ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

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

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии 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 (*gost.e-ecolog.ru

© Стандартинформ, 2016

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

Содержание

1 Область применения 1
2 Термины и определения 1
3 Сокращения 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 описанны 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.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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;

Издание официальное

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 неправомочным образом.

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

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

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

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

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

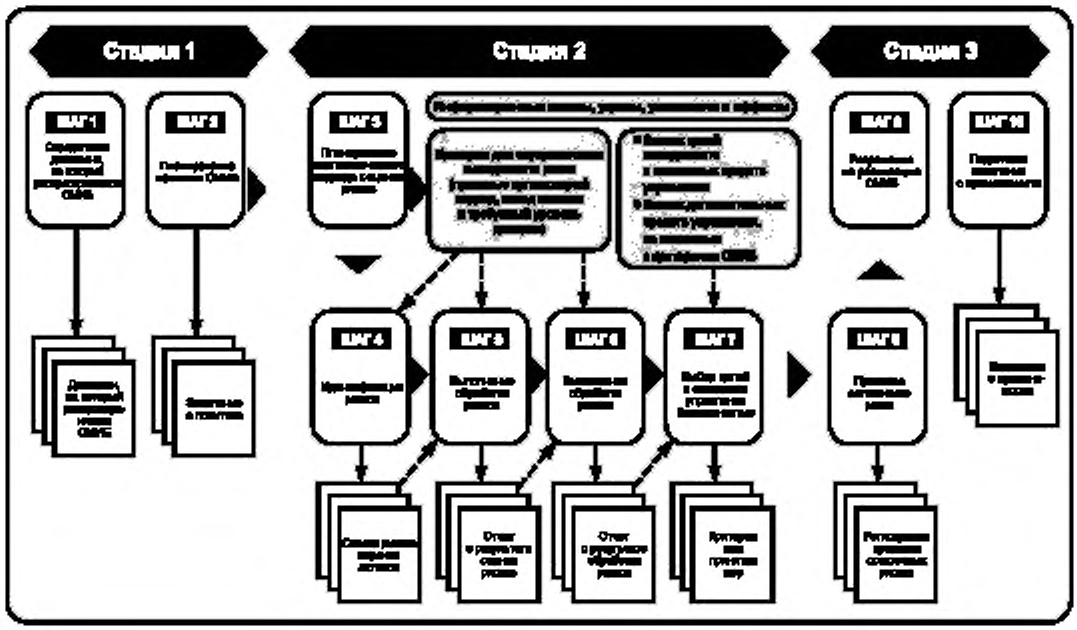

Рисунок 1 — Шаги реализации СМИБ

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 ответственностей 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.

c) Смешанный подход.

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

d) 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 a) 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.

a) 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.

b) 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.

c) Центр удаленного обслуживание 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	№	участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность; Д — доступность)	Пример средств управления	У	В	П	О
А.5 Политика информационной безопасности	А.5.1 Направляющая роль руководства в сфере информационной безопасности	Обеспечить направляющую роль менеджмента и поддержку информационной безопасности в соответствии с требованиями бизнеса и соответствующими законодательными и регламентирующими требованиями.	Должен быть разработан, одобрен руководством, опубликован и доведен до персонала и соответствующих внешних сторон комплекс политик информационной безопасности.	—	—	—	—	—	—	—	—	—
			С тем, чтобы гарантировать постоянную пригодность, соответствие и результативность политик информационной безопасности, они должны пересматриваться через запланированные интервалы времени или когда произведены существенные изменения.	—	—	—	—	—	—	—	—	—
А.6 Организация системы информационной безопасности	А.6.1 Внутренняя организация	Осуществлять менеджмент информационной безопасности в рамках организации	Руководство должно активно поддерживать безопасность в пределах организации посредством четкого руководства, продемонстрированных обязательств, подробного распределения и признания ответственности за информационную безопасность.	—	—	—	—	—	—	—	—	—

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
			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 получений 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 средств 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, проистекающие из деловых 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 средств управления	У	В	П	О
		информацию, которые доступны внешним сторонам, обрабатываются 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.	—	—	—	—	—	—	—	—	—
			Соглашения с третьими сторонами, включающие доступ, обработку, сообщение или менеджмент информации организации или средств, обрабатывающих информацию, или добавление изделий или услуг к средствам, обрабатывающим информацию, должны включать в себя все значимые требования защиты.	36	С1	m	Отказ (угроза Д) сетевого оборудования со 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

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
							Уничтожение (угроза Д) сетевого оборудования со стороны поставщика интернет-служб приводит к потере Д к СУО.	Контракты на поставку сторонних услуг (ключевой менеджмент) предотвращают недоступность службы, указывая сферу ответственности со стороны поставщика интернет-служб.	3 > 2	2	1	6 > 4
				37	С1	п	Отказ (угроза Д) или разъединение кабеля природоохранного средства от сетевого оборудования со стороны поставщика интернет-служб приводит к потере Д к СУО.	Контракты на поставку сторонних услуг (обслуживание, проверка, резервное копирование) предотвращают недоступность службы, указывая сферу ответственности со стороны поставщика интернет-служб.	3 > 2	2	1	6 > 4
							Поврежденное (угроза Д) природоохранного оборудования для 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
							Уничтожение (угроза Д) природоохранного средства для сетевого оборудования со стороны поставщика интернет-служб приводит к потере Д к СУО.	Контракты на поставку сторонних услуг (ключевой менеджмент) предотвращают недоступность 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 средств управления	У	В	П	О
А.7 Менеджмент активов	А.7.1 Ответственность за активы	Достичь и поддерживать в рабочем состоянии подходящую защиту организационных активов.	Все активы должны быть четко определены, и должен быть составлен и должен поддерживаться в рабочем состоянии реестр всех важных активов. Вся информация и активы, связанные со средствами, обрабатывающими информацию, должны «находиться во владении» назначенной части организации. Должны быть определены, документированы и внедрены правила для приемлемого использования информации и активов, связанных со средствами, обрабатывающими информацию.	—	—	—	—	—	—	—	—	—
	А.7.2 Классификация информации	Гарантировать, что информация обеспечена соответствующим уровнем защиты.	Информация должна быть классифицирована с точки зрения ее значения, законодательных требований, уязвимости и критичности для 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 средств управления	У	В	П	О
			В соответствии со схемой классификации, принятой организацией, должен быть разработан и реализован подходящий набор процедур маркировки и обработки информации.	—	—	—	—	—	—	—	—	—
А.8 Защита человеческих ресурсов	А.8.1 Перед наймом на работу А.8.2 Во время выполнения работы А.8.3 Завершение или изменение работы по найму	Гарантировать, что служащие, подрядчики и пользователи третьей стороны понимают свою ответственность и подходят для должностей, на которые они рассматриваются, а также снизить риск кражи, мошенничества или неправильного использования средств. Гарантировать, что все служащие, подрядчики и пользователи третьей стороны осознают угрозы	Роли и ответственность служащих, подрядчиков и пользователей третьей стороны в отношении безопасности должны быть определены и задокументированы в соответствии с политикой информационной безопасности организации.	—	—	—	—	—	—	—	—	—
			Проверки верификации в фоновом режиме по всем кандидатам в служащие, в подрядчики и в пользователи третьей стороны должны проводиться в соответствии с имеющими отношение к делу законами, нормами и этикой, и должны быть пропорциональны	—	—	—	—	—	—	—	—	—

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
		информационной безопасности и хлопоты по защите информации, свою ответственность и свои обязательства, и оснащены для того, чтобы поддерживать организационную политику безопасности во время своей обычной работы, а также для того, чтобы снизить риск ошибки человека. Гарантировать, что служащие, подрядчики и пользователи третьей стороны уходят из организации или меняют службу в установленном порядке.	деловым требованиям, классификации информации, которая будет доступной, и предполагаемым рискам.									
			Как часть договорного обязательства, служащие, подрядчики и пользователи третьей стороны должны согласиться и подписать сроки и условия договора личного найма, в котором должны быть указаны их ответственность за информационную безопасность и ответственность организации за информационную безопасность. Должна быть четко определена и назначена ответственность за осуществление окончания или изменения работы по найму.	11	A1	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 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	№	участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средств управления	У	В	П	О
				12	А1	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	№	участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средств 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 техническим персоналом центра 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 техническим персоналом центра СУО. Кроме того, неавторизованное использованиетехническим 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.	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
								Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
							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 основным обслуживающим персоналом.	3	3	1	9
				52	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 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	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
								использование техническим персоналом центра СУО предотвращением противозаконной деятельности операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
				52	E1	a	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 тех. персоналом центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6
				53	E1	c	Удаление или замена на участке лечащим врачом приводит к раскрытию нарушению 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 средств 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 организацией политиками и процедурами.	—	—	—	—	—	—	—	—	—
			Все служащие организации и, если это имеет отношение к делу, подрядчики и пользователи 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 СУО.	Тренинги 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	№	участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средств управления	У	В	П	О
				28	B1	0	Неверная установка (угроза К) приводит к неожиданному раскрытию (угроза К) персональной медицинской информации.	Тренинги 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
				48	D1							
				59	E1	h	Неверный ввод (угроза Ц) и случайное удаление (угроза Д) ведут к перебою в Д к СУО.	Тренинги 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
А.8 Защита человеческихх ресурсов	А.8.3 Завершение или изменение работы по найму	Гарантировать, что служащие, подрядчики и пользователи третьей стороны уходят из организации или меняют службу упорядоченно.	Все служащие, подрядчики и пользователи третьей стороны должны вернуть все активы организации, находящиеся в их владении, по окончании их работы по найму, договора или соглашения. Права доступа всех служащих, подрядчиков и пользователей третьей стороны к информации и средствам, обрабатывающим информацию, должны быть	51	E1	a	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 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 средств 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 Физическая безопасность и охрана окружающей среды	А.9.1 Зона безопасности	Предотвратить несанкционированный физический доступ, нанесение ущерба и вмешательство в недвижимость и информацию организации.	Для защиты зон, в которых находятся информация и средства, обрабатывающие информацию, должны использоваться периметры безопасности (барьеры, такие как стены, управляемый картами 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.	Перегородки 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 средств управления	У	В	П	О
			Зоны безопасности должны быть защищены подходящими средствами управления входом, с целью гарантировать, что только персоналу, имеющему разрешение, позволен доступ.	11	А1	а	Несанкционированный вход в систему (угроза К) третьих лиц, персонала медицинского учреждения, сетевых администраторов медучреждения 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 средств управления	У	В	П	О
				13	A1	c	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, приводя к раскрытию персональной медицинской информации.	Утилизация шредером может предотвратить просмотр или удаление страниц третьими лицами, персоналом центра удаленного технического обслуживания или сетевыми администраторами центра удаленного технического обслуживания. Управление входом в помещение может ограничить вход третьими лицами, персоналу центра удаленного технического обслуживания или сетевым администраторам центра удаленного технического обслуживания и блокирует просмотр и удаление страниц.	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	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 средств управления	У	В	П	О
							обслуживания приводит к раскрытию (угроза К) персональной медицинской информации.					
				16	A1	f	Удаление оборудования центра удаленного технического обслуживания и дисков лицами, не являющимися персоналом центра удаленного технического обслуживания, приводит к раскрытию (угроза К) персональной медицинской информации .	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	3	1	9 > 6
				17	A1	f	Уничтожение (угроза Д) оборудования центра удаленного технического обслуживания 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
				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 недоступность службы, вызванную уничтожением, предотвращая 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 средств управления	У	В	П	О
				22	B1	j	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, персонала 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	B1	k	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 средств 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 недоступность службы, вызванную уничтожением оборудования, предотвращая доступ к оборудованию неавторизованных лиц.	3 > 2	2	1	6 > 4
				27	B1 B2	n	Уничтожение (угроза Д) природоохранного средства для сетевого оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Управление ключами защиты может предотвратить недоступность службы, вызванную уничтожением оборудования, предотвращая 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 средств управления	У	В	П	О
				42	D1	j	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление страниц (угроза К) лицами, не являющимися сетевыми администраторами 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 средств управления	У	В	П	О
				45	D1	m	Удаление (угроза К) оборудования центра удаленного технического обслуживания, почтовых серверов и их дисков лицами, не являющимися сетевыми администраторами медицинских учреждений, приводит к раскрытию персональной медицинской информации.	Управление входом в помещение может предотвратить вход в помещение лиц, не являющихся сетевыми администраторами медицинского учреждения, чтобы избежать удаления сетевого оборудования медицинского учреждения, почтовых серверов или их дисков предотвращая присутствие неавторизованных лиц.	3 > 2	3	1	9 > 6
							Уничтожение (угроза Д) оборудования центра удаленного технического обслуживания 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
				47	D1	n	Уничтожение (угроза Д) природоохранного средства для сетевого оборудования медицинского учреждения 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

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
				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 средств 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

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
			и руководящие принципы для работы в зонах безопасности.				удаленного технического обслуживания приводит к раскрытию персональной медицинской информации.	отсутствии других членов, предотвращая удаление бумажных страниц.				
				14	A1	d	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.	Управление ключами защиты несколькими лицами может ограничить технический персонал центра удаленного технического обслуживания от доступа к дискам при отсутствии других пользователей.	3 > 2	3	1	9 > 6
				16	A1	f	Удаление (угроза К) оборудование 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 средств управления	У	В	П	О
				21	В1	i	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 средств 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 несколькими лицами может ограничить доступ к дискам сетевым администраторам центра удаленного технического обслуживания в отсутствии других лиц и предотвратить раскрытие персональной медицинской информации посредством сетевого оборудования центра удаленного технического обслуживания, предотвращая доступ авторизованных лиц к диску в отсутствии 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 отсутствии 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 средств 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

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
							персональной медицинской информации, хранимой в сети медицинского учреждения, и раскрытию информации.					
				41	D1	Р	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 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 средств управления	У	В	П	О
				42	D1	j	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 средств управления	У	В	П	О
				45	D1	m	Удаление (угроза К) сетевого оборудования, 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, почтовым 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	Вынос (угроза К) или замена актива на участке лечащим врачом приводит к раскрытию или фальсификации персональной медицинской информации.	Управление ключами защиты несколькими лицами может ограничить взаимодействие врача с информационной средой на диске в отсутствии других членов организации (в одиночку), чтобы. предотвратить авторизованному лицу взаимодействовать 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 средств управления	У	В	П	О
							раскрытию или фальсификации персональной медицинской информации.	учреждения, предотвращая доступ к дискам 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 рассекречивание 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

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
				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 средств управления	У	В	П	О
				45	D1	m	Анализ (угроза К) утечки электромагнитных волн от сетевого оборудования медицинского учреждения приводит к раскрытию персональной медицинской информации.	Обеспечивая наличие расстояния между местонахождением сетевого оборудования медицинского учреждения и дорогой, можно предотвратить раскрытие персональной медицинской информации, предотвращая прием электромагнитных волн утечки.	3 > 2	3	1	9 > 6
				56	E1	f	Несанкционированное вмешательство (угроза К) в оборудование, подлежащее техническому обслуживанию, приводит к непредвиденному раскрытию персональной медицинской информации.	Предусмотрено блокирование при обнаружении следов несанкционированного вмешательства.	3 > 2	3	1	9 > 6
							Анализ утечки (угроза К) электромагнитных волн от оборудования, подлежащего техническому обслуживанию, приводит к раскрытию персональной медицинской информации.	Обеспечивая наличие расстояния между местонахождением оборудования, подлежащего техническому обслуживанию, и дорогой, можно предотвратить раскрытие персональной медицинской информации, предотвращая прием электромагнитных волн утечки.	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
			Оборудование должно быть защищено от нарушений энергоснабжения и других нарушений, вызванных сбоями во вспомогательном оборудовании.	—	—	—	—	—	—	—	—	—
			Источник энергии и кабели связи, по которым передаются данные или вспомогательные информационные услуги, должны быть защищены от перехвата или повреждения.	—	—	—	—	—	—	—	—	—
			Оборудование должно проходить соответствующее техническое обслуживание, чтобы гарантировать его долгосрочную доступность и целостность.	—	—	—	—	—	—	—	—	—
			Оборудование, информация или программное обеспечение не должны 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 средств управления	У	В	П	О
			Все единицы оборудования, содержащие носители информации, должны быть проверены, чтобы гарантировать, что любые уязвимые данные и лицензированное программное обеспечение было удалено или надежно перезаписано перед ликвидацией.	11	А1	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 напоминания техническому персоналу центра удаленного технического обслуживания об удалении персональной медицинской информации, таким образом, снижая риск ошибки, связанной с человеческим фактором.	3 > 2	3	1	9 > 6
А.9 Физическая безопасность и охрана окружающей среды	А.9.2 Защита оборудования	Избежать потерь, ущерба, краж или рассекречивания ресурсов и сбоев 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	Е1	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 медицинского учреждения, основным техническим персоналом других компаний, основным техническим персоналом или системными администраторами медицинского учреждения приводит к раскрытию персональной медицинской информации.	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 средств управления	У	В	П	О
			чистого экрана в отношении устройств обработки информации (А.11.3.3).									
А.10 Менеджмент средств связи и эксплуатации	А.10.1 Процедуры эксплуатации и ответственность	Гарантировать правильную и безопасную работу средств, обрабатывающих информацию.	Процедуры эксплуатации должны быть документированы, поддерживаться в рабочем состоянии, и быть доступными для всех пользователей, которым они нужны.	—	—	—	—	—	—	—	—	—
			Изменения в средствах и системах, обрабатывающих информацию, должны управляться.	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
				21	В1 В2	і	Несанкционированный вход (угроза К) при помощи атаки с «перебором 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 средств управления	У	В	П	О
							источника любым лицом приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.	Контроль маршрута (без подключения к оборудованию центра удаленного технического обслуживания) предотвращает удаленное подключение к оборудованию центра удаленного технического обслуживания. Общие меры администрирования сети для сетевого оборудования центра удаленного технического обслуживания включают в себя контроль доступа (информации при входе в систему), особенно на выходе центра удаленного технического обслуживания, разделение сети / принудительный путь (FW) / фильтрацию и защиту порта удаленной диагностики.				
				24	B1	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.	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	№	участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средств управления	У	В	П	О
								Противовирусные меры могут обнаружить и удалить программные закладки или программы хищения информации.				
				41	D1	р	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в сетевое оборудование медицинского учреждения из внешнего источника лицами, не входящими 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 центра удаленного технического обслуживания, и к раскрытию информации.	Создается группа по расследованию инцидентов (ГРИ) для ускорения восстановления ущерба, вызванного неавторизованным доступом. Общие меры администрирования сети для сетевого оборудования центра удаленного технического обслуживания включают в себя контроль доступа (информации при входе 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

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
				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
				55	E1	e						
			Обязанности и области ответственности должны быть разделены, с целью снизить количество возможностей неразрешенного или непреднамеренного изменения или неправильного 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 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
А.10 Менеджмент средств связи и эксплуатации	А.10.2 Управление предоставлением услуг третьей стороной.	Реализовать и поддерживать подходящий уровень информационной безопасности и предоставления услуг в соответствии с соглашениями о предоставлении услуг третьей стороной.	Должно быть гарантировано, что средства управления безопасностью, описания услуг и уровни предоставления, включенные в соглашение о предоставлении услуг третьей стороны, реализуются, эксплуатируются и поддерживаются третьей стороной.	—	—	—	—	—	—	—	—	—
			Услуги, отчеты и записи, предоставляемые третьей стороной, должны постоянно контролироваться и анализироваться; регулярно должны проводиться аудиты.	—	—	—	—	—	—	—	—	—
			Должен осуществляться менеджмент изменений в предоставлении услуг, включая поддержание в рабочем состоянии и улучшение существующей политики, процедур и средств управления в области защиты информации, с учетом критичности вовлеченных 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 средств 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 злонамеренного и 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	A1	e	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	B1	I						
				44	D1							
				55	E1	e						

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
			Если использование мобильного кодирования разрешено, то конфигурация должна гарантировать, что разрешенное мобильное кодирование работает в соответствии с четко определенной политикой защиты, а выполнение неразрешенного мобильного кодирования должно быть предотвращено.									
	А. 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.	17	А1	f	Отказ (угроза Д) оборудования 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
				18	А1	g	Отказ (угроза Д) оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				
				26	В1 В2	m	Отказ (угроза Д) сетевого 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 средств управления	У	В	П	О
				27	B1 B2	n	Отказ (угроза Д) или отсоединение кабеля (угроза Д) природоохранного средства от сетевого оборудования медицинского учреждения приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				
				46	D1	m	Отказ (угроза Д) сетевого оборудования медицинского учреждения приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				
				47	D1	n	Отказ (угроза Д) или отсоединение кабеля Д природоохранного средства от сетевого оборудования медицинского учреждения приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				
				57	E1	f	Отказ (угроза Д) оборудования, подлежащего техническому обслуживанию, приводит к потере Д к СУО.	Техническое обслуживание, контрольные проверки и резервирование данных может предотвратить недоступность служб.				
				58	E1	g	Отказ (угроза Д) природоохранного оборудования, для оборудования, подлежащего техническому обслуживанию, 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 средств 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 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. Характеристики защиты, уровни услуги и требования менеджмента всех сетевых служб должны быть выявлены и включены в любое соглашение по сетевым услугам, независимо от того, предоставляются ли эти услуги внутренне или берутся из внешних источников.	27	B2	i	Несанкционированный вход (угроза К) при помощи атаки с «перебором 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 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.	1	3	1	3
							Взлом (угроза К) сетевого оборудования центра удаленного технического обслуживания при помощи незаконно полученного пароля из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит кнеавторизованному использованию (угроза К)	Периодическое изменение пароля предотвращает взлом сетевого оборудования центра удаленного технического обслуживания.				

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
							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	Проверка внутреннего маршрута на стороне центра удаленного технического обслуживания несколькими лицами, чтобы обнаружить следы прослушивания маршрута несколькими лицами.				

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
							использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию информации.					
							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 несколькими лицами может ограничить доступ к дискам сетевым администраторам центра удаленного технического обслуживания в отсутствии других лиц и предотвратить раскрытие персональной медицинской информации посредством сетевого оборудования центра удаленного технического обслуживания, предотвращая, тем самым, доступ авторизованных лиц к диску 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 средств 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 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. Характеристики защиты, уровни услуги и требования менеджмента всех сетевых служб должны быть выявлены и включены в любое соглашение по сетевым услугам, независимо от того, предоставляются ли эти услуги внутренне или берутся из внешних источников.	22	B2	J	Если соответствующий актив оставлен для ремонта или контроля, то просмотр или удаление (угроза К) страниц лицами, не являющимися сетевыми администраторами 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 (с отдельной коммуникационной трассой) может ограничить вход в помещение лиц, не являющихся сетевыми администраторами центра удаленного технического обслуживания, и предотвратить просмотр или удаление страниц, предотвращая присутствие неавторизованных лиц.	1	3	1	3
							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 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				

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
								страниц, предотвращая вход в помещение авторизованных лиц в отсутствии других лиц.				
				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.				
							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 средств управления	У	В	П	О
				24	B2	l	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
А.10 Менеджмент средств связи и эксплуатации	А.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 сетевого оборудования, 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 услуги, и требования менеджмента всех сетевых служб должны быть	—	—	—	—	—	—	—	—	—

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
			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 средств 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 техническогообслуживания и дорогой, 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 квалификации операторов.				
	А.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	c	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

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
							администраторами центра удаленного технического обслуживания, приводя к раскрытию (угроза К) персональной медицинской информации.	в помещение третьих лиц, персонала или сетевых администраторов центра удаленного технического обслуживания и блокировать просмотр или удаление бумажных страниц.				
А.10 Менеджмент средств связи и эксплуатации	А.10.7 Обработка носителей информации	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	B1	j	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 допуская присутствие 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 средств управления	У	В	П	О
				42	D1	j	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 коммуникационной 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 неправильного использования.	—	—	—	—	—	—	—	—	—
			Системная документация должна быть защищена от неразрешенного доступа.	—	—	—	—	—	—	—	—	—

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
А.10 Менеджмент средств связи и эксплуатации	А.10.8 Обмен информацией А.10.9 Службы электронной торговли	Поддерживать защиту информации и программного обеспечения, обмениваемых в рамках организации и со сторонними компаниями. Гарантировать защиту услуг электронной торговли, а также их безопасное использование.	Между организацией и внешними сторонами должны быть установлены соглашения для обмена информацией и программным обеспечением.	—	—	—	—	—	—	—	—	—
А.10 Менеджмент средств связи и эксплуатации	А.10.8 Обмен информацией А.10.9 Службы электронной торговли	Поддерживать защиту информации и программного обеспечения, обмениваемых в рамках организации и со сторонними компаниями. Гарантировать защиту услуг электронной торговли, а также их безопасное использование.	Носитель, содержащий информацию, должен быть защищен от неразрешенного доступа, неправильного использования или порчи в ходе транспортировки за физические границы организации.	—	—	—	—	—	—	—	—	—
			Информация, вовлеченная в сделки в режиме онлайн, должна быть защищена для того, чтобы предотвратить неполную передачу, неправильную маршрутизацию,	—	—	—	—	—	—	—	—	—

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
			неразрешенное изменение сообщения, неразрешенное разглашение, неразрешенное дублирование или повторное воспроизведение сообщения. Информация, вовлеченная в электронную торговлю, протекающая 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.	—	—	—	—	—	—	—	—	—

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
			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 взаимозависимостью систем деловой информации.	—	—	—	—	—	—	—	—	—
А.10 Менеджмент средств 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 информации техническим персоналом центра удаленного технического обслуживания. Кроме того, может быть также обнаружено неавторизованное использование персональной медицинской информации 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 средств 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 накопленного опыта (подтверждение квалификации) могут ограничить неавторизованное использование техническим 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, 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.	12	А1	а	Неавторизованное использование (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания его техническим персоналом изнутри приводит к угрозе раскрытия информации.	Внутренний аудит записей может обнаружить неавторизованное использование техническим персоналом центра удаленного технического обслуживания. Кроме того, неавторизованное использование техническим персоналом центра удаленного технического обслуживания может быть также обнаружено, так как внутренний аудит запрещает				

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
			Средства ведения журнала и информация журнала должны 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.					осуществление противозаконной работы. Проверки конфиденциальности и накопленного опыта (подтверждение квалификации) могут ограничить неавторизованное использование техническим 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, 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	51	Е1	а	Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию основным персоналом на участке, 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 основным техническим персоналом.	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
			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.	52	E1	a	Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию, техническим персоналом центра удаленного технического обслуживания 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 основным техническим персоналом.	3 > 2	3	1	9 > 6
							Неавторизованное использование (угроза К) или замена (угроза Ц) терапевтами персональной медицинской информации из внутреннего источника в оборудование, подлежащее обслуживанию системными администраторами медицинского учреждения или основным персоналом, приводит к раскрытию (угроза К) или некорректности (угроза Ц) информации.	Внутренний аудит записей может обнаружить неавторизованное использование персональной медицинской информации врачами, системными администраторами медицинского учреждения или основным техническим персоналом. Кроме того, может быть также обнаружено неавторизованное использование врачами, системными администраторами медицинского учреждения или основным техническим персоналом, 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 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 техническим персоналом 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 техническим персоналом СУО предотвращением противозаконной практики операторов. Ведение записей (лиц, запрашивающих действия, типы, даты, и т. д.) в сочетании с внутренним аудитом.				
				12	A1	a	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 техническим персоналом центра СУО, так как внутренний аудит запрещает осуществление противозаконной работы. 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 средств управления	У	В	П	О
								квалификации) могут ограничить неавторизованное использование техническим персоналом СУО предотвращением противозаконной практики 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.	51	Е1	а	Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию основным техническим персоналом на участке, приводит к некорректности информации.	Внутренний аудит записей может обнаружить неавторизованное использование персональной медицинской информации врачами, системными администраторами медицинского учреждения или основным техническим персоналом. Кроме того, неавторизованное использование персональной медицинской информации врачами, системными администраторами медицинского учреждения или основным техническим персоналом может быть также обнаружено, так как внутренний аудит запрещает	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
								осуществление противозаконной работы. Проверки конфиденциальности и накопленного 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	a	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 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 средств управления	У	В	П	О
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.	52	Е1	а	Неавторизованное использование (угроза К) или замена (угроза Ц) терапевтами персональной медицинской информации из внутреннего источника в оборудовании, подлежащем обслуживанию, системными администраторами медицинского учреждения или основным персоналом, приводит к раскрытию (угроза К) или некорректности (угроза Ц) информации.	Внутренний аудит записей может обнаружить неавторизованное использование персональной медицинской информации врачами, системными администраторами медицинского учреждения или основным техническим персоналом. Кроме того, может быть также обнаружено неавторизованное использование врачами, системными администраторами медицинского учреждения или основным техническим персоналом, так как внутренний аудит запрещает осуществление противозаконной работы. Проверки конфиденциальности и накопленного опыта (подтверждение квалификации) могут ограничить неавторизованное использование врачами, системными администраторами медицинского учреждения или основным техническим персоналом посредством предотвращения 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 средств управления	У	В	П	О
								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 пределах организации или зоны безопасности должны быть синхронизированы с согласованным источником точного времени.	—	—	—	—	—	—	—	—	—
А.11 Управление доступом	А.11.1 Деловые требования к управлению доступом	Управлять доступом к информации.	На основе деловых требований и требований защиты к доступу должна быть создана, задокументирована и проанализирована политика управления доступом.	—	—	—	—	—	—	—	—	—
	А.11.2 Менеджмент 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 предоставлять и аннулировать доступ ко всем информационным системам и услугам.	12	А1	а	Несанкционированный вход (угроза К) третьими сторонами, персоналом и системными администраторами центра удаленного технического обслуживания при помощи атаки с «перебором по словарю» в оборудование 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 средств управления	У	В	П	О
							технического обслуживания приводит к неавторизованному использованию (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания и раскрытию (угроза К) информации.					
				21	B1	i	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в сетевое оборудование центра удаленного технического обслуживания из внешнего источника любого лица приводит к неавторизованному 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 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	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средств 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 атаки с «перебором 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 средств управления	У	В	П	О
А.11 Управление доступом	А.11.2 Менеджмент 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 предоставлять и аннулировать доступ ко всем информационным системам и услугам.	21	B2	i	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в сетевое оборудование центра удаленного технического обслуживания из внешнего источника любого лица приводит к неавторизованному 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 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), особенно на выходе центра удаленного технического обслуживания, разделение сети / принудительный путь (FW) / фильтрацию и защиту порта удаленной 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	№	участок	Актив	Пример угрозы (К — конфиденциальность; Ц — целостность, Д — доступность)	Пример средств управления	У	В	П	О
				41	D1	Р	Несанкционированный вход (угроза К) при помощи атаки с «перебором 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 «перебором 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

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
							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 Менеджмент 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 предоставлять и аннулировать доступ ко всем информационным системам и услугам.	51	Е1	а	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в оборудование, подлежащее техническому обслуживанию, 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 средств управления	У	В	П	О
							Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем 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 основным техническим персоналом.	3 > 2	3	1	9 > 6
				52	E1	a	Несанкционированный вход (угроза К) из внешнего источника при помощи атаки с «перебором по словарю» в оборудование, подлежащее техническому обслуживанию, технического персонала центра удаленного технического обслуживания других компаний приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранимой на 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 несанкционированный вход технического персонала центра удаленного технического обслуживания других компаний.	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
							Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем 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 «перебором 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, 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 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 средств управления	У	В	П	О
А.11 Управление доступом	А.11.2 Менеджмент доступа пользователей	Гарантировать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам.	Назначение и использование привилегий должно быть ограничено и должно управляться.	12	А1	а	Несанкционированный вход (угроза К) третьих сторон, персонала и сетевых администраторов центра удаленного технического обслуживания при помощи атаки с «перебором по словарю» в оборудование центра удаленного технического обслуживания приводит к неавторизованному использованию (угроза К) персональной медицинской информации в оборудовании центра удаленного технического обслуживания и 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 третьих сторон, персонала или сетевых администраторов центра удаленного технического обслуживания.	3 > 2	3	1	9 > 6
				21	В1	i	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» из внутреннего источника лица, не являющегося сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранящейся в сети	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 третьих сторон, персонала или сетевых администраторов				

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
							центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	центра удаленного технического обслуживания.				
				41	D1	Р	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» из внутреннего источника лица, не являющегося сетевым администратором центра удаленного технического обслуживания, приводит к неавторизованному использованию (угроза К) персональной медицинской информации, хранящейся в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	Разработка управления маршрутом, чтобы принудительно установить путь и определить подключаемое оборудование.	3 > 2	3	1	9 > 6
				51	E1	а	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в оборудование, подлежащее техническому обслуживанию, третьих лиц, персонала медицинского учреждения, сетевых администраторов медицинского учреждения или основного технического персонала	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	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
							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 Менеджмент доступа пользователей	Гарантировать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам.	Назначение и использование привилегий должно быть ограничено, и должно управляться.	51	Е1	а	Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию, основным 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 основным техническим персоналом.	3 > 2	3	1	9 > 6
				52	Е1	а	Замена (угроза Ц) персональной медицинской информации в оборудовании, подлежащем техническому обслуживанию, 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 средств управления	У	В	П	О
							Несанкционированный вход (угроза К) из внутреннего источника при помощи атаки с «перебором по словарю» оборудования, подлежащего техническому обслуживанию, третьими сторонами, персоналом или сетевыми администраторами медицинского учреждения приводит к несанкционированному использованию (угроза К) персональной медицинской информации, 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 средств управления	У	В	П	О
А.11 Управление доступом	А.11.3 Ответственности пользователя	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	i	Взлом (угроза К) сетевого 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 сетевого оборудования 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 средств управления	У	В	П	О
							центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.					
							Взлом (угроза К) сетевого оборудования центра удаленного технического обслуживания, используя незаконно полученный пароль из внутреннего источника лицом, не являющимся сетевым администратором центра удаленного технического обслуживания, приводит к несанкционированному использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	Периодическое изменение пароля предотвращает взлом сетевого оборудования центра удаленного технического обслуживания.				
					B2		Взлом (угроза К) сетевого оборудования центра удаленного технического обслуживания при помощи, используя незаконно полученный пароль, из внешнего источника любым лицом приводит к несанкционированному	Периодическое изменение пароля предотвращает взлом сетевого оборудования центра удаленного технического обслуживания.				

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
							использованию (угроза К) персональной медицинской информации, хранимой в сети центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.					
				41	D1	Р	Взлом (угроза К) сетевого оборудования медицинского учреждения, используя 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 сетевого оборудования 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 средств управления	У	В	П	О
А.11 Управление доступом	А.11.3 Ответственности пользователя	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	Р	Взлом (угроза К) сетевого оборудования медицинского учреждения, используя незаконно 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 сетевого оборудования медицинского учреждения.	3 > 2	3	1	9 > 6
				51	E1	а	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 средств управления	У	В	П	О
							оборудования, подлежащего обслуживанию, и к раскрытию (угроза К) информации.					
				52	E1	a	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, хранимой 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

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
							использованию (угроза К) персональной медицинской информации, хранимой в оборудовании, подлежащем техническому обслуживанию, и к раскрытию (угроза К) информации.					
			Пользователи должны гарантировать, что оборудование, работающее в автоматическом режиме, имеет подходящую защиту.	—	—	—	—	—	—	—	—	—
А.11 Управление доступом	А.11.4 Управление доступом к сети	Предотвращать неразрешенный доступ к сетевым услугам.	Пользователям должен быть предоставлен доступ только к тем службам, на которые им выдано разрешение.	—	—	—	—	—	—	—	—	—
			Подходящие методы аутентификации должны использоваться для управления доступом дистанционных пользователей.	21	B1 B2	I	Несанкционированный вход (угроза К) при помощи атаки с «перебором 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	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	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
							центра удаленного технического обслуживания, и к раскрытию (угроза К) информации.	технического обслуживания. Обшие 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.				
				40	D1	Р	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в сетевое оборудование медицинского учреждения из внешнего источника лицами, не входящими в состав персонала центра удаленного технического обслуживания, включая персонал центров удаленного технического обслуживания других компаний, приводит к несанкционированному использованию (гроза К) персональной	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	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
							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.				
							Несанкционированный вход (угроза К) при помощи атаки с «перебором 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.	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
А.11 Управление доступом	А.11.4 Управление доступом к сети	Предотвращать неразрешенный доступ к сетевым услугам.	Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений с конкретных мест и оборудования.	—	—	—	—	—	—	—	—	—
			Физический и логический доступ к портам диагностирования и конфигурации должен управляться.	21	B1 B2	i	Несанкционированный вход (угроза К) при помощи атаки с «перебором 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. Обшие 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	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
								сети / принудительный путь (FW) / фильтрацию и защиту порта удаленной диагностики.				
				41	D1	Р	Несанкционированный вход (угроза К) при помощи атаки с «перебором по словарю» в сетевое оборудование медицинского учреждения из внешнего источника лицами, не входящими в состав персонала центра удаленного технического обслуживания, включая персонал центров удаленного технического обслуживания других компаний, приводит к несанкционированному 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 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 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

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
			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.	—	—	—	—	—	—	—	—	—

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
	А.11.5 Управление доступом к операционной системе	Предотвращать неразрешенный доступ к операционным системам.	Доступ к операционным системам должен управляться процедурой защищенного входа в систему.	—	—	—	—	—	—	—	—	—
			Все пользователи должны иметь уникальный идентификатор (ID пользователя) только для их персонального использования, и должна быть выбрана 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 средств 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	Предотвращать 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 отдельную (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 средств управления	У	В	П	О
		Обеспечить информационную безопасность при использовании средств мобильных 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 техническое обслуживание информационных систем	А.12.1 Требования к защите информационных систем А.12.2 Корректная 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.	—	—	—	—	—	—	—	—	—
		Избежать ошибок, потери, неавторизованного изменения или злоупотребления информации в приложениях.	Должно осуществляться подтверждение соответствия данных, вводимых в приложения, чтобы убедиться, что эти данные являются верными и применимыми.	—	—	—	—	—	—	—	—	—

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
			Подтверждения соответствия должны быть включены в приложения, чтобы обнаруживать любое повреждение информации посредством обработки ошибок или сознательных действий.	—	—	—	—	—	—	—	—	—
			Должны быть определены требования по обеспечению аутентичности и защиты целостности сообщений в приложениях, а также должны быть определены и реализованы надлежащие средства управления.	—	—	—	—	—	—	—	—	—
			Выходные данные из приложений должны проходить подтверждение соответствия, чтобы гарантировать, что обработка хранимой информации является правильной и подходящей.	—	—	—	—	—	—	—	—	—

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
	А.12.3 Управление доступом с использованием криптографии	Защитить конфиденциальность, аутентичность или целостность информации криптографическими средствами.	Должна быть разработана и применена политика по использованию криптографических средств управления защитой информации.	1a 29 39	A2 B2 C1	b	Если стойкость (угроза К) алгоритма шифрования, метода передачи ключа недостаточна, то зашифрованные данные расшифровываются, что приводит к раскрытию (угроза К) персональной медицинской информации.	Применение аттестованного алгоритма шифрования, ключа защиты и метода передачи ключа может предотвратить расшифровку закодированной персональной медицинской информации.	3 > 2	3	1	9 > 6
			Должно быть принято распределение ключей, чтобы поддерживать использование организацией методов криптографии.	—	—	—	—	—	—	—	—	—
А.12 Приобретение, разработка и техническое обслуживание информационных систем	А.12.4 Защита системных файлов	Гарантировать защиту системных файлов.	Должны быть приняты процедуры, чтобы управлять установкой программного обеспечения в операционных системах.	—	—	—	—	—	—	—	—	—
			Тестовые данные должны быть тщательно выбираться и управляться.	—	—	—	—	—	—	—	—	—
			Доступ к исходному тексту программы должен быть ограничен.	—	—	—	—	—	—	—	—	—

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
	А.12.5 Защита в процессах разработки и поддержки	Обеспечивать защиту прикладного системного программного обеспечения и информации.	Реализация изменений должна управляться путем использования формальных процедур управления изменениями.	—	—	—	—	—	—	—	—	—
			При изменении операционных систем деловые критичные приложения должны быть проанализированы и протестированы, чтобы гарантировать отсутствие неблагоприятного влияния на организационные операции или защиту.	—	—	—	—	—	—	—	—	—
			Изменения в пакетах программ не должны поощряться, должны быть ограничены необходимыми изменениями, и все изменения должны строго управляться.	—	—	—	—	—	—	—	—	—
			Должны предотвращаться возможности для утечки.	—	—	—	—	—	—	—	—	—
			Разработка программного обеспечения, приобретаемого на стороне, должна быть под надзором и постоянным контролем 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 средств управления	У	В	П	О
	А.12.6 Менеджмент технической уязвимости	Снизить риски, возникающие из эксплуатации опубликованных технических уязвимостей.	Должна получаться своевременная информация о технически уязвимых местах используемых информационных систем, должна оцениваться подверженность организации влиянию через такие уязвимые места, и должны быть предприняты подходящие меры для решения проблемы связанного с этим риска.	—	—	—	—	—	—	—	—	—
А.13 Менеджмент инцидентов в системе информационной безопасности	А.13.1 Сообщение о событиях и слабостях в системе информационной безопасности	Гарантировать, что о событиях и слабостях в системе информационной безопасности, связанных с информационными системами, сообщается способом, дающим возможность произвести своевременное корректирующее действие.	О событиях в системе информационной безопасности надо сообщать по соответствующим служебным каналам как можно быстрее.	—	—	—	—	—	—	—	—	—
			От всех служащих, подрядчиков и сторонних пользователей информационных систем и услуг надо потребовать отмечать любые наблюдаемые или подозрительные слабости защиты в системах 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 средств управления	У	В	П	О
	А.13.2 Управление инцидентами защиты информации и улучшениями	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 защиты 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 средств 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 информационных систем или бедствий, а также гарантировать своевременное возобновление деловых операций.	Должен быть разработан и должен поддерживаться в рабочем состоянии управляемый процесс для обеспечения непрерывности бизнеса для всей организации, который рассматривает требования защиты информации, необходимые для непрерывности бизнеса организации.	—	—	—	—	—	—	—	—	—
			Должны быть выявлены события, которые могут вызвать прерывания деловых процессов, вместе с вероятностью и негативным влиянием таких прерываний и их последствий на информационную безопасность.	—	—	—	—	—	—	—	—	—
			Должны быть разработаны и реализованы планы для поддержания в рабочем состоянии или восстановления операций и обеспечения доступности информации на требуемом уровне и	17	A1	f	Поврежденное оборудования центра удаленного 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 восстановление.	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 средств управления	У	В	П	О
			в течение необходимых временных масштабов, следующих за прерыванием или сбоем в критичных деловых процессах.	18	A1	g	Поврежденное природоохранного средства (угроза Д) центра удаленного технического обслуживания приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановление.				
				26	B1 B2	m	Поврежденное сетевое оборудование центра удаленного 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 восстановление.				
				27	B1 B2	n	Поврежденное природоохранное средство (угроза Д) для сетевого оборудования центра удаленного технического обслуживания приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановление.				
				46	D1	m	Поврежденное сетевое оборудование медицинского учреждения (угроза Д) приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановление.				
				47	D1	n	Поврежденное природоохранное средство (угроза Д) для сетевого оборудования медицинского учреждения приводит к потере Д к СУО.	Аварийные меры и планы восстановления после аварии могут снизить потери при аварии и обеспечить быстрое восстановление.				

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
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 информационных систем 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 техническому 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 природоохранное 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 средств управления	У	В	П	О
			Планы обеспечения непрерывности бизнеса должны регулярно тестироваться и обновляться, с целью гарантировать, что они пополняются современными данными и результативны.	—	—	—	—	—	—	—	—	—
А.15 Соответствие	А.15.1 Соответствие правовым требованиям	Избегать нарушений любых законодательных, уставных, нормативных или договорных обязательств, и любых требований защиты.	Все имеющие отношение к делу требования закона, нормативные и договорные требования, а также способ организации выполнить 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 средств управления	У	В	П	О
			которого могут иметься права на интеллектуальную собственность, и по использованию лицензионных программных продуктов.									
А.15 Соответствие	А.15.1 Соответствие правовым требованиям	Избегать нарушений любых законодательных, уставных, нормативных или договорных обязательств, и любых требований защиты.	Важные записи должны быть защищены от потери, уничтожения и фальсификации, в соответствии с требованиями закона, нормативными, договорными и деловыми требованиями.	—	—	—	—	—	—	—	—	—
			Защита и конфиденциальность данных должны быть гарантированы в соответствии с применимым законодательством, нормативами и, при наличии, договорными условиями.	—	—	—	—	—	—	—	—	—
			Надо удерживать пользователей от использования средств, обрабатывающих информацию, для неразрешенных 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 средств управления	У	В	П	О
			Криптографические средства управления доступом должны использоваться с соблюдением всех соответствующих соглашений, законов и правил.	—	—	—	—	—	—	—	—	—
	А.15.2 Соответствие политике и стандартам защиты, а также техническое соответствие	Гарантировать соответствие систем политикам и стандартам обеспечения защиты организации.	Менеджеры должны гарантировать, что все процедуры защиты в пределах их зоны ответственности выполняются правильно, с целью достичь соответствия политике и стандартам защиты.	—	—	—	—	—	—	—	—	—
			Информационные системы должны регулярно проверяться на соответствие стандартам реализации системы защиты.	—	—	—	—	—	—	—	—	—
	А.15.3 Комментарии к аудиту информационных систем	Максимизировать результативность и минимизировать помехи для/от процесса аудита информационных систем.	Требования аудита и деятельность по аудиту, включающая проверки в действующих системах, должны быть тщательно спланированы и согласованы, с целью минимизировать риск срыва деловых 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 средств управления	У	В	П	О
			Доступ к инструментальным средствам аудита информационных систем должен быть защищен, чтобы предотвратить любое возможное неправильное 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 информации; h — операторы, работающие с персональной медицинской информации; i — персональная медицинской информации 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 p: 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 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.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru