роль руковод- ства в сфере информа- ционной безопас- ности	Обеспечить направляю- щую роль ме- неджмента и поддержку ин- формационной безопасности в соответствии с требова- ния- ми бизнеса и соответствую- щими законо- дательными и регламентиру- ющими требо- ваниями.	Должен быть раз- работан, одобрен руководством, опубликован и до- веден до персонала и соответствующих внешних сторон комплекс политик информационной безопасности.	—	—	—	—	—	—	—	—	—
			С тем, чтобы гаран- тировать постоян- ную пригодность, соответствие и результативность политик информа- ционной безопасно- сти должны пере- сматриваться через запланированные интервалы времени или когда произве- дены существенные изменения.	—	—	—	—	—	—	—	—	—
А.6 Орга- низация системы информа- ционной безопас- ности	А.6.1 Внутренняя организа- ция	Осуществлять менеджмент информацион- ной безопас- ности в рамках организации	Руководство должно активно поддержи- вать безопасность в пределах органи- зации посредством четкого руководства, продемонстрирован- ных обязательств, подробного распре- деления и призна- ния ответственности за информационную безопасность.	—	—	—	—	—	—	—	—	—

10

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Деятельность по информационной безопасности должна быть скоординирована представителями различных частей организации с соответствующими ролями и рабочими функциями.	—	—	—	—	—	—	—	—	—
			Вся ответственность за информационную безопасность должна быть четко определена.	—	—	—	—	—	—	—	—	—
			Должен быть определен и реализован процесс менеджмента получения разрешения для новых средств, обрабатывающих информацию.	—	—	—	—	—	—	—	—	—
			Требования к конфиденциальности или соглашения о неразглашении, отражающие потребности организации в информационной безопасности, должны быть выявлены и должны регулярно анализироваться. Должны поддерживаться подходящие контакты с компетентными органами.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Должны поддерживаться надлежащие контакты со специальными группами или другими форумами специалистов по защите, а также профессиональными ассоциациями.	—	—	—	—	—	—	—	—	—
			Подход организации к менеджменту информационной безопасности и ее реализации (т. е. цели управления, средства управления, политика, процессы и процедуры для информационной безопасности) должны независимо анализироваться через запланированные интервалы, или когда происходят значительные изменения в реализации защиты.	—	—	—	—	—	—	—	—	—
	А.6.2 Внешние стороны	Поддерживать в рабочем состоянии информационную безопасность организации и средства, обрабатывающие	Должны быть выявлены риски для информации организации и средств, обрабатывающих информацию, происходящие из депозитных процессов, вовлекающих внешние	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
		информацию, которые доступны внешним сторонам, обрабатываемые внешними сторонами, сообщены внешним сторонам или управляются внешними сторонами.	стороны, а перед предоставлением доступа должны быть реализованы надлежащие средства управления. Все выявленные требования защиты должны быть рассмотрены до того, как клиентам будет предоставлен доступ к информации или активам организации.	—	—	—	—	—	—	—	—	—
			Соплашения с третьими сторонами, включающие доступ, обработку, обмен или менеджмент информации организации или средств, обрабатывающих информацию, или добавление изданий или услуг к средствам, обрабатывающим информацию, должны включать в себя все значимые требования защиты.	36	С1	т	Отказ (угроза Д) сетевого оборудования стороны поставщика интернет-служб приводит к недоступности службы СУО.	Контракты на поставку сторонних услуг (обслуживание, проверка, резервное копирование) предотвращают недоступность службы, указывая сферу ответственности со стороны поставщика интернет-служб.	3 > 2	2	2	12 > 4
							Поврежденное (угроза Д) сетевого оборудования со стороны поставщика интернет-служб приводит к потере Д к СУО.	Контракты на поставку сторонних услуг (меры в случае аварии и планы по непрерывной работе) предотвращают недоступность службы, указывая сферу ответственности со стороны поставщика интернет-служб.	3 > 2	2	1	6 > 4

14 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							Уничтожение (угроза Д) сетевого оборудования со стороны постав- щика интернет-служб приводит к потере Д к СУО.	Контракты на поставку сторонних услуг (ключе- вой менеджмент) предотвращают недо- ступность службы, указывая сферу ответ- ственности со стороны поставщика интернет- служб.	3 > 2	2	1	6 > 4
				37	С1	п	Отказ (угроза Д) или разъединение кабеля природоохранного средства от сетевो- го оборудования со стороны поставщика интернет-служб приво- дит к потере Д к СУО.	Контракты на поставку сторонних услуг (об- служивание, проверка, резервное копирова- ние) предотвращают недоступность служ- бы, указывая сферу ответственности со стороны поставщика интернет-служб.	3 > 2	2	1	6 > 4
							Поврежденное (угро- за Д) природоохранно- го оборудования для сетевого оборудования со стороны постав- щика интернет-служб приводит к потере Д к СУО.	Контракты на поставку сторонних услуг (меры в случае аварии и пла- ны по непрерывной работе) предотвра- щают недоступность службы, указывая сферу ответственности со стороны постав- щика интернет-служб.	3 > 2	2	1	6 > 4
							Уничтожение (угроза Д) природоохранного средства для сетево- го оборудования со стороны поставщика интернет-служб приво- дит к потере Д к СУО.	Контракты на поставку сторонних услуг (ключе- вой менеджмент) пре- дотвращают недо- ступность службы, указывая сферу ответственности со стороны поставщика интернет-служб.	3 > 2	2	1	6 > 4

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.7 Ме- неджмент активов	А.7.1 Ответ- ственность за активы	Достичь и под- держивать в рабочем со- стоянии подхо- дящую защиту организацион- ных активов.	Все активы должны быть четко опреде- лены, и должен быть составлен и должен поддерживаться в рабочем состоянии реестр всех важных активов. Вся информация и активы, связанные со средствами, об- рабатывающими ин- формацию, должны «находиться во владении» назначенной части организации. Должны быть опре- делены, документи- рованы и внедрены правила для при- емлемого использо- вания информации и активов, связанных со средствами, об- рабатывающими информацию.	—	—	—	—	—	—	—	—	—
	А.7.2 Классифи- кация ин- формации	Гарантиро- вать, что информация обеспечена соответствующим уровнем защиты.	Информация должна быть классифициро- вана с точки зрения ее значения, зако- нодательных требо- ваний, уязвимости и критичности для организации.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСОМЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			В соответствии со схемой классифика- ции, принятой организацией, дол- жен быть разрабо- тан и реализован подходящий набор процедур марки- ровки и обработки информации.	—	—	—	—	—	—	—	—	—
А.8 Защи- та чело- веческих ресурсов	А.8.1 Перед наймом на работу А.8.2 Во время вы- полнения работы А.8.3 Заверше- ние или изменение работы по найму	Гарантировать, что служащие, подрядчики и пользователи третьей сторо- ны понимают свою ответ- ственность и подходят для должностей, на которые они рассматрива- ются, а также снизить риск кражи, мошен- ничества или неправильного использования средств. Гарантиро- вать, что все служащие, подрядчики и пользователи третьей сторо- ны осознали угрозы	Роли и ответствен- ность служащих, подрядчиков и пользователей третьей стороны в отношении без- опасности должны быть определены и задокументированы в соответствии с по- литикой информаци- онной безопасности организации.	—	—	—	—	—	—	—	—	—
			Проверки верифи- кации в фоновом режиме по всем кандидатам в служе- щие, в подрядчики и в пользователей третьей стороны должны проводиться в соответствии с имеющимися отноше- ние к делу законами, нормами и этикой, и должны быть про- порциональны	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСОМЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
		информацион- ной безопасно- сти и хлопоты по защите информации, свою ответ- ственность и свои обяза- тельства, и оснащены для того, чтобы поддерживать организацион- ную политику безопасности во время сво- ей обычной работы, а так- же для того, чтобы снизить риск ошибки человека. Гарантировать, что служащие, подрядчики и пользователи третьей сторо- ны уходят из организации или меняют службу в уста- новленном по- рядке.	деловым требовани- ям, классификации информации, кото- рая будет доступной, и предполагаемым рискам. Как часть догово- рного обязательства, служащие, подря- дчики и пользователи третьей стороны должны согласиться и подписать сроки и условия договора личного найма, в котором должны быть указаны их ответственность за информаци- онную безопасность и ответственность организации за ин- формационную без- опасность. Должна быть четко определена и на- значена ответствен- ность за осущест- вление окончания ра- боты по найму.	11	А1	а	Неавторизованное ис- пользование (угроза К) техническим персона- лом центра удаленного технического обслужи- вания персональной медицинской инфор- мации на локальном оборудовании центра удаленного техниче- ского обслуживания приводит к угрозе рас- крытия информации.	Внутренний аудит записей может обна- ружить неавторизо- ванное использование техническим персона- лом центра СУО. Кро- ме того, неавторизо- ванное использование техническим персона- лом центра СУО мо- жет быть обнаружено в связи с ограничени- ем противозаконной работы. Проверки конфиденци- альности и прошлого опыта (подтверждение квалификации) могут ограничить неавто- ризованное исполь- зование техническим персоналом центра СУО предотвращени- ем противозаконной деятельности операто- ров. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.	3 > 2	3	1	9 > 6

18 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				12	A1	а	Неавторизованное использование (угроза К) техническим персоналом центра удаленного технического обслуживания персональной медицинской информации на локальном оборудовании центра удаленного технического обслуживания приводит к угрозе раскрытия информации.	Внутренний аудит записей может обнаружить неавторизованное использование техническим персоналом центра СУО. Кроме того, неавторизованное использование техническим персоналом центра СУО может быть обнаружено в связи с ограничением противозаконной работы. Проверки конфиденциальности и прошлого опыта (подтверждение квалификации) могут ограничить неавторизованное использование техническим персоналом центра СУО предотвращением противозаконной деятельности операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участки	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				19	A1	h	Подкуп приводит к раскрытию (угроза К) персональной медицинской информации.	Проверки конфиденциальности и прошлого опыта (подтверждение квалификации) могут ограничить неавторизованное использование технических персональных данных СУО предотвращением противозаконной деятельности операторов.	3 > 2	3	1	9 > 6
				28	B1	o						
				28	B2							
				48	D1							
				51	E1	a	Неавторизованное использование (угроза К) техническим персоналом центра удаленного технического обслуживания персональной медицинской информации на локальном оборудовании центра удаленного технического обслуживания приводит к угрозе раскрытия информации.	Внутренний аудит записей может обнаружить неавторизованное использование технических персональных данных СУО. Кроме того, неавторизованное использование технических персональных данных СУО может быть обнаружено в связи с ограничением противозаконной работы. Проверки конфиденциальности и прошлого опыта (подтверждение квалификации) могут ограничить неавторизованное использование технических персональных данных СУО предотвращением противозаконной деятельности операторов.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
								Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
							Замена основным обслуживающим пер- соналом персональной медицинской инфор- мации в оборудовании, подлежащем техниче- скому обслуживанию, приводит к нарушению Ц информации.	Управление конфи- денциальностью ин- формации (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и за- прет стирания файла) может предотвратить замену файлов основ- ным обслуживающим персоналом.	3	3	1	9
				52	E1	а	Неавторизованное ис- пользование (угроза К) техническим персона- лом центра удаленного технического обслужи- вания персональной медицинской инфор- мации на локальном оборудовании центра удаленного техниче- ского обслуживания приводит к угрозе рас- крытия информации.	Внутренний аудит записей может обна- ружить неавторизи- рованных пользователей техническим персо- налом центра СУО. Кроме того, неавто- ризованные использо- вание техническим персоналом центра СУО может быть об- наружено в связи с ограничением проти- вопозажной работы. Проверки конфиденци- альности и прошлого опыта (подтверждение квалификации) могут ограничить неавтори- зованных	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Аспект	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
								использование технического персоналом центра СУО предотвращением деятельности конной деятельности операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
				52	E1	а	Замена основным обслуживающим персоналом персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию, приводит к нарушению Ц информации.	Управление конфиденциальностью информации (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и запрет стирания файла) может предотвратить замену файлов технического обслуживания.	3 > 2	3	1	9 > 6
				53	E1	с	Удаление или замена на участке лечащим врачом приводит к раскрытию нарушения К или угрозе Ц персональной медицинской информации.	Конфиденциальность может ограничить неавторизованное использование сдерживанием и предотвращением незаконных действий, однако сама по себе ее влияние незначительно.	3	3	1	9

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				59	E1	h	Подкуп приводит к раскрытию К персональной медицинской информации.	Проверки конфиденциальности и прошлого опыта могут ограничить неавторизованное использование вследствие подкупа посредством ограничения и предотвращения противозаконных действий операторов.	3 > 2	3	1	9 > 6
		Руководство должно требовать от сотрудников, подрядчиков и третьих сторон применять правила обеспечения защиты в соответствии с установленными организациями политикой и процедурами.		—	—	—	—	—	—	—	—	—
		Все службам организации и, если это имеет отношение к делу, подрядчикам и пользователям, третьей стороны, должны получить подходящую подготовку по повышению осведомленности и регулярные обновления организационной политики и процедур, насколько это имеет отношение к их рабочим функциям.		19	A1	h	Неверный ввод (угроза Ц) и случайное удаление (угроза Д) ведут к перебою в Д к СГО.	Тренинг и выработка стандартных навыков могут предотвратить перебои в работе, вызванные неверным или случайным удалением, поддерживая и повышая квалификации операторов.	3 > 2	3	2	18 > 12

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участки	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				28	B1	0	Неверная установка (угроза К) приводит к неожиданному раскры- тию (угроза К) персо- нальной медицинской информации.	Тренинги и выработка стандартных навыков могут предотвратить перебои в работе, вы- званные неверным или случайным удале- нием, поддерживая и повышая квалифика- цию операторов.	3 > 2	3	2	18 > 12
				48	D1							
				59	E1	h	Неверный ввод (угроза Ц) и случайное удале- ние (угроза Д) ведут к перебою в Д к СУО.	Тренинги и выработка стандартных навыков могут предотвратить перебои в работе, вы- званные неверным или случайным удалением, поддерживая и повы- шая квалификации операторов.	3 > 2	3	2	18 > 12
А.8 Защи- та чело- веческих ресурсов	А.8.3 Заверше- ние или изменение работы по найму	Гарантировать, что служащие, подрядчики и пользователи третьей сторо- ны уходят из организации или меняют службу упоря- дочно.	Все служащие, под- рядчики и пользова- тели третьей сторо- ны должны вернуть все активы органи- зации, находящиеся в их владении, по окончании их работы по найму, договора или соглашения. Права доступа всех служащих, подряд- чиков и пользовате- лей третьей стороны к информации и средствам, обраба- тывающим инфор- мацию, должны быть	51	E1	a	Замена основным обслуживающим пер- соналом персональной медицинской инфор- мации в оборудовании, подлежащем техниче- скому обслуживанию. Приводит к нарушению Ц информации.	Управление конфи- денциальностью ин- формации (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и за- прет стирания файла) может предотвратить замену файлов тех- ническим персоналом центра удаленного технического обслужи- вания.	3 > 2	3	1	9 > 6

24 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			удалены по окончании срока их работы по найму, договора или соглашения, или же скорректированы при изменении.									
			Сотрудники, нарушившие правила конфиденциальности, подлежат формальному дисциплинарному процессу.				—	—				—
А.9 Финансовая безопасность и охрана окружающей среды	А.9.1 Зона безопасности	Предотвратить несанкционированный физический доступ, нанесение ущерба и вмешательство в деятельность и невозможность и информацию организации.	Для защиты зон, в которых находятся информация и средства, обрабатывающие информацию, должны использоваться периметры безопасности (барьеры, такие как стены, управляемый картой турникет на входе или контролируемая человеком вахта).	51	Е1	а	Подглядывание (угроза К) экрана на участке третьими лицами, персоналом медицинского учреждения, сетевыми администраторами медицинского учреждения или основным персоналом других компаний приводит к неавторизованному использованию (нарушению К) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию, и раскрытию информации.	Переговорки предотвращают незапланированные визиты случайных лиц	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Зоны безопасности должны быть защищены подходящими средствами управления входом, с целью гарантировать, что только персоналу, имеющему разрешение, предоставлен доступ.	11	A1	а	Несанкционированный вход в систему (угроза К) третьих лиц, персонала медицинского учреждения, сетевых администраторов медицинского учреждения или основного технического персонала компании путем просматривания (угроза К) с экрана, словарной атакой на оборудование центра удаленного технического обслуживания или действием от имени авторизованного лица при помощи незаконным образом полученного пароля, приводит к неавторизованному использованию (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания и раскрытию информации.	Управление входом в помещение может ограничить вход в помещение третьих лиц, персонала центра удаленного технического обслуживания или сетевых администраторов центра удаленного технического обслуживания, предотвращая таким образом просмотр с экрана, несанкционированный вход или фальсификацию авторизованного лица.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				13	A1	с	Если лечащий врач оставляет соответствующий актив в связи с ремонтом или по причине невозможности его отсоединения, то он может быть просмотрен (угроза К) или страницы могут быть удалены третьими лицами, персоналом центра удаленного технического обслуживания или сетевыми администраторами центра удаленного технического обслуживания.	Утилизация шредером может предотвратить просмотр или удаление страниц третьими лицами, персоналом центра удаленного технического обслуживания или сетевыми администраторами центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6
				14	A1	d	Если соответствующий ресурс оставлен в связи с ремонтом или по причине невозможности его отсоединения, удаление страниц третьими лицами, персоналом центра удаленного технического обслуживания или сетевыми администраторами центра удаленного технического обслуживания.	Управление ключами защиты может предотвратить удаление дисков третьими лицами, персоналом центра удаленного технического обслуживания или администратором центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				16	A1	f	обслуживания приводит к раскрытию (угроза К) персональной медицинской информации.		3 > 2	3	1	9 > 6
				17	A1	f	Удаление оборудования центра удаленного технического обслуживания и дисков лицами, не являющимися персоналом центра удаленного технического обслуживания, а также пропажу оборудования и дисков.	Управление входом в помещение может предотвратить вход в помещение лиц, не являющихся персоналом центра удаленного технического обслуживания, а также пропажу оборудования и дисков.	3 > 2	2	1	6 > 4
				18	A1	g	Уничтожение (угроза Д) оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Управление ключами защиты может предотвратить несанкционированный доступ к оборудованию неавторизованных лиц.	3 > 2	2	1	6 > 4
				18	A1	g	Уничтожение (угроза Д) природоохранной системы для оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Управление ключами защиты может предотвратить несанкционированный доступ к оборудованию неавторизованных лиц.	3 > 2	2	1	6 > 4

28 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				22	В1	И	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление (угроза К) страниц лицами, не являющимися сетевым администратором центра удаленного технического обслуживания, приводит к раскрытию персональной медицинской информации.	Утилизация шредером может предотвратить просмотр или удаление страниц сетевыми администраторами центра удаленного технического обслуживания. Управление входом в помещение может ограничить вход в помещение третьих лиц, персонал центра удаленного технического обслуживания или сетевых администраторов центра удаленного технического обслуживания, предотвращая, таким образом, просмотр или удаление страниц, предотвращая присутствие неавторизованных лиц.	3 > 2	3	1	9 > 6
				23	В1	К	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление (угроза К) страниц лицами, не являющимися сетевым администратором центра удаленного технического обслуживания, приводит к раскрытию персональной медицинской информации.	Управление ключами защиты может предотвратить доступ и удаление дисков лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, предотвращая доступ к дискам неавторизованных лиц.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				25	B1	m	Удаление (угроза К) оборудования центра удаленного технического обслуживания, почтовых серверов и их дисков лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, приводит к раскрытию персональной медицинской информации.	Управление ключами защиты может предотвратить удаление сетевого оборудования, почтовых серверов или дисков лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, предотвращая доступ неавторизованных лиц.	3 > 2	3	1	9 > 6
				26	B1 B2	m	Уничтожение (угроза Д) оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Управление ключами защиты может предотвратить доступ к оборудованию неавторизованных лиц.	3 > 2	2	1	6 > 4
				27	B1 B2	p	Уничтожение (угроза Д) природоохранного средства для сетевого оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Управление ключами защиты может предотвратить доступ к оборудованию неавторизованных лиц.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				42	D1	i	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление страниц (угроза К) лицами, не являющимися сетевыми администраторами учреждения медицинского учреждения, приводит к раскрытию персональной медицинской информации.	Утилизация шредером может предотвратить просмотр или удаление страниц лицами, не являющимися сетевыми администраторами медицинского учреждения. Управление входом в помещение (аппаратной трассировки связи) может ограничить вход в помещение лиц, не являющихся сетевыми администраторами медицинского учреждения, и предотвращает просмотр или удаление страниц, предотвращая присутствие неавторизованных лиц.	3 > 2	3	1	9 > 6
				43	D1	k	Если соответствующий ресурс оставлен для ремонта или контроля, то удаление (угроза К) страниц лицами, не являющимися сетевыми администраторами медицинского учреждения, приводит к раскрытию персональной медицинской информации.	Управление ключами защиты может предотвратить доступ и удаление дисков лицами, не являющимися сетевыми администраторами медицинского учреждения, предотвращая доступ к диску неавторизованных лиц.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				45	D1	m	Удаление (угроза К) оборудования центра удаленного техниче- ского обслуживания, почтовых серверов и их дисков лицами, не являющимися сетевы- ми администраторами медицинских учрежде- ний, приводит к рас- крытию персональной медицинской инфор- мации.	Управление входом в помещение может предотвратить вход в помещение лиц, не являющихся сетевыми администраторами медицинского учреж- дения, чтобы избежать удаления сетевого оборудования меди- цинского учреждения, почтовых серверов или их дисков предот- вращая присутствие неавторизованных лиц.	3 > 2	3	1	9 > 6
							Уничтожение (угроза Д) оборудования цен- тра удаленного техни- ческого обслуживания приводит к потере Д к СУО.	Управление ключами защиты может предот- вратить недоступность службы, вызванную уничтожением обо- рудования, предотвра- щая доступ к оборудо- ванию неавторизован- ных лиц.	3 > 2	2	1	6 > 4
				47	D1	n	Уничтожение (угроза Д) природоохранного средства для сетевого оборудования меди- цинского учреждения приводит к потере Д к СУО.	Управление ключами защиты может предот- вратить недоступность службы, вызванную уничтожением обо- рудования, предотвра- щая доступ к оборудо- ванию неавторизован- ных лиц.	3 > 2	2	1	6 > 4

32 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				54	E1	d	Если лечащий врач оставляет актив для дальнейшей работы, удаление (угроза К) на участке третьими лицами, то персоналом медицинского учреждения, сетевыми администраторами медицинского учреждения, основного технического персонала других компаний, основного технического персонала или системного администратора медицинского учреждения приводит к раскрытию персональной медицинской информации.	Управление ключами защиты может предотвратить доступ к информационным носителям третьим лицам, персоналу медицинского учреждения, сетевым администраторам медицинского учреждения, основному техническому персоналу других компаний, основному техническому персоналу или системному администратору медицинского учреждения, чтобы избежать удаление информации на носителях.	3 > 2	3	1	9 > 6
				56	E1	f	Удаление (угроза К) оборудования, подлежащего техническому обслуживанию лицами, не являющимися системными администраторами медицинского учреждения, и его дисков приводит к раскрытию персональной медицинской информации.	Удаление (угроза К) оборудования, подлежащего техническому обслуживанию лицами, не являющимися системными администраторами медицинского учреждения, и его дисков приводит к раскрытию К персональной медицинской информации.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				57	E1	f	Уничтожение (угроза Д) оборудования, подлежащего техническому обслуживанию, приводит к потере Д к СУО.	Управление ключами защиты может предотвратить недоступность службы, вызванную уничтожением оборудования, предотвращая доступ к оборудованию неавторизованных лиц.	3 > 2	2	1	6 > 4
				58	E1	g	Уничтожение (угроза Д) природоохранного средства для оборудования, подлежащего техническому обслуживанию, приводит к потере Д к СУО.	Управление ключами защиты может предотвратить недоступность службы, вызванную уничтожением, предотвращая доступ к оборудованию неавторизованных лиц.	3 > 2	2	1	6 > 4
		Должна быть разработана и применена физическая защита против ущерба от огня, наводнения, землетрясения, взрыва, общественных беспорядков и других форм естественного или искусственного бедствия.		—	—	—	—	—	—	—	—	—
		Должна быть разработана и применена физическая защита офисов, комнат и оборудования. Должна быть разработана и применена физическая защита		13	A1	c	Если соответствующий актив оставлен для ремонта или по причине невозможности его отсоединения, то удаление (угроза К) страниц техническим персоналом центра	Управление ключами защиты несколькими лицами может ограничить технический персонал центра удаленного технического обслуживания от входа в помещения при	3 > 2	3	1	9 > 6

3.4 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			и руководящие принципы для работы в зонах безопасности.	14	A1	d	удаленного технического обслуживания приводит к раскрытию персональной медицинской информации. Если соответствующий актив оставлен для ремонта или по причине невозможности его отсоединения, то удаление (угроза К) страниц техническим персоналом центра удаленного технического обслуживания приводит к раскрытию персональной медицинской информации.	отсутствии других членов, предотвращая удаление бумажных страниц.	3 > 2	3	1	9 > 6
				16	A1	f	Удаление (угроза К) оборудования центра удаленного технического обслуживания и дисков техническим персоналом центра удаленного технического обслуживания приводит к раскрытию персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить удаление оборудования центра удаленного технического обслуживания и дисков сетевыми администраторами центра удаленного технического обслуживания, предотвращая доступ авторизованных лиц при отсутствии других пользователей.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				21	В1	И	Прослушивание (угроза К) в сети центра удаленного технического обслуживания из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.	Проверка внутреннего маршрута со стороны центра удаленного технического обслуживания, чтобы обнаружить следы прослушивания маршрута.	3 > 2	3	1	9 > 6
							Прослушивание (угроза К) в сети центра удаленного технического обслуживания из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.	Проверка внутреннего маршрута со стороны центра удаленного технического обслуживания несколькими лицами, чтобы обнаружить следы прослушивания маршрута несколькими лицами.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				21	B1	i	Подглядывание (угроза К) через сетевое оборудование центра удаленного технического обслуживания сетевым администратором центра удаленного технического обслуживания приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.	Управление ключами защиты нескольких лиц может ограничить доступ к дискам сетевым администраторам центра удаленного технического обслуживания других лиц и предотвратить раскрытие персональной медицинской информации посредством сетевого оборудования центра удаленного технического обслуживания, предотвращая доступ авторизованных лиц к диску в отсутствие других лиц.	3 > 2	3	1	9 > 6
				22	B1	j	Если соответствующий актив оставлен для ремонта или контроля, удаление (угроза К) бумажных страниц сетевым администратором центра удаленного технического обслуживания приводит к раскрытию персональной медицинской информации.	Управление входом в помещение (с отдельной коммуникационной трассой) несколькими лицами может предотвратить вход в помещение сетевого администратора центра удаленного технического обслуживания при отсутствии других лиц, и ограничить удаление бумажных страниц, предотвращая вход в помещение авторизованных лиц в отсутствие других лиц.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				23	B1	k	Если соответствующий актив оставлен для ремонта или контроля, удаление (угроза К) бумажных страниц сетевым администратором центра удаленного технического обслуживания приводит к раскрытию К персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить доступ к дискам сетевым администраторам центра удаленного технического обслуживания при отсутствии других лиц, предотвращая доступ авторизованных лиц к диску без присутствия других лиц.	3 > 2	3	1	9 > 6
				25	B1	m	Удаление (угроза К) оборудования центра удаленного технического обслуживания, почтовых серверов и их дисков сетевым администратором центра удаленного технического обслуживания приводит к раскрытию персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить доступ к сетевому оборудованию, почтовым серверам и их дискам сетевыми администраторами центра удаленного технического обслуживания, предотвращая доступ авторизованного лица при отсутствии других пользователей.	3 > 2	3	1	9 > 6
				41	D1	P	Прослушивание (угроза К) в сети медицинского учреждения из внутреннего источника лицом, не являющимся сетевым администратором медицинского учреждения, приводит к неавторизованному использованию (угроза К)	Проверка внутреннего маршрута со стороны медицинского учреждения обнаруживает следы прослушивания маршрута.	3 > 2	3	1	9 > 6

38 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участки	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию информации.					
				41	D1	P	Прослушивание (угроза К) в сети медицинского учреждения из внутреннего источника сетевым администратором медицинского учреждения приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	Проверка внутреннего маршрута со стороны медицинского учреждения несколькими лицами обнаруживает следы прослушивания на маршруте несколькими лицами.	3 > 2	3	1	9 > 6
							Подглядывание (угроза К) посредством сетевого оборудования медицинского учреждения сетевым администратором медицинского учреждения приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию информации.	Управление ключами защиты несколькими лицами может ограничить доступ к дискам сетевых администраторов в медицинского учреждения в отсутствии других лиц и предотвратить раскрытие персональной медицинской информации посредством сетевого оборудования медицинского учреждения, предотвращая доступ авторизованных лиц к диску без присутствия других лиц.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				42	D1	i	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление бумажных страниц (угроза К) сетевым администратором медицинского учреждения приводит к раскрытию персональной медицинской информации.	Управление входом в помещение (с отдельной коммуникационной трассой) несколькими лицами может предотвратить вход в помещение сетевым администраторам медицинского учреждения при отсутствии других лиц и ограничить удаление бумажных страниц, предотвращая вход в помещение авторизованных лиц при отсутствии других лиц.	3 > 2	3	1	9 > 6
				43	D1	k	Если соответствующий актив оставлен для ремонта или контроля, то удаление (угроза К) бумажных страниц сетевым администратором медицинского учреждения приводит к раскрытию персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить доступ к дискам сетевым администраторам центра удаленного технического обслуживания при отсутствии других лиц, предотвращая доступ авторизованных лиц к диску без присутствия других лиц.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				45	D1	m	Удаление (угроза К) серверов, почтовых серверов и их дисков сетевым администратором медицинского учреждения приводит к раскрытию персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить доступ к сетевому оборудованию, подключенным к серверам и их дискам сетевыми администраторами медицинского учреждения, предотвращая доступ авторизованного лица при отсутствии других пользователей.	3 > 2	3	1	9 > 6
				54	E1	d	Вывоз (угроза К) или замена активизированных печатных форм врачом приводит к раскрытию или фальсификации персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить взаимодействие врача с информационной средой на диске в отсутствие других членов организации (в одиночку), чтобы предотвратить авторизованному лицу взаимодействие с информационной средой при отсутствии других лиц.	3 > 2	3	1	9 > 6
				56	E1	f	Удаление (угроза К) или изменение (угроза Ц) оборудования, подлежащего техническому обслуживанию системными администраторами медицинского учреждения, и его дисков приводит к	Управление ключами защиты несколькими лицами может ограничить удаление оборудования, подлежащего техническому обслуживанию, и его дисков сетевыми администраторами медицинского	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							раскрытию или фальсификации персональной медицинской информации.	учреждения, предоставляющая доступ к данным авторизованных лиц при отсутствии других лиц.				
			Места доступа, такие как зоны поставки и загрузки, а также другие места, где не имеющие разрешения лица могут войти в помещения, должны управляться и, если возможно, должны быть изолированы от средств, обрабатывающих информацию, с целью избежать неразрешенного доступа.	—	—	—	—	—	—	—	—	—
А.9 Физическая безопасность и охрана окружающей среды	А.9.2 Защита оборудования	Предотвратить гибель, ущерб, кражу или расхищение активов и сбои в деятельности организации.	Оборудование должно быть размещено или защищено так, чтобы снизить риски от угроз и опасностей окружающей среды, а также количество возможностей неразрешенного доступа.	18	А1	f	Анализ (угроза К) утечки электромагнитных волн, исходящих от оборудования центра удаленного технического обслуживания, приводит к раскрытию персональной медицинской информации.	Обеспечивая наличие расстояния между местонахождением оборудования центра удаленного технического обслуживания и дорогой, можно предотвратить раскрытие персональной медицинской информации, предотвращая прием электромагнитных волн утечки.	3 > 2	3	1	9 > 6

42 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				25	B1	m	Несанкционированное вмешательство (угроза К) в сетевое оборудование центра удаленного технического обслуживания приводит к непредвиденному раскрытию персональной медицинской информации.	Предусмотрено блокирование при обнаружении следов несанкционированного вмешательства.	3 > 2	3	1	9 > 6
							Анализ (угроза К) утечки электромагнитных волн, исходящих от сетевого оборудования центра удаленного технического обслуживания или кабелей, приводит к раскрытию персональной медицинской информации.	Обеспечивая наличие расстояния между местонахождением оборудования центра удаленного технического обслуживания и дорогой, можно предотвратить раскрытие персональной медицинской информации, предотвращая прием электромагнитных волн утечки.	3 > 2	3	1	9 > 6
				45	D1	m	Несанкционированное вмешательство (угроза К) в сетевое оборудование медицинского учреждения приводит к непредвиденному раскрытию персональной медицинской информации.	Предусмотрено блокирование при обнаружении следов несанкционированного вмешательства.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				45	D1	m	Анализ (угроза К) утечки электромагнит- ных волн от сетевого оборудования меди- цинского учреждения приводит к раскрытию персональной меди- цинской информации.	Обеспечивая наличие расстояния между ме- стонахождением се- тевого оборудования медицинского учреж- дения и дорогой, мож- но предотвратить рас- крытие персональной медицинской инфор- мации, предотвращая прием электромагнит- ных волн утечки.	3 > 2	3	1	9 > 6
				56	E1	f	Несанкционирован- ное вмешательство (угроза К) в оборудо- вание, подлежащее техническому обслу- живанию, приводит к непредвиденному рас- крытию персональной медицинской инфор- мации.	Предусмотрено блокирование при обнаружении следов несанкционированного вмешательства.	3 > 2	3	1	9 > 6
							Анализ утечки (угроза К) электромаг- нитных волн от обору- дования, подлежащего техническому обслу- живанию, приводит к рас- крытию персональной медицинской инфор- мации.	Обеспечивая наличие расстояния между местонахождением оборудования, подле- жащего техническому обслуживанию, и до- рогой, можно предот- вратить раскрытие персональной меди- цинской информации. предотвращая прием электромагнитных волн утечки.	3 > 2	3	1	9 > 6

44 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Оборудование должно быть защи- щено от нарушений энергоснабжения и других нарушений, вызванных сбоями во вспомогательном оборудовании.	—	—	—	—	—	—	—	—	—
			Источник энергии и кабели связи, по которым передаются данные или вспомо- гательные инфор- мационные услуги, должны быть защи- щены от перехвата или повреждения.	—	—	—	—	—	—	—	—	—
			Оборудование должно проходить соответствующее техническое об- служивание, чтобы гарантировать его долгосрочную до- ступность и целост- ность.	—	—	—	—	—	—	—	—	—
			Оборудование, информация или программное обе- спечение не долж- ны выноситься за пределы помещений организации без предварительного разрешения.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Все единицы обслуживания, содержащие информацию, должны быть проверены, чтобы гарантировать, что любые уязвимые данные и лицензированное программное обеспечение было удалено или надежно перезаписано перед ликвидацией.	11	A1	а	Если технический персонал центра удаленного технического обслуживания забывает удалить персональную медицинскую информацию на участке, это приводит к непредвиденному раскрытию информации.	Автоматическое стирание во время выхода из системы устраняет необходимость наложения технического персонала удаленного технического обслуживания персональной медицинской информации, таким образом, снижая риск ошибки, связанной с человеческим фактором.	3 > 2	3	1	9 > 6
A.9 Физическая безопасность и охрана окружающей среды	A.9.2 Защита оборудования	Избегать потерь, ущерба, краж или расхищения ресурсов и объектов деятельности организации.	Оборудование, информация или программное обеспечение не должны выноситься за пределы помещений организации без предварительного разрешения. Защита должна быть применена к оборудованию вне помещений, с учетом различных рисков работы за пределами помещений организации. Необходимо применять политику чистого стола в отношении бумаг и накопителей информации, а также политику	53	E1	с	Если лечащий врач оставляет соответствующий актив для своей работы, то просмотр или удаление (угроза К) на участке третьими лицами, персоналом медицинского учреждения, системными администраторами административного медицинского учреждения, основным техническим персоналом других компаний, основным техническим персоналом или системными администраторами медицинского учреждения, предотвращая оставление ресурса без присмотра.	Очистка диска может предотвратить просмотр или удаление бумажных страниц третьими лицами, персоналом медицинского учреждения, системными администраторами медицинского учреждения, основным техническим персоналом других компаний, основным техническим персоналом или системными администраторами медицинского учреждения, предотвращая оставление ресурса без присмотра.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менеджмент средств связи и эксплуатации	А.10.1 Процедуры эксплуатации и ответственность	Гарантировать правильную и безопасную работу средств, обрабатывающих информацию.	чистого экрана в отношении устройств обработки информации (А.11.3.3).	—	—	—	—	—	—	—	—	—
			Процедуры эксплуатации должны быть документированы, поддерживаться в рабочем состоянии, и быть доступными для всех пользователей, которым они нужны.	15	А1	е	Установка программных закладок или программ хищения информации (угроза Ц) приводит к раскрытию персональной медицинской информации.	Группа по расследованию инцидентов (ГРИ) быстро устраняет ущерб, вызванный программными закладками или программами хищения информации, благодаря противовирусным мерам. Противовирусные меры могут обнаружить и удалить программные закладки или программы хищения информации.	3 > 2	3	2	18 > 12
			Изменения в средствах и системах, обрабатывающих информацию, должны управляться.	21	В1 В2	и	Несанкционированный вход (угроза К) при помощи атаки с «перехватом по словарю» в сетевое оборудование центра удаленного технического обслуживания из внешнего	Создается группа по расследованию инцидентов (ГРИ) для ускорения восстановления ущерба, вызванного неавторизованным доступом.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							источника любым лицом приводит к не- авторизованному ис- пользованию (угроза К) персональной ме- дицинской информа- ции, хранимой в сети центра удаленного технического обслужи- вания, и к раскрытию информации.	Контроль маршрута (без подключения к оборудованию центра удаленного техниче- ского обслуживания) предотвращает уда- ленное подключение к оборудованию центра удаленного техниче- ского обслуживания. Общие меры админи- стрирования сети для сетевого оборудова- ния центра удаленного технического обслужи- вания включают в себя контроль доступа (ин- формации при входе в систему), особенно на выходе центра уда- ленного технического обслуживания, раз- деление сети / прину- дительный путь (FW) / фильтрацию и защиту порта удаленной диа- гностики.	3 > 2	3	2	18 > 12
				24	В1	I	Установка програм- мных закладок или программ хищения информации (угроза Ц) приводит к раскрытию персональной меди- цинской информации.	Группа по расследова- нию инцидентов (ГРИ) быстро устраняет ущерб, вызванный программными заклад- ками или программами хищения информации, благодаря противоре- чественным мерам.				

48 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
								Противовирусные меры могут обнару- жить и удалить про- граммные закладки или программы хище- ния информации.				
				41	D1	p	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» в сетевое оборудование медицинского учреж- дения из внешнего источника лицами, не входящими в состав персонала центра уда- ленного технического обслуживания, вклю- чая персонал центров удаленного техниче- ского обслуживания других компаний, при- водит к неавторизован- ному использованию (угроза К) персональ- ной медицинской ин- формации, хранимой в сети центра уда- ленного технического обслуживания, и к рас- крытию информации.	Создается группа по расследованию инци- дентов (ГРИ) для уско- рения восстановления ущерба, вызванного неавторизованным доступом. Общие меры админи- стрирования сети для сетового оборудова- ния центра удаленного технического обслужи- вания включают в себя контроль доступа (ин- формации при входе в систему), особенно на выходе центра уда- ленного технического обслуживания, раз- деление сети / прину- дительный путь (FW) / фильтрацию и защиту порта удаленной диа- гностики.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				44	D1	I	Установка программных закладок или программ хищения информации (угроза Ц) приводит к раскрытию персональной медицинской информации.	Группа по расследованию инцидентов (ГРИ) быстро устраняет ущерб, вызванный программными закладками или программами хищения информации, благодаря противовирусным мерам. Противовирусные меры могут обнаружить и удалить программные закладки и программы хищения информации.	3 > 2	3	2	18 > 12
			Обязанности и обязанности ответственные должны быть разделены, с целью снизить количество возможностей не-разрешенного или непреднамеренного изменения или не-правильного использования активов организации.	—	—	—	—	—	—	—	—	—
			Средства разработки, испытания и эксплуатации должны быть разделены для снижения риска неавторизованного доступа или внесения изменений в операционную систему.	16	A1	f	Несанкционированный вход (угроза К) в оборудование центра удаленного технического обслуживания приводит к непредвиденному раскрытию персональной медицинской информации.	Предусмотрено блокирование при обнаружении следов несанкционированного вмешательства.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСОМЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менедж- мент средств связи и эксплуа- тации	А.10.2 Управле- ние пред- ставлен- ем услуг третьей стороной.	Реализовать и поддерживать подходящий уровень ин- формационной безопасности и предоста- вления услуг в соответствии с сопоставлениями о предоставлении услуг тре- тей стороной.	Должно быть гаран- тировано, что сред- ства управления безопасностью, опи- сания услуг и уровни предоставления, включенные в согла- шение о предостав- лении услуг третьей стороны, реализуют- ся, эксплуатируются и поддерживаются третьей стороной.	—	—	—	—	—	—	—	—	—
			Услуги, отчеты и за- писи, представле- мые третьей сторо- ной, должны постоянно контролироваться и анализироваться; регулярно должны проводиться аудиты.	—	—	—	—	—	—	—	—	—
			Должен осущест- вляться менедж- мент изменений в предоставлении услуг, включая под- держание в рабочем состоянии и улучше- ние существующей политики, процедур и средств управления в области защиты информации, с уче- том критичности во- влеченных деловых систем и процессов и переоценки рисков.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
	А.10.3 Планирование и приемка систем	Минимизировать риск системных сбоев.	Использование ресурсов должно постоянно контролироваться, регулироваться, и должны делаться прогнозы будущих требований производительности, чтобы гарантировать требуемые характеристики работы системы.	—	—	—	—	—	—	—	—	—
			Должны быть созданы критерии приемки новых информационных систем, усовершенствований и новых версий, и должны быть выполнены подходящие испытания системы(систем) в ходе разработки и перед приемкой.	—	—	—	—	—	—	—	—	—
А.10 Менеджмент средств связи и эксплуатации	А.10.4 Защита от злоупотребления мобильного кодирования	Обеспечить целостность программного обеспечения и информации.	Должны быть реализованы средства управления обнаружением, предотвращением и восстановлением, имеющие целью защитить от злонамеренного кодирования, а также надлежащие процедуры [повышения] осведомленности пользователей.	15	А1	е	Установка программных закладок или программ хищения информации (угроза Ц) приводит к раскрытию персональной медицинской информации.	Группа по расследованию инцидентов (ГРИ) быстро устраняет ущерб, вызванный программными закладками или программами хищения информации, благодаря противовирусным мерам. Противовирусные меры могут обнаружить и удалить программные закладки и программы хищения информации.	3 > 2	3	2	18 > 12
				24	В1	1						
				44	Д1							
				55	Е1	е						

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Если использование мобильного кодирования разрешено, то конфигурация должна гарантировать, что разрешенное мобильное кодирование работает в соответствии с четко определенной политикой защиты, а выполнение неразreshенного мобильного кодирования должно быть предотвращено.	17	A1	f	Отказ (угроза Д) обслуживания центра удаленного технического обслуживания приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.	3 > 2	2	2	12 > 8
	A.10.5 Резервное копирование данных	Поддерживать целостность и доступность информации и средств обработки информации.	Резервные копии информации и программного обеспечения должны регулярно сниматься и проверяться в соответствии с согласованной политикой резервного копирования.	18	A1	g	Отказ (угроза Д) обслуживания центра удаленного технического обслуживания приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				
				26	B1 B2	m	Отказ (угроза Д) серверного оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				27	B1 B2	n	Отказ (угроза Д) или отсоединение кабеля (угроза Д) природоох- ранного средства от сетевых оборудования медицинского учреж- дения приводит к по- тере Д к СУО.	Техническое обслужи- вание, контрольные проверки и резервиро- вание данных может предотвратить недо- ступность служб.				
				46	D1	m	Отказ (угроза Д) сете- вого оборудования ме- дицинского учрежде- ния приводит к потере Д к СУО.	Техническое обслужи- вание, контрольные проверки и резервиро- вание данных может предотвратить недо- ступность служб.				
				47	D1	n	Отказ (угроза Д) или отсоединение кабеля Д природоох- ранного средства от сетевых оборудования медицинского учреж- дения приводит к по- тере Д к СУО.	Техническое обслужи- вание, контрольные проверки и резервиро- вание данных может предотвратить недо- ступность служб.				
				57	E1	f	Отказ (угроза Д) обору- дования, подлежащего техническому обслу- живанию, приводит к потере Д к СУО.	Техническое обслужи- вание, контрольные проверки и резервиро- вание данных может предотвратить недо- ступность служб.				
				58	E1	g	Отказ (угроза Д) при- родоохранного обо- рудование, для обору- дования, подлежащего техническому обслу- живанию, приводит к потере Д к СУО.	Техническое обслужи- вание, контрольные проверки и резервиро- вание данных может предотвратить недо- ступность служб.				

54 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менедж- мент средств связи и эксплуа- тации	А.10.6 Менедж- мент без- опасности сети	Обеспечить информацион- ную безопас- ность в сетях и защиту под- держивающей инфраструк- туры.	Должны осущест- вляться адекватный менеджмент сети и адекватное управле- ние сетью для того, чтобы сеть была защищена от угроз и для того, чтобы поддерживать в рабочем состоянии защиту для систем и приложений, исполь- зующих сеть, вклю- чая информацию в пути. Характеристики за- щиты, уровни услуги и требования менед- жмента всех сетевых служб должны быть выявлены и включе- ны в любое согла- шение по сетевым услугам, независимо от того, предостав- ляются ли эти услуги внутренне или берутся из внешних источников.	27	В2	И	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» в сетевое оборудование центра удаленного технического обслужи- вания из внутреннего источника лицом, не являющимся сетевым администратором цен- тра удаленного техни- ческого обслуживания, приводит к неавторизи- рованному использованию (угроза К) персон- альной медицинской информации, храня- мой в сети центра уда- ленного технического обслуживания, и к рас- крытию информации.	Управление привле- чениями (вход в систему в качестве пользова- теля/привилегирован- ного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для вхо- да в систему) может предотвратить несанк- ционированный вход лиц, не являющихся сетевыми администра- торами центра уда- ленного технического обслуживания.	1	3	1	3
							Взлом (угроза К) се- тевой инфраструктуры центра удаленного технического обслу- живания при помощи незаконно полученного пароля из внутреннего источника лицом, не являющимся сетевым администратором цен- тра удаленного техни- ческого обслуживания, приводит к неавторизи- рованному использованию (угроза К)	Периодическое из- менение пароля превращает взлом сетевой инфраструк- туры центра удаленного технического обслужи- вания.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	ИД	Участки	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.					
							Прослушивание (угроза К) в сети центра удаленного технического обслуживания из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.	Проверка внутреннего маршрута на стороне центра удаленного технического обслуживания, чтобы обнаружить следы прослушивания маршрута.				
							Прослушивание (угроза К) в сети центра удаленного технического обслуживания из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.	Проверка внутреннего маршрута на стороне центра удаленного технического обслуживания несколькими лицами, чтобы обнаружить следы прослушивания маршрута несколькими лицами.				

56 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							использованию (угроза К) персональ- ной медицинской ин- формации, хранимой в сети центра уда- ленного технического обслуживания, и к рас- крытию информации.					
							Подглядывание (угро- за К) через сетевое оборудование центра удаленного техниче- ского обслуживания сетевым администра- тором центра удален- ного технического об- служивания приводит к неавторизованному использованию (угроза К) персональной меди- цинской информации, хранимой в сети цен- тра удаленного техни- ческого обслуживания, и к раскрытию инфор- мации.	Управление ключами защиты нескольких лицами может ограничить доступ к дискам сетевым адми- нистраторам центра удаленного техниче- ского обслуживания в отсутствии других лиц и предотвратить рас- крытие персональной медицинской инфор- мации посредством сетевого оборудова- ния центра удаленного технического обслужи- вания, предотвращая, тем самым, доступ авторизованных лиц к дискету без присутствия иных лиц.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менеджмент средств связи и эксплуатации	А.10.6 Менеджмент безопасности сети	Обеспечить информационную безопасность в сетях и защиту под- держивающей инфраструк- туры.	Должны осу- ществляться адекватный менеджмент сети и адекватное управле- ние сетью для того, чтобы сеть была за- щищена от угроз и для того, что- бы поддерживать в рабочем состоянии защиту для систем и приложений, исполь- зующих сеть, вклю- чая информацию в пути. Характеристики за- щиты, уровни услуги и требования менед- жмента всех сетевых служб должны быть выявлены и включе- ны в любое согла- шение по сетевым услугам, независимо от того, предостав- ляются ли эти ус- луги внутренне или берутся из внешних источников.	22	В2	У	Если соответствующий актив оставлен для ремонта или контро- ля, то просмотр или удаление (угроза К) страниц лицами, не являющимися сетевы- ми администраторами центра удаленного технического обслужи- вания, приводит к рас- крытию персональной медицинской инфор- мации.	Утилизация шредером может предотвратить просмотр или удале- ние страниц сетевыми администраторами центра удаленного технического обслужи- вания. Управление входом в помещение (с от- дельной коммуни- кационной трассой) может ограничить вход в помещение лиц, не являющихся сетевыми администраторами центра удаленного технического обслу- живания, и предот- вратить просмотр или удаление страниц, предотвращая присут- ствие неавторизован- ных лиц.	1	3	1	3
							Если соответствующий актив оставлен для ремонта или контроля, то удаление (угроза К) бумажных страниц са- етвым администрато- ром центра удаленного технического обслужи- вания приводит к рас- крытию персональной медицинской инфор- мации.	Управление входом в помещение (с отдель- ной коммуникацион- ной трассой) несколь- кими лицами может предотвратить вход в помещение сетевого администратора цен- тра удаленного техни- ческого обслуживания при отсутствии дру- гих лиц, и ограничить уда- ление бумажных				

58 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				23	B2	k	Если соответствующий актив оставлен для ремонта или контроля, удаление (угроза К) бумажных страниц лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, приводит к раскрытию персональной медицинской информации.	Проверка внутреннего маршрута со стороны центра удаленного технического обслуживания, чтобы обнаружить следы прослушивания маршрута.	страниц, предотвращая вход в помещение авторизованных лиц в отсутствие других лиц.			
							Если соответствующий актив оставлен для ремонта или контроля, то удаление (угроза К) бумажных страниц сетевым администратором центра удаленного технического обслуживания приводит к раскрытию персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить доступ к дискам для сетевых администраторов центра удаленного технического обслуживания при отсутствии других лиц, предотвращая доступ авторизованных лиц к диску без присутствия других лиц.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				24	B2	I	Установка программных закладок или программ хищения информации (угроза Ц) приводит к раскрытию персональной медицинской информации.	Группа по расследованию инцидентов (ГРИ) быстро устраняет ущерб, вызванный программными закладками или программами хищения информации, благодаря противовирусным мерам. Противовирусные меры могут обнаружить и удалить программные закладки и программы хищения информации.	1	3	2	6
A.10 Менеджмент средств связи и эксплуатации	A.10.6 Менеджмент безопасности сети	Обеспечить информационную безопасность в сетях и защиту поддерживающей инфраструктуры.	Должны осуществляться адекватный менеджмент сети и адекватное управление сетью для того, чтобы сеть была защищена от угроз и для того, чтобы поддерживать в рабочем состоянии защиту для систем и приложений, использующих сеть, включая информацию в пути.	25	B2	m	Удаление (угроза К) оборудования центра удаленного технического обслуживания, почтовых серверов и их дисков лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, приводит к раскрытию (угроза К) персональной медицинской информации.	Управление ключами защиты может предотвратить удаление серверов почтовых серверов или дисков центра удаленного технического обслуживания лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, предотвращая доступ неавторизованным лицам.	1	3	1	3
			Характеристики защиты, уровни защиты, и требования менеджмента всех сетевых служб должны быть	—	—	—	—	—	—	—	—	—

60 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			выявлены и включены в любое соглашение по сетевым услугам, независимо от того, предоставляются ли эти услуги внутренне или берутся из внешних источников.									
							Удаление (угроза К) оборудования центра удаленного технического обслуживания, почтовых серверов и их дисков сетевым администратором центра удаленного технического обслуживания приводит к раскрытию (угроза К) персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить доступ к сетевому оборудованию, почтовым серверам и их дискам для сетевых администраторов центра удаленного технического обслуживания, предотвращая доступ неавторизованным лицам при отсутствии других лиц.				
							Несанкционированное вмешательство (угроза К) в сетевое оборудование центра удаленного технического обслуживания приводит к непредвиденному раскрытию (угроза К) персональной медицинской информации.	Предусмотрено блокирование при обнаружении следов несанкционированного вмешательства.				
							Анализ утечки электромагнитных волн (угроза К), исходящих	Обеспечивая наличие расстояния между месторасположением				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							от сетевого оборудования центра удаленного технического обслуживания или кабелей, приводит к раскрытию (угроза К), персональной медицинской информации.	сетевого оборудования центра удаленного технического обслуживания и дорожной, можно предотвратить раскрытие персональной медицинской информации, предотвращая прием электромагнитных волн утечки.				
				28	B2	0	Неверная установка (угроза К) приводит к неожиданному раскрытию (угроза К) персональной медицинской информации.	Тренинги и стандарты навыков могут предотвратить перебои в работе, вызванные неверным вводом или случайным удалением, поддерживая и повышая квалификацию операторов.				
	A.10.7 Обработка носителей информации	Предотвращать неразрешенное разглашение, изменение, удаление или уничтожение активов, а также прерывание деловых операций.	Должны быть приняты процедуры менеджмента съемных носителей информации. Если носитель больше не требуется, то он должен быть ликвидирован надежно и безопасно, используя формальные процедуры.	13	A1	с	Если лечащий врач оставляет соответствующий актив для ремонта или по причине невозможности его отсоединения, то это может вызвать просмотр или удаление (угроза К) бумажных страниц третьими лицами, персоналом или сетевыми	Утилизация шредером может предотвратить просмотр или удаление страниц третьими лицами, персоналом или сетевыми администраторами центра удаленного технического обслуживания. Управление входом в помещение может ограничить вход	3 > 2	3	1	9 > 6

62 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менед- жмент средств связи и эксплуа- тации	А.10.7 Об- работка носителей информа- ции	Предотвращать неразрешенное разглашение, изменение, удаление или уничтожение активов, а также прерывание деловых операций.	Если носитель больше не требуется, то он должен быть ликвидирован надежно и безопасно, используя формальные процедуры.	22	В1	И	администраторами центра удаленного технического обслуживания, приводя к раскрытию (угроза К) персональной медицинской информации.	в помещении третьих лиц, персонала или сетевых администраторов центра удаленного технического обслуживания и бло-кирование просмотра или удаление бумажных страниц.	3 > 2	3	1	9 > 6
							Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление (угроза К) бумажных страниц лицами, не являющимися сетевыми администраторами центра удаленного технического обслуживания, приводит к раскрытию (угроза К) персональной медицинской информации.	Утилизация шредером может предотвратить просмотр или удаление страниц сетевыми администраторами центра удаленного технического обслуживания. Управление входом в помещение (с отдельной коммуникационной трассой) может ограничить вход в помещение лицам, не являющимся сетевыми администраторами центра удаленного технического обслуживания и предотвратить просмотр или удаление страниц, не допускающая присутствие неавторизованных лиц.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участки	Активы	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				42	D1	i	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или изъятие бумажных страниц (угроза К) лицами, не являющимися сетевыми администраторами медицинского учреждения, приводит к раскрытию (угроза К) персональной медицинской информации.	Утилизация шредером может предотвратить просмотр или изъятие страниц лицами, не являющимися сетевыми администраторами медицинского учреждения. Управление входом в помещение (с отдельной коммуникционной трассой) может ограничить вход в помещение лиц, не являющихся сетевыми администраторами медицинского учреждения и предотвращает просмотр или изъятие страниц, не допуская присутствие неавторизованных лиц.	3 > 2	3	1	9 > 6
			Должны быть созданы процедуры для обработки и хранения информации, с целью защитить эту информацию от неразрешенного разглашения или неправомерного использования.	—	—	—	—	—	—	—	—	—
			Системная документация должна быть защищена от неразрешенного доступа.	—	—	—	—	—	—	—	—	—

34 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менед- жмент средств связи и эксплуа- тации	А.10.8 Обмен информа- цией А.10.9 Службы электрон- ной тор- говли	Поддерживать защиту ин- формации и программного обеспечения, обменивае- мых в рамках организации и со сторонними компаниями. Гарантировать защиту услуг электронной торговли, а также их без- опасное ис- пользование.	Между организа- цией и внешними сторонами должны быть установлены соглашения для об- мена информацией и программным обе- спечением.	—	—	—	—	—	—	—	—	—
А.10 Менед- жмент средств связи и эксплуа- тации	А.10.8 Обмен информа- цией А.10.9 Службы электрон- ной тор- говли	Поддерживать защиту ин- формации и программного обеспечения, обменивае- мых в рамках организации и со сторонними компаниями. Гарантировать защиту услуг электронной торговли, а также их без- опасное ис- пользование.	Носитель, содержа- щий информацию, должен быть за- щищен от нераз- решенного доступа, неправильного использования или порчи в ходе транс- портировки за фи- зические границы организации. Информация, во- влеченная в сделки в режиме онлайн, должна быть за- щищена для того, чтобы предотвратить неполную передачу, неправильную марш- рутизацию.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			неразрешенное изменение сообщения, неразрешенное разглашение, неразрешенное дублирование или повторное воспроизведение сообщения. Информация, вовлеченная в электронную торговлю, предоставляющая через общедоступные сети, должна быть защищена от мошеннической деятельности, споров по договору и неразрешенного разглашения и изменения.									
			Должны быть приняты официальная политика обмена, процедуры обмена и средства управления обменом, чтобы защитить обмен информации через использование всех типов средств связи.				—	—	—	—	—	—
			Информация, включенная в электронный обмен сообщениями, должна быть защищена надлежащим образом.				—	—	—	—	—	—

66 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Целостность информации, сделанной доступной в общедоступной системе, должна быть защищена для того, чтобы предотвратить неразрешенное изменение.									
			Должны быть разработаны и внедрены политика и процедуры, с целью защитить информацию, связанную с взаимосвязанностью систем деловой информации.									
А.10 Менеджмент связи и эксплуатации	А.10.10 Постоянный контроль	Обнаруживать неавторизованную деятельность по обработке информации.	Контрольные журналы, записывающие деятельность пользователей, исключения и события в системе защиты информации, должны генерироваться и храниться в течение согласованного периода, с целью помочь в будущих расследованиях и в постоянном контроле над управлением доступом. Средства ведения журнала и информация журнала должны	11	А1	а	Неавторизованное использование (угроза К) техническим персоналом центра удаленного технического обслуживания персональной медицинской информации и оборудования центра удаленного технического обслуживания на участке приводит к угрозе раскрытия информации.	Внутренний аудит записей может обнаружить неавторизованное использование персональной медицинской информацией техническим персоналом центра удаленного технического обслуживания. Кроме того, может быть также обнаружено неавторизованное использование персональной медицинской информацией техническим персоналом центра удаленного технического обслуживания, так как	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			быть защищены от подделки и неразрешенного доступа. Деятельность системного администратора и системного оператора должна вноситься в журнал. Неисправности должны регистрироваться в журнале, анализироваться, и должно предприниматься соответствующее действие.					внутренний аудит запрещает осуществление противозаконной работы. Проверки конфиденциальности и накопление опыта (подтверждение квалификации) могут ограничить неавторизованное использование технических средств персоналом центра СУО посредством предотвращения противозаконной деятельности операторов. Ведение записей (лиц, запрашивающих действия, типы, даты и т. д.) в сочетании с внутренним аудитом.				
А.10 Менеджмент средств связи и эксплуатации	А.10.10 Постоянный контроль	Обнаруживать неавторизованную деятельность по обработке информации.	Контрольные журналы, записывающие деятельность пользователей и события в системе защиты информации, должны генерироваться и храниться в течение согласованного периода, с целью помочь в будущих расследованиях и в постоянном контроле над управлением доступом.	12	А1	а	Неавторизованное использование (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания персоналом и внутриприводит к угрозе раскрытия информации.	Внутренний аудит записей может обнаружить неавторизованное использование технических персоналом центра удаленного технического обслуживания. Кроме того, неавторизованное использование технического персоналом центра удаленного технического обслуживания может быть также обнаружено, так как внутренний аудит запрещает				

88 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Средства ведения журнала и Информа- ция журнала должны быть защищены от подделки и неразре- шенного доступа. Деятельность адми- нистратора и си- стемного оператора должна вноситься в журнал. Неисправности должны регистриро- ваться в журнале, анализироваться, и должно предприни- маться соответствую- щее действие.					осуществление проти- возаконной работы. Проверки конфиденци- альности и накоплен- ного опыта (подтверж- дение квалификации) могут ограничить неавторизованное ис- пользование техниче- ским персоналом цен- тра СУО посредством предотвращения про- тивоакционной деятель- ности операторов. Ведение записей (лиц, запрашивающих дей- ствия, типы, даты и т. д.) в сочетании с вну- тренним аудитом.				
А.10 Менед- жмент средств связи и эксплуа- тации	А.10.10 Постоян- ный кон- троль	Обнаружи- вать неавто- ризованную деятельность по обработке информации.	Контрольные жур- налы, записываю- щие деятельность пользователей, ис- ключения и события в системе защиты информации, долж- ны генерироваться и храниться в тече- ние согласованного периода, с целью помощи в будущих расследованиях и в постоянном контро- ле над управлением доступом. Средства ведения журнала и Информа- ция журнала должны	51	E1	а	Замена (угроза Ц) персональной меди- цинской информации в оборудовании, под- лежащем техниче- скому обслуживанию основным персоналом на участке, приводит к некорректности ин- формации.	Управление привиле- гиями (контроль до- ступа) в сочетании с контролем доступа. Контроль доступа (защита записи и за- прет стирания файла) может предотвратить замену файлов ос- новным техническим персоналом.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

[illegible]

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
								Проверки конфиденциальности и накопление опыта (подтверждение квалификации) могут ограничить неавторизованное использование врачами, системными администраторами медицинского учреждения или основным техническим персоналом посредством предотвращения противозаконной деятельности операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
А.10 Менеджмент средств связи и эксплуатации	А.10.10 Постоянный контроль	Обнаруживать неавторизованную деятельность по обработке информации.	Должны быть созданы процедуры для постоянного контроля над использованием средств, обрабатывающих информацию, а результаты деятельности по постоянному контролю должны регулярно анализироваться.	11	А1	а	Неавторизованное использование (угроза К) техническим персоналом центра удаленного технического обслуживания персональной медицинской информации в оборудовании центра удаленного технического обслуживания участка приводит к угрозе раскрытия информации.	Внутренний аудит записей может обнаружить неавторизованное использование персональной медицинской информации техническим персоналом центра СУО. Кроме того, может быть обнаружено неавторизованное использование технического персонала центра СУО, так как внутренний аудит запрещает осуществление противозаконной работы.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средств управления	У	В	П	О
								Проверки конфиденциальности и накопленного опыта (подтверждение квалификации) могут ограничить неавторизованное использование технического персонала СУО предотвращением противозаконной практики операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
				12	A1	а	Неавторизованное использование (угроза К) персональной медицинской информации в оборудовании СУО техническим персоналом СУО из внутреннего источника приводит к раскрытию информации.	Внутренний аудит записей может обнаружить неавторизованное использование персональной медицинской информации техническим персоналом центра СУО. Кроме того, может быть обнаружено неавторизованное использование технического персоналом центра СУО, так как внутренний аудит заставляет осуществлять противозаконную работу. Проверки конфиденциальности и накопленного опыта (подтверждение				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менед- жмент средств связи и эксплуа- тации	А.10.10 Постоян- ный кон- троль	Обнаружи- вать неавто- ризованную деятельность по обработке информации.	Должны быть созда- ны процедуры для постоянного контро- ля над использова- нием средств, обра- батывающих инфор- мацию, а результаты деятельности по по- стоянному контролю должны регулярно анализироваться.	51	E1	а	Замена (угроза Ц) персональной меди- цинской информации в оборудовании, подде- жащем техническому обслуживанию основ- ным техническим пер- соналом на участке, приводит к некоррек- тности информации.	квалификации) могут ограничить неавто- ризованное исполь- зование техническим персоналом СУО предотвращением про- тивоакционной практики операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
								осуществление противозаконной работы. Проверки конфиденциальности и накопление опыта (подтверждение квалификации) могут ограничить неавторизованное использование персональной медицинской информации врачами, системными администраторами медицинского учреждения или основным техническим персоналом посредством предотвращения противозаконной деятельности операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
				52	E1	а	Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию, техническим персоналом центра удаленного технического обслуживания, действующим извне, приводит к некорректности информации.	Управление привилегиями (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и запрет стирания файла) может предотвратить замену файлов технического персоналом центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.10 Менед- жмент средств связи и эксплуа- тации	А.10.10 Постоян- ный кон- троль	Обнаружи- вать неавто- ризованную деятельность по обработке информации.	Должны быть созда- ны процедуры для постоянного контро- ля над использова- нием средств, обра- батывающих инфор- мацию, а результаты деятельности по по- стоянному контролю должны регулярно анализироваться.	52	E1	а	Неавторизованное ис- пользование (угроза К) или замена (угроза Ц) терапевтами персо- нальной медицинской информации из вну- треннего источника в оборудовании, подде- жащем обслуживанию, системными админи- страторами медицин- ского учреждения или основным персоналом, приводит к раскрытию (угроза К) или некор- ректности (угроза Ц) информации.	Внутренний аудит запи- сей может обнаружить неавторизованное ис- пользование персо- нальной медицинской информации врачами, системными админи- страторами медицин- ского учреждения или основным техническим персоналом. Кроме того, может быть такое обнаружено неавтори- зованное использова- ние врачами, системны- ми администраторами медицинского учреж- дения или основным техническим персона- лом, так как внутренний аудит запрещает осу- ществление противоза- конной работы. Проверки конфиденци- альности и накоплен- ного опыта (подтверж- дение квалификации) могут ограничить неавторизованное ис- пользование врачами, системными админи- страторами медицин- ского учреждения или основным техническим персоналом посред- ством предотвращения противозаконной дея- тельности операторов.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.11 Управление доступом								Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
			Часы всех имеющих отношение к делу систем обработки информации в пре- делах организации или зоны безопас- ности должны быть синхронизированы с согласованным источником точного времени.	—	—	—	—	—	—	—	—	—
	А.11.1 Де- ловые тре- бования к управле- нию досту- пом	Управлять доступом к ин- формации.	На основе деловых требований и тре- бований защиты к доступу должна быть создана, за- документирована и проанализирована политика управле- ния доступом.	—	—	—	—	—	—	—	—	—
	А.11.2 Ме- неджмент доступа пользо- вателей	Гарантировать доступ зарегис- трированного пользователя и предотвра- щать нераз- решенный до- ступ к инфор- мационным системам.	Должна быть уста- новлена формаль- ная процедура ре- гистрации и снятия с регистрации поль- зователей, с целью предоставлять и аннулировать доступ ко всем инфор- мационным и услугам.	12	А1	а	Несанкционированный вход (угроза К) третьи- ми сторонами, персо- налом и системными администраторами центра удаленного тех- нического обслужива- ния при помощи атак с «перехватом по сло- варю» в оборудовании центра удаленного	(Не требуется никаких мер)	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				21	В1	И	технического обслуживания приводит к неавторизованному использованию (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания и раскрытию (угроза К) информации. Несанкционированный вход (угроза К) при помощи атаки с «перехватом по словарю» в сетевое оборудование центра удаленного технического обслуживания из внешнего источника любого лица приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранящейся в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	Создается группа по расследованию инцидентов (ГРИ) для ускорения восстановления от ущерба, вызванного неавторизованным доступом. Управление маршрутом (без подключения к оборудованию центра удаленного технического обслуживания) предотвращает удаленное подключение к оборудованию центра удаленного технического обслуживания. Общие меры по администрированию сети для сетевого оборудования центра удаленного технического обслуживания включают в себя контроль доступа (информации для входа в систему).	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Акт	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
								особенно на выходе центра удаленного технического обслуживания, разделение сети / принудительный путь (FW) / фильтрацию и защиту порта удаленной диагностики.				
							Несанкционированный вход (угроза К) при помощи атак с «переломом по словарю» в сетевое оборудование центра удаленного технического обслуживания из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	Управление привилегиями (вход в систему в качестве пользователя / привилегированного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для входа в систему) может предотвратить несанкционированный вход лиц, не являющихся сетевыми администраторами центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.11 Управление доступом	А.11.2 Ме- неджмент доступа пользо- вателей	Гарантировать доступ зарегистри- рованного пользователя и предотвра- щать нераз- решенный до- ступ к инфор- мационным системам.	Должна быть уста- новлена формаль- ная процедура ре- гистрации и снятия с регистрации поль- зователей с целью предоставлять и аннулировать доступ ко всем Информа- ционным системам и услугам.	21	В2	И	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» в сетевое оборудование центра удаленного технического обслу- живания из внешнего источника любого лица приводит к неавтори- зованному использо- ванию (угроза К) персо- нальной медицинской информации, храни- мой в сети центра уда- ленного технического обслуживания, и к раскрытию (угроза К) информации.	Создается группа по расследованию инци- дентов (ГРИ) для уско- рения восстановления от ущерба, вызванного неавторизованным доступом. Управление маршру- том (без подключе- ния к оборудованию центра удаленного технического обслу- живания) предотвращает удаленное подключе- ние к оборудованию центра удаленного технического обслу- живания. Общие меры по администрированию сети для сетевого обо- рудования центра уда- ленного технического обслуживания вклю- чают в себя контроль доступа (информации для входа в систему), особенно на выходе центра удаленного тех- нического обслужива- ния, разделение сети / принудительный путь (FW) / Фирму и защиту порта удален- ной диагностики.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участки	Акт	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				41	D1	Р	Несанкционированный вход (угроза К) при помощи атаки с «переломом по словарю» в сетевое оборудование медицинского учреждения из внешнего источника лиц, не входящих в состав персонала центра удаленного технического обслуживания, включая персонал центров удаленного технического обслуживания других компаний, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	Создается группа по расследованию инцидентов (ГРИ) для ускорения восстановления от ущерба, вызванного неавторизованным доступом. Общие меры по администрированию сети для сетевого оборудования центра удаленного технического обслуживания включают в себя контроль доступа (информации для входа в систему), особенно на выходе центра удаленного технического обслуживания, разделение сети / принудительный путь (FW) / фильтрацию и защиту порта удаленной диагностики.	3 > 2	3	1	9 > 6
							Несанкционированный вход (угроза К) при помощи атаки с «переломом по словарю» в сетевое оборудование медицинского учреждения из внутреннего источника лиц, не являющихся сетевыми администраторами медицинского учреждения, приводит	Управление привилегиями (вход в систему в качестве пользователя / привилегированного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для входа в систему) может предотвратить несанкционированный вход	3 > 2	3	1	9 > 6

88 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	лиц, не являющихся сетевыми администраторами медицинского учреждения.				
А.11 Управление доступом	А.11.2 Механизм доступа пользователей	Гарантировать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам.	Должна быть установлена формальная процедура регистрации и снятия с регистрации пользователей с целью предоставления и аннулирования доступа ко всем информационным системам и услугам.	51	Е1	а	Несанкционированный вход (угроза К) при помощи атаки с «переворотом по словарю» в оборудование, подложное техническое обслуживание, третьих лиц, персонала медицинского учреждения, сетевых администраторов медицинского учреждения или основного технического персонала других компаний, любого лица из внешнего источника приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	Управление привилегиями (вход в систему в качестве пользователя / привилегированного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для входа в систему) может предотвратить незаконный вход третьих лиц, персонала и сетевого администратора медицинского учреждения или основного технического персонала других компаний, блокируя работу неавторизованного лица.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							Замена (угроза Ц) персональной медицинской информации в оборудовании, под-лежащем техническому обслуживанию основным техническим персоналом, приводит к некорректности (угроза Ц) информации.	Управление привилегиями (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и запрет стирания файла) может предотвратить замену файлов новым техническим персоналом.	3 > 2	3	1	9 > 6
				52	E1	а	Несанкционированный вход (угроза К) из внешнего источника при помощи атаки с «перехватом по словарию» в оборудовании, подлежащем техническому обслуживанию, технического персонала удаленного технического обслуживания других компаний приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой на оборудовании, под-лежащем техническому обслуживанию, и к раскрытию (угроза К) информации.	Управление привилегиями (вход в систему в качестве пользователя/привилегированного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для входа в систему) может предотвратить несанкционированный вход технического персонала центра удаленного технического обслуживания других компаний.	3 > 2	3	1	9 > 6

82 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	ИД	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							Замена (угроза Ц) персональной медицинской информации в оборудовании, подлечащем техническому обслуживанию, техническим персоналом центра удаленного технического обслуживания, действующим извне, приводит к некорректности (угроза Ц) информации.	Управление привилегиями (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и запрет стирания файла) может предотвратить замену файлов техническим персоналом центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6
							Несанкционированный вход (угроза К) из внутреннего источника при помощи атаки с «переворотом по словарю» в оборудование, подлежащее техническому обслуживанию, третьих сторон, персонала и сетевых администраторов медицинского учреждения приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в оборудовании, подлечащем техническому обслуживанию, и к раскрытию (угроза К) информации.	Управление привилегиями (вход в систему в качестве пользователя / привилегированного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для входа в систему) может предотвратить незаконный вход третьих лиц, персонала и сетевого администратора медицинского учреждения.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.11 Управление доступом	А.11.2 Ме- неджмент доступа пользо- вателей	Гарантировать доступ зарегистри- рованного пользо- вателя и предотвра- щать нераз- решенный до- ступ к инфор- мационным системам.	Назначение и ис- пользование приви- легий должно быть ограничено и долж- но управляться.	12	А1	а	Несанкционированный вход (угроза К) третьих сторон, персонала и сетевых администрато- ров центра удаленного технического обслу- живания при помощи атаки с «перебором по словарю» в оборудова- ние центра удаленного технического обслужи- вания приводит к не- авторизованному ис- пользованию (угроза К) персональной меди- цинской информации в оборудовании центра удаленного техниче- ского обслуживания и раскрытию (угроза К) информации.	Управление привиле- гиями (вход в систему в качестве пользовате- ля / привилегирован- ного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для вхо- да в систему) может предотвратить несанк- ционированный вход третьих сторон, персо- нала или сетевых ад- министраторов центра удаленного техниче- ского обслуживания.	3 > 2	3	1	9 > 6
				21	В1	і	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» из внутреннего источника лица, не являющегося сетевым администрато- ром центра удален- ного технического об- служивания, приводит к неавторизованному использованию (угроза К) персональной меди- цинской информации, хранящейся в сети	Управление привиле- гиями (вход в систему в качестве пользовате- ля / привилегирован- ного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для вхо- да в систему) может предотвратить несанк- ционированный вход третьих сторон, пер- сонала или сетевых администраторов				

34 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	ИД	Участки	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							центра удаленного технического обслужи- вания, и к раскрытию (угроза К) информации.	центра удаленного технического обслужи- вания.				
				41	D1	P	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» из внутреннего источника лица, не являющегося сетевым администрато- ром центра удаленного технического обслу- живания, приводит к неавторизованному ис- пользованию (угроза К) персональной медицин- ской информации, хра- нящейся в сети центра удаленного техниче- ского обслуживания, и к раскрытию (угроза К) информации.	Разработка управле- ния маршрутом, чтобы принудительно уста- новить путь и опреде- лить подключаемое оборудование.	3 > 2	3	1	9 > 6
				51	E1	a	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» в оборудование, подде- жающее техническому обслуживанию, тре- тух лиц, персонала медицинского учреж- дения, сетевых адми- нистраторов медицин- ского учреждения или основного техническо- го персонала	Управление привилегиями(вход в систему в качестве пользователя / приви- легируемого пользо- вателя) в сочетании с контролем доступа. Контроль доступа (ин- формации для входа в систему) может пре- дотерать незакон- ный вход третьих лиц, персонала и сетевых администраторов	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							других компаний, любого лица из внешнего источника приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранящейся в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	медицинского учреждения или основного технического персонала других компаний, блокируя работу неавторизованного лица.				
А.11 Управление доступом	А.11.2 Механизм доступа пользователей	Гарантировать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам.	Назначение и использование привилегий должно быть ограничено, и должно управляться.	51	E1	а	Замена (угроза Ц) персональной медицинской информации, подделывающей техническому обслуживанию, основному техническим персоналом на участке приводит к некорректности (угроза Ц) информации.	Управление привилегиями (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и запрет стирания файла) может предотвратить замену файлов новым техническим персоналом.	3 > 2	3	1	9 > 6
				52	E1	а	Замена (угроза Ц) персональной медицинской информации, подделывающей техническому обслуживанию, основному техническим персоналом центра удаленного технического обслуживания, выполненная извне, приводит к некорректности (угроза Ц) информации.	Управление привилегиями (контроль доступа) в сочетании с контролем доступа. Контроль доступа (защита записи и запрет стирания файла) может предотвратить замену файлов техническим персоналом центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							Несанкционированный вход (угроза К) из внутреннего источника при помощи атаки с «перехватом по слуху» оборудования, подлежащего техническому обслуживанию, третьими сторонами, персоналом или серверными администраторами медицинского учреждения приводит к несанкционированному использованию (угроза К) персональной медицинской информацией, хранящейся в оборудовании, подлежащем техническому обслуживанию, и к раскрытию (угроза К) информации.	Управление привилегиями (вход в систему в качестве пользователя/привилегированного пользователя) в сочетании с контролем доступа. Контроль доступа (информации для входа в систему) может предотвратить незаконный вход третьих лиц, персонала и сетевых администраторов медицинского учреждения.	3 > 2	3	1	9 > 6
									—	—	—	—
			Назначение паролей должно управляться через формальный процесс менеджмента.	—	—	—	—		—	—	—	—
			Руководство должно анализировать права доступа пользователей через регулярные интервалы, используя формальный процесс.	—	—	—	—		—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.11 Управление доступом	А.11.3 От- ветствен- ности пользо- вателя	Предотвращать неразрешенный доступ пользователей, а также компрометацию или кражу информации и средств, обрабатывающих информацию.	От пользователей надо потребовать следовать хорошим методам защиты при выборе и использовании паролей.	12	А1	а	Третьи лица, персонал или системные администраторы центра удаленного технического обслуживания при помощи незаконно полученного пароля из оборудования центра удаленного технического обслуживания, действующие от имени авторизованного пользователя, могут осуществить несанкционированное использование (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания и раскрытие (угроза К) информации.	Периодическое изменение пароля предотвращает взлом оборудования центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6
				21	В1	и	Взлом (угроза К) серверного оборудования центра удаленного технического обслуживания, используя незаконно полученный пароль, любым лицом из внешнего источника, приводит к несанкционированному использованию (угроза К) персональной медицинской информации, хранимой в сети	Периодическое изменение пароля предотвращает взлом серверного оборудования центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6

88 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	ИД	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							центра удаленного технического обслужи- вания, и к раскрытию (угроза К) информа- ции.					
							Взлом (угроза К) се- тевого оборудования центра удаленного технического обслу- живания, используя незаконно полученный пароль из внутреннего источника лицом, не являющимся сетевым администратором цен- тра удаленного техни- ческого обслуживания, приводит к несанкцио- нированному использо- ванию (угроза К) персо- нальной медицинской информации, хранимой в сети центра уда- ленного технического обслуживания, и к раскрытию (угроза К) информации.	Периодическое из- менение пароля предотвращает взлом сетевых устройств центра удаленного технического обслужи- вания.				
					В2		Взлом (угроза К) се- тевого оборудования цен- тра удаленного техни- ческого обслуживания при помощи, используя незаконно полученный пароль, из внешнего источника любым ли- цом приводит к несанк- ционированному	Периодическое из- менение пароля предотвращает взлом сетевых устройств центра удаленного технического обслужи- вания.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.					
				4.1	D1	P	Взлом (угроза К) серверного оборудования медицинского учреждения, использующего незаконно полученный пароль, из внешнего источника лицами, не входящими в состав персонала центра удаленного технического обслуживания, включая персонал центра удаленного технического обслуживания других компаний, приводит к несанкционированному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	Периодическое изменение пароля предотвращает взлом серверного оборудования медицинского учреждения.	3 > 2	3	1	9 > 6

90 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.11 Управление доступом	А.11.3 От- ветствен- ности пользо- вателя	Предотвращать неразрешенный доступ пользователей, а также компрометацию или кражу информации и средств, обрабатывающих информацию.	От пользователей надо потребовать следовать хорошим методам защиты при выборе и использовании паролей.	41	D1	P	Взлом (угроза К) сетевого оборудования медицинского учреждения, использующего законно полученный пароль, из внутреннего источника лицами, не являющимися сетевыми администраторами медицинского учреждения, приводит к несанкционированному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	Периодическое изменение пароля предотвращает взлом оборудования медицинского учреждения.	3 > 2	3	1	9 > 6
				51	E1	a	Взлом (угроза К) при помощи незаконно полученного пароля из оборудования, подлежащего обслуживанию на участке третьими лицами, персоналом медицинского учреждения, сетевыми администраторами медицинского учреждения или основным техническим персоналом других компаний, приводит к несанкционированному использованию (угроза К) персональной медицинской информации	Периодическое изменение пароля предотвращает взлом оборудования, подлежащего техническому обслуживанию.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
				52	E1	а	Взлом (угроза К) оборудования, подлежащего техническому обслуживанию техническим персоналом центра удаленного технического обслуживания других компаний, из внешнего источника при помощи незаконно полученного пароля, приводит к несанкционированному использованию (угроза К) персональной медицинской информации, хранящейся в оборудовании, подлежащем техническому обслуживанию, и к раскрытию (угроза К) информации.	Периодическое изменение пароля предотвращает взлом оборудования, подлежащего техническому обслуживанию.	3 > 2	3	1	9 > 6
							Использование незаконно полученного пароля из внутреннего источника или взлом (угроза К) врачами, третьими лицами, персоналом или системными администраторами медицинского учреждения приводит к несанкционированному	Периодическое изменение пароля предотвращает взлом оборудования, подлежащего техническому обслуживанию.	3 > 2	3	1	9 > 6

92 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							использованию (угро- за К) персональной медицинской информа- ции, хранимой в оборудо- вании, подлежащем техническому обслужи- ванию, и к раскрытию (угроза К) информации.					
			Пользователи долж- ны гарантировать, что оборудование, работающее в авто- матическом режиме, имеет подходящую защиту.	—	—	—	—	—	—	—	—	—
А.11 Управле- ние досту- пом	А.11.4 Управле- ние досту- пом к сети	Предотвращать нераз- решенный досту- п к сетевым услугам.	Пользователям дол- жен быть предостав- лен доступ только к тем службам, на которые им выдано разрешение.	—	—	—	—	—	—	—	—	—
			Подходящие методы аутентификации должны использо- ваться для управле- ния доступом дис- танционных пользо- вателей.	21	В1 В2	1	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» в сетевое оборудование центра удаленного технического обслужи- вания из внешнего ис- точника любым лицом, приводит к несанк- ционированному ис- пользованию (угроза К) персональной меди- цинской информации, хранимой в сети	Создается группа по расследованию инци- дентов (ГРИ) для уско- рения восстановления от ущерба, вызванного несанкционированным доступом. Управление маршру- том (без подключения к оборудованию цен- тра удаленного техни- ческого обслуживания) предотвращает уда- ленное подключение к оборудованию центра удаленного	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	ИД	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							центра удаленного технического обслужи- вания, и к раскрытию (угроза К) информа- ции.	технического обслужи- вания. Общие меры по администрированию сети для сетевого обо- рудования центра уда- ленного технического обслуживания вклю- чают в себя контроль доступа (информации для входа в систему), особенно на выходе центра удаленного технического обслужи- вания, разделение сети / принудительный путь (FW) / фильтрацию и защиту порта удален- ной диагностики.	3 > 2	3	1	9 > 6
				40	D1	P	Несанкционированный вход (угроза К) при помощи атаки с «пере- бором по словарю» в сетевое оборудование медицинского учреж- дения из внешнего источника лицами, не входящими в состав персонала центра уда- ленного технического обслуживания, вклю- чая персонал центров удаленного техниче- ского обслуживания других компаний, приводит к несанк- ционированному ис- пользованию (угроза К) персональной	Создается группа по расследованию инци- дентов (ГРИ) для уско- рения восстановления от ущерба, вызванного несанкционированным доступом. Управление маршру- том (без подключения к оборудованию цен- тра удаленного техни- ческого обслуживания) предотвращает уда- ленное подключение к оборудованию центра удаленного техниче- ского обслуживания. Общие меры по адми- нистрированию сети для сетевого				

94 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	ИД	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
							медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	оборудования центра удаленного технического обслуживания включают в себя контроль доступа (информации для входа в систему), особенно на выходе центра удаленного технического обслуживания, разделение сети / принудительный путь (FW) / фильтрацию и защиту порта удаленной диагностики.	3 > 2	3	1	9 > 6
							Несанкционированный вход (угроза К) при попытке атаки с «перехватом по словарю» в сетевое оборудование медицинского учреждения из внешнего источника техническим персоналом центра удаленного технического обслуживания других компаний или техническим персоналом центра удаленного технического обслуживания приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию (угроза К) информации.	Разработка управления маршрутом, чтобы принудительно установить путь и определить подключаемое оборудование.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.11 Управление доступом	А.11.4 Управление доступом к сети	Предотвращать неразрешенный доступ к сетевым услугам.	Автоматическая идентификация обслуживания должна рассматриваться как средство аутентификации соединений с конкретными мест и оборудования.	—	—	—	—	—	—	—	—	—
			Физический и логический доступ к портам диагностирования и конфигурации должен управляться.	21	В1 В2	i	Несанкционированный вход (угроза К) при помощи атаки с «переворотом по словарю» в сетевое оборудование центра удаленного технического обслуживания, из внешнего источника любым лицом, приводит к несанкционированному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	Создается группа по расследованию инцидентов (ГРИ) для ускорения восстановления от ущерба, вызванного несанкционированным доступом. Управление маршрутом (без подключения к оборудованию центра удаленного технического обслуживания) предотвращает удаленное подключение к оборудованию центра удаленного технического обслуживания. Общие меры по администрированию сети для сетевого обслуживания центра удаленного технического обслуживания включают в себя контроль доступа (информации для входа в систему), особенно на выходе центра удаленного технического обслуживания, разделение	3 > 2	3	1	9 > 6

96 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средства управления	У	В	П	О
								сети / принудительный путь (FW) / фильтрацию и защиту порта удален- ной диагностики.				
				41	D1	P	Несанкционированный вход (угроза К) при помощи атаки с «пере- воротом по словарю» в сетевое оборудование медицинского учреж- дения из внешнего источника лицами, не входящими в состав персонала центра уда- ленного технического обслуживания, вклю- чая персонал центров удаленного техниче- ского обслуживания других компаний, приводит к несанк- ционированному ис- пользованию (угроза К) персональной меди- цинской информации, хранимой в сети меди- цинского учреждения, и раскрытию (угроза К) информации.	Создается группа по расследованию инци- дентов (ГРИ) для уско- рения восстановления от ущерба, вызванного несанкционированным доступом. Управление маршру- том (без подключения к оборудованию центра удаленного техниче- ского обслуживания) предотвращает уда- ленное подключение к оборудованию центра удаленного техниче- ского обслуживания. Об- ширные меры по админи- стрированию сети для сетевого оборудования центра удаленного технического обслужи- вания включают в себя контроль доступа (ин- формации для входа в систему), особенно на выходе центра уда- ленного технического обслуживания, раз- деление сети / прину- дительный путь (FW) / фильтрацию и защиту порта удаленной диа- гностики.	3 > 2	3	1	9 > 6

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Группы информационных служб, пользователей и информационных систем должны быть разделены в сети.	—	—	—	—	—	—	—	—	—
А.11 Управление доступом	А.11.4 Управление доступом к сети	Предотвращать неразрешенный доступ к сетевым услугам.	Для совместно эксплуатируемых сетей, особенно тех, которые простираются за границы организации, возможность пользователей по подключению к сети должна быть ограничена в соответствии с политикой управления доступом и требованиями деловых приложений.	—	—	—	—	—	—	—	—	—
			Должны быть реализованы средства управления маршрутизацией для сетей, чтобы гарантировать, что компьютерные связи и информационные потоки не нарушают политику управления доступом деловых приложений.	—	—	—	—	—	—	—	—	—

98 Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
	А.11.5 Управление доступом к опе- рационной системе	Предотвращать неразрешенный доступ к операционным системам.	Доступ к операционным системам должен управляться процедурой защитыного входа в систему.	—	—	—	—	—	—	—	—	—
			Все пользователи должны иметь унифицированный идентификатор (ID пользователя) только для их персонального использования, и должна быть выделена подходящая методика аутентификации для подтверждения заявленной личности пользователя.	—	—	—	—	—	—	—	—	—
			Системы для управления паролями должны быть интерактивными и должны обеспечивать качественные пароли.	—	—	—	—	—	—	—	—	—
			Использование утилит, способных блокировать средства управления системы и приложений должно быть ограничено и должно надежно управляться.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Неактивные сеансы должны завершаться по истечении определенного периода бездействия.	—	—	—	—	—	—	—	—	—
			Необходимо использовать ограничения по времени соединения для обеспечения дополнительной защиты в приложениях с высокой степенью риска.	—	—	—	—	—	—	—	—	—
А.11 Управление доступом	А.11.6 Управление доступом к приложениям и информации А.11.7 Мобильная обработка и телеобработка	Предотвратить неразрешенный доступ к информации, содержащейся в прикладных системах.	Доступ пользователей и технического персонала к информации и функциям и прикладной системы должен быть ограничен в соответствии с определенной политикой управления доступом.	—	—	—	—	—	—	—	—	—
			Уязвимые системы должны иметь отделимую (изолированную) компьютерную среду.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
		Обеспечить информационную безопасность при использовании средств обработки и телеобработки	Должна быть принята официальная политика и должны быть приняты надлежащие меры обеспечения защиты от рисков использования мобильных компьютерных средств и средств связи.	—	—	—	—	—	—	—	—	—
			Должны быть разработаны и внедрены политика, оперативные планы и процедуры для деятельности по телеобработке.	—	—	—	—	—	—	—	—	—
А.12 Приобретение, разработка и технические обслуживание живания информационных систем	А.12.1 Требования к защите информации информационных систем А.12.2 Корректирующая обработка в приложениях	Гарантировать, что защита является неотъемлемой частью информационных систем.	В формулировках деловых требований для новых информационных систем или улучшений существующих информационных систем должны быть определены требования к средствам управления защитой.	—	—	—	—	—	—	—	—	—
		Избегать ошибок, потери, неавторизованного изменения или злоупотребления информацией в приложениях.	Должно осуществляться подтверждение соответствия данных, вводимых в приложение, чтобы убедиться, что эти данные являются верными и приемлемыми.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСОМЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Подтверждения со- ответствия должны быть включены в приложения, чтобы обнаруживать любое повреждение инфор- мации посредством обработки ошибок или сознательных действий.	—	—	—	—	—	—	—	—	—
			Должны быть опре- делены требования по обеспечению аутентичности и за- щиты целостности сообщений в при- ложениях, а также должны быть опре- делены и реализо- ваны надлежащие средства управле- ния.	—	—	—	—	—	—	—	—	—
			Выходные данные из приложений должны проходить подтверждение со- ответствия, чтобы гарантировать, что обработка хранимой информации явля- ется правильной и подходящей.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участки	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
	А.12.3 Управ- ление доступом с исполь- зованием криптогра- фии	Защитить кон- фиденциаль- ность, аутен- тичность или целостность информации криптографи- ческими сред- ствами.	Должна быть разра- ботана и применена политика по исполь- зованию криптогра- фических средств управления защитой информации.	1а	A2	b	Если стойкость (угроза К) алгоритма шифрования, метода передачи ключа недо- статочна, то зашифро- ванные данные рас- шифровываются, что приводит к раскрытию (угроза К) персональ- ной медицинской ин- формации.	Применение аттесто- ванного алгоритма шифрования, ключа защиты и метода передачи ключа может предотвратить рас- шифровку закодиро- ванной персональной медицинской инфор- мации.	3 > 2	3	1	9 > 6
				29	B2				—	—	—	—
				39	C1				—	—	—	—
А.12 Приоб- речение, разработ- ка и тех- ническое обслуживание информа- ционных систем	А.12.4 Защита системных файлов	Гарантиро- вать защиту системных файлов.	Должно быть при- нято распределение ключей, чтобы под- держивать использо- вание организацией методов криптогра- фии.	—	—	—	—	—	—	—	—	—
				—	—	—	—	—	—	—	—	—
				—	—	—	—	—	—	—	—	—
			Тестовые данные должны быть тща- тельно выбираться и управляться.	—	—	—	—	—	—	—	—	—
				—	—	—	—	—	—	—	—	—
			Доступ к исходному тексту программы должен быть огра- ничен.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
	А.12.5 Защита в процес- сах раз- работки и поддержки	Обеспечи- вать защиту прикладного системного программного обеспечения и информации.	Реализация измене- ний должна управ- ляться путем исполь- зования формальных процедур управления изменениями.	—	—	—	—	—	—	—	—	—
			При изменении опе- рационных систем деловые критичные приложения должны быть проанализиро- ваны и протестиро- ваны, чтобы гаран- тировать отсутствие неблагоприятного влияния на органи- зационные операции или защиту.	—	—	—	—	—	—	—	—	—
			Изменения в пакетах программ не должны поощряться, должны быть ограничены необходимыми из- менениями, и все изменения должны строго управляться.	—	—	—	—	—	—	—	—	—
			Должны предостав- ляться возможности для утечки.	—	—	—	—	—	—	—	—	—
			Разработка про- граммного обеспе- чения, приобретаемого на стороне, должна быть под надзором и постоянным контро- лем организации.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
	А.12.6 Менед- жмент тех- нической уязвимо- сти	Снизить риски, возникающие из эксплуа- тации опу- бличованных технологий уязвимостей.	Должна получаться своевременная ин- формация о техни- чески уязвимых ме- стах используемых информационных систем, должна оце- ниваться подвержен- ность организации влиянию через такие уязвимые места, и должны быть предприняты под- ходящие меры для решения проблемы связанного с этим риска.	—	—	—	—	—	—	—	—	—
А.13 Менед- жмент ин- цидентов в системе информа- ционной безопас- ности	А.13.1 Сообще- ние о со- бытиях и слабостях в системе информа- ционной безопас- ности	Гарантировать, что о событиях и слабостях в системе ин- формационной безопасности, связанных с информацион- ными система- ми, сообщается способом, дающим воз- можность про- извести своевре- менное кор- ректирующее действие.	О событиях в систе- ме информационной безопасности надо сообщать по соот- ветствующим слу- жебным каналам как можно быстрее. От всех служащих, подрядчиков и сто- ронних пользовате- лей информацион- ных систем и услуг надо потребовать отменить любые на- блюдаемые или по- дозрительные сла- бости защиты в си- стемах или услугах и сообщать о них.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
	А.13.2 Управление инцидентами защиты информации и утечками	Обеспечить применение последовательного и эффективного подхода к управлению инцидентами в системе информационной безопасности.	Должны быть установлены ответственность руководства и процедуры, чтобы гарантировать быструю, результативную и упорядоченную реакцию на инциденты в системе информационной безопасности.	—	—	—	—	—	—	—	—	—
			Должны быть приняты механизмы для того, чтобы дать возможность определить количество типов, объемов и издержек инцидентов в системе информационной безопасности и постоянно их контролировать.	—	—	—	—	—	—	—	—	—
			Если последующее действие против лица или организации после инцидента защищает информации включает судебное разбирательство (гражданское или уголовное), то необходимо собрать доказательства, сохранить и предоставить в соответствии с правилами изложения доказательств в соответствующей юрисдикции	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
А.14 Ме- неджерство непрерывности бизнес-деятель- ности	А.14.1 Аспекты инфор- мационной безо- пасности ме- неджмента непрерыв- ности биз- неса	Противо- действовать прерываниям в деловых операциях, за- щитить критич- ные деловые процессы от влияния суще- ственных сбоях информаци- онных систем или бедствий, а также га- рантировать своевременное возобновление деловых опе- раций.	Должен быть раз- работан и должен поддерживаться в рабочем состоянии управляемый про- цесс для обеспече- ния непрерывности бизнеса для всей организации, кото- рый рассматривает требования защиты информации, необ- ходимые для непре- рывности бизнеса организации.	—	—	—	—	—	—	—	—	—
			Должны быть вы- явлены события, которые могут вы- звать прерывания деловых процессов, вместе с вероятно- стью и негативным влиянием таких прерываний и их последствий на ин- формационную без- опасность.	—	—	—	—	—	—	—	—	—
			Должны быть раз- работаны и реа- лизованы планы для поддержания в рабочем состоянии или восстановления операций и обеспе- чения доступности информации на тре- буемом уровне и	17	А1	f	Поврежденное обо- рудование центра уда- ленного технического обслуживания (угроза Д) приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановле- ние.	3 > 2	2	1	6 > 4

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			в течение необходи- мых временных мас- штабов, следующих за прерыванием или сбоем в критичных деловых процессах.	18	A1	g	Поврежденное приро- доохранное средство (угроза Д) центра уда- ленного технического обслуживания приво- дит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановле- ние.				
				26	B1 B2	m	Поврежденное сетевое оборудование центра удаленного техниче- ского обслуживания (угроза Д) приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановле- ние.				
				27	B1 B2	n	Поврежденное приро- доохранное средство (угроза Д) для сетевого оборудования центра удаленного техниче- ского обслуживания приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановле- ние.				
				46	D1	m	Поврежденное сетевое оборудование меди- цинского учреждения (угроза Д) приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановле- ние.				
				47	D1	n	Поврежденное приро- доохранное средство (угроза Д) для сетевого оборудования меди- цинского учреждения приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановле- ние.				

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средства управления	У	В	П	О
А.14 Менеджмент непрерывности бизнес-деятельности	А.14.1 Аспекты информационной безопасности менеджмента непрерывности бизнеса	Противодействовать прерываниям в деловых операциях, защитить критичные деловые процессы от влияния существенных сбоев в информационных системах или бедствий, а также гарантировать своевременное возобновление деловых операций.	Должны быть разработаны и реализованы планы для поддержания в рабочем состоянии или восстановления операций и обеспечения доступности информации на требуемом уровне и в течение необходимых временных масштабов, следующих за прерыванием или сбоем в критичных деловых процессах.	57	E1	f	Поврежденное оборудование, подлежащее обслуживанию (угроза Д), приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановление.	3 > 2	2	1	6 > 4
				58	E1	g	Поврежденное природоохрannое средство (угроза Д) оборудования, подлежащего техническому обслуживанию, приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановление.	—	—	—	—
			Должна поддерживаться в рабочем состоянии единая структура планов обеспечения непрерывности бизнеса, с целью гарантировать, что все планы согласованы, с целью последовательного обращения к требованиям защиты информации и определения приоритетов для тестирования и поддержания в рабочем состоянии.			—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Планы обеспечения непрерывности бизнеса должны регулярно тестироваться и обновляться, с целью гарантировать, что они пополняются современными данными и результатами.	—	—	—	—	—	—	—	—	—
А.15 Соответствие	А.15.1 Соответствие правовым требованиям	Избегать нарушений любых законодательных, уставных, нормативных или договорных обязательств, и любых требований защит.	Все имеющиеся отношения к делу требования закона, нормативные и договорные требования, а также способ организации выполнения эти требования должны быть четко определены, документированы и должны пополняться последними данными для каждой информационной системы и организации.	—	—	—	—	—	—	—	—	—
			Должны быть реализованы подходящие процедуры, чтобы гарантировать соответствие законодательным, нормативным и договорным требованиям по использованию материала, в отношении	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			которого могут иметься права на интеллектуальную собственность, и по использованию лицензионных про- граммных продуктов.									
А.15 Соответ- ствие	А.15.1 Со- ответствие правовым требова- ниям	Избегать нару- шений любых законодатель- ных, уставных, нормативных или договор- ных обяза- тельств, и любых требо- ваний защиты.	Важные записи должны быть за- щищены от потери, уничтожения и фальсификации, в соответствии с тре- бованиями закона, нормативными, дого- ворными и деловы- ми требованиями.	—	—	—	—	—	—	—	—	—
			Защита и конфиден- циальность данных должны быть гаран- тированы в соответ- ствии с применимым законодательством, нормативами и, при наличии, договорны- ми условиями.	—	—	—	—	—	—	—	—	—
			Надо удерживать пользователей от использования средств, обрабаты- вающих информа- цию, для неразре- шенных целей.	—	—	—	—	—	—	—	—	—

Продолжение таблицы А.1

Раздел ИСО/МЭК 27001-2005	Подраздел ИСО/МЭК 27001-2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Криптографические средства управле- ния доступом долж- ны использоваться с соблюдением всех соответствующих соглашений, законов и правил.	—	—	—	—	—	—	—	—	—
	А.15.2 Со- ответствие политике и стан- дартам защиты, а также тех- ническое соответ- ствие	Гарантировать соответствие систем полити- кам и стандар- там обеспе- чения защиты организации.	Менеджеры должны гарантировать, что все процедуры за- щиты в пределах их зоны ответствен- ности выполняются правильно, с целью достичь соответ- ствия политике и стандартам защиты.	—	—	—	—	—	—	—	—	—
			Информационные системы должны регулярно прове- ряться на соответ- ствие стандартам реализации системы защиты.	—	—	—	—	—	—	—	—	—
	А.15.3 Коммента- рии к ауди- ту инфор- мационных систем	Максимизиро- вать результа- тивность и ми- нимизировать помехи для ют процесса ауди- та информаци- онных систем.	Требования аудита и деятельность по аудиту, включающая проверки в действу- ющих системах, должны быть тща- тельно спланирова- ны и согласованы, с целью минимизиро- вать риск срыва де- ловых процессов.	—	—	—	—	—	—	—	—	—

Окончание таблицы А.1

Раздел ИСО/МЭК 27001:2005	Подраздел ИСО/МЭК 27001:2005	Цели	Средства управления для реализации целей	№	Участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средства управления	У	В	П	О
			Доступ к инструмен- тальным средствам аудита информаци- онных систем доп- жен быть защищен, чтобы предотвра- тить любое возмож- ное неправомерное употребление или компрометацию.	—	—	—	—	—	—	—	—	—

Комментарии к таблице А.1

1 Заголовки столбцов таблицы

Заголовок	Значение
Раздел	Раздел, подраздел, задачи и средства управления для решения приведены из ИСО/МЭК 27001:2005.
Подраздел	
Цель управления	
Средства управления	
№	Номер угрозы из приложения А, ИСО/ТО 11633-1.
Участок	A1 — оборудование центра удаленного технического обслуживания (ЦОУ); A2 — A1 для ВЧП; B1 — внутренняя сеть ЦОУ; B2 — B1 для ВЧП; C1 — внешняя сеть; D1 — внутренняя сеть медицинского учреждения;
Актив	a — персональная медицинская информация в памяти, на диске и экране; b — алгоритмы, ключи и метод распределения ключей шифрования; c — записи и распечатки персональной медицинской информации; d — средства резервного копирования персональной медицинской информации; e — программное обеспечение, работающее с персональной медицинской информацией; f — оборудование, работающее с персональной медицинской информацией; g — природоохранные системы для оборудования, работающего с персональной медицинской информацией; h — операторы, работающие с персональной медицинской информацией; i — персональная медицинская информация во внутренней сети ЦОУ; j — записи и распечатки коммуникационного следа персональной медицинской информации; k — средства резервного копирования трассировки связи персональной медицинской информации; l — программное обеспечение сетевого оборудования; m — сетевое оборудование; n — природоохранные системы сетевого оборудования; o — операторы сетевого оборудования r: персональная мед. информация во внутренней сети медицинского учреждения.
Пример угрозы	Пример угрозы
Пример средств управления	Пример средств управления
У (Уязвимость)	Уровень конфиденциальности, целостности или доступности (таблицы А.2—А.4 ИСО/МЭК 27001). Показан уровень до выбора средств управления и после
В (Влияние)	Уровень влияния (см. 5 ниже)
П (вероятность выхода из строя)	Уровень вероятности выхода из строя (см. 6 ниже)
О (Оценка)	Уровень оценки = уязвимость х влияние х вероятность выхода из строя. Показывается уровень до выбора средств управления и после

2 Уровни конфиденциальности

3	Серьезная уязвимость от подглядывания / кражи, несанкционированного входа / подлога или выноса
2	Средняя уязвимость от подглядывания / кражи, несанкционированного входа / подлога или выноса
1	Незначительная уязвимость от подглядывания / кражи, несанкционированного входа / подлога или выноса

3 Уровни целостности

3	Серьезная уязвимость при выполнении или отказе в выполнении изменения, замены или удаления
2	Средняя уязвимость при выполнении или отказе в выполнении изменения, замены или удаления
1	Незначительная уязвимость при выполнении или отказе в выполнении изменения, замены или удаления

4 Уровни доступности

3	Серьезная уязвимость при обслуживании прерывания из-за отказа, бедствия, кабельного разрыва или отказа службы
2	Средняя уязвимость при обслуживании прерывания из-за отказа, бедствия, кабельного разрыва или отказа службы
1	Незначительная уязвимость при обслуживании прерывания из-за отказа, бедствия, кабельного разрыва или отказа службы

5 Уровни влияния

3	Вероятность большого влияния на выполнение операций
2	Вероятность небольшого влияния на выполнение операций
1	Незначительное влияние на выполнение операций

6 Уровни вероятности выхода из строя

3	Высокая вероятность
2	Низкая вероятность
1	Незначительная вероятность

Библиография

- [1] ISO/IEC 9797-1:1999
Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher
- [2] 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
- [3] ISO/IEC 27001:2005
Information technology — Security techniques — Information security management systems — Requirements
- [4] ISO/IEC 27002:2005
Information technology — Security techniques — Code of practice for information security management
- [5] ISO/IEC Guide 73:2002
Risk management — Vocabulary — Guidelines for use in standards

УДК 004.61:006.354

ОКС 35.240.80

Ключевые слова: здравоохранение, информатизация здоровья, информационная безопасность, менеджмент безопасности, удаленное техническое обслуживание, медицинские устройства, медицинские информационные системы, реализация систем

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 21.04.2016. Подписано в печать 04.05.2016. Формат 60×84 $\frac{1}{8}$. Гарнитура Ариал.
Усл. печ. л. 13,95. Уч.-изд. л. 13,00. Тираж 30 экз. Зак. 1226.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru

