ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 27799— 2015

Информатизация здоровья

МЕНЕДЖМЕНТ ЗАЩИТЫ ИНФОРМАЦИИ В ЗДРАВООХРАНЕНИИ ПО ИСО/МЭК 27002

(ISO 27799:2008, IDT)

Издание официальное

Москва
Стандартинформ
2016

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 28 декабря 2015 г. № 2219-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 27799:2008 «Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002» («Health informatics — Information security management in health using ISO/IEC 27002», IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

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

© 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
1.1 Общие положения . . . 1
1.2 Исключения из области применения . . . 1
2 Нормативные ссылки . . . 2
3 Термины и определения . . . 2
3.1 Термины здравоохранения . . . 2
3.2 Термины по защите информации . . . 3
4 Сокращения . . . 4
5 Защита медицинской информации . . . 4
5.1 Цели защиты медицинской информации . . . 4
5.2 Защита информации в рамках управления информацией . . . 5
5.3 Управление информацией в рамках управления организацией и клинической практикой . . . 5
5.4 Медицинская информация, подлежащая защите . . . 6
5.5 Угрозы и уязвимости защиты медицинской информации . . . 6
6 Практический план действий по внедрению ИСО/МЭК 27002 . . . 7
6.1 Систематизация стандартов ИСО/МЭК 27002 и ИСО/МЭК 27001 . . . 7
6.2 Обязательство руководства по внедрению ИСО/МЭК 27002 . . . 8
6.3 Создание, эксплуатация, обслуживание и улучшение СМИБ . . . 8
6.4 Планирование. Создание СМИБ . . . 9
6.5 Действие. Внедрение и эксплуатация СМИБ . . . 16
6.6 Проверка. Мониторинг и проверка СМИБ . . . 16
6.7 Улучшение. Обслуживание и улучшение СМИБ . . . 17
7 Использование ИСО/МЭК 27002 в здравоохранении . . . 18
7.1 Общие положения . . . 18
7.2 Политика защиты информации . . . 18
7.3 Организация защиты информации . . . 19
7.4 Управление активами . . . 21
7.5 Безопасность человеческих ресурсов . . . 23
7.6 Физическая безопасность и безопасность среды . . . 25
7.7 Управление коммуникациями и деятельностью . . . 26
7.8 Контроль доступа . . . 30
7.9 Заказ, проектирование и обслуживание информационных систем . . . 33
7.10 Управление инцидентами защиты информации . . . 35
7.11 Аспекты защиты информации в управлении непрерывностью бизнеса . . . 35
7.12 Соответствие . . . 36
Приложение А (справочное) Угрозы защиты медицинской информации . . . 38
Приложение В (справочное) Задачи и сопутствующие документы СМИБ . . . 42
Приложение С (справочное) Потенциальная польза и требуемые свойства инструментов поддержки . . . 46
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . 48
Библиография . . . 49

Введение

Настоящий стандарт представляет собой руководство для медицинских организаций и других хранителей персональной медицинской информации о том, как лучше всего сохранить конфиденциальность, целостность и доступность такой информации путем внедрения ИСО/МЭК 27002[1)]. В частности, настоящий стандарт касается особых потребностей в области менеджмента защиты информации в сфере здравоохранения и специфичных условиях его выполнения. В то время как защита и безопасность персональной информации очень важны для всех частных лиц, корпораций, организаций и правительств, в сфере здравоохранения существуют особые требования, которые должны быть соблюдены для обеспечения конфиденциальности, целостности, возможности проверки и доступности персональной медицинской информации. Этот тип информации рассматривается многими как один из самых конфиденциальных видов персональной информации. Защита этой конфиденциальности необходима, если должна поддерживаться конфиденциальность объекта оказания медицинской помощи. Для обеспечения безопасности пациентов должна быть защищена целостность медицинской информации, и важным компонентом этой защиты является обеспечение того, чтобы весь жизненный цикл информации полностью поддавался проверке. Доступность медицинской информации также имеет большое значение для эффективного предоставления медицинских услуг. Системы информатизации здоровья должны соответствовать специфичным потребностям для того, чтобы оставаться в рабочем состоянии на фоне стихийных бедствий, системных сбоев и атак типа «отказ в обслуживании». Следовательно, защита конфиденциальности, целостности и доступности медицинской информации требует опыта, специфичного для сектора здравоохранения.

Эффективный менеджмент IT-защиты в области здравоохранения становится все более необходимым при все более широком использовании беспроводных и интернет-технологий при предоставлении медицинских услуг. При ненадлежащем применении эти сложные технологии повысят риски для конфиденциальности, целостности и доступности медицинской информации. Независимо от размера, расположения и модели предоставления услуг, все медицинские организации должны иметь строгий контроль, чтобы защитить вверенную им медицинскую информацию. Тем не менее, многие специалисты в области здравоохранения работают как самостоятельные врачи или небольшие клиники, которые не имеют выделенных информационно-технологических ресурсов для управления защитой информации. Поэтому медицинские учреждения должны иметь четкое, сжатое и специфичное для здравоохранения руководство по выбору и реализации такого контроля. Это руководство должно быть адаптируемо к широкому диапазону размеров, мест применения и моделей предоставления услуг, имеющихся в здравоохранении. Наконец, с ростом электронного обмена персональной медицинской информацией между работниками здравоохранения в принятии общих рекомендаций для управления защитой информации в сфере здравоохранения имеются очевидные преимущества.

ИСО/МЭК 27002 уже широко используется для управления защитой информационных технологий для информатизации здоровья через национальные или региональные руководства в Австралии, Канаде, Франции, Нидерландах, Новой Зеландии, Южной Африке и Великобритании. В других странах также растет интерес к этому. Настоящий стандарт опирается на опыт, накопленный в ходе попыток стран обеспечить защиту персональной медицинской информации и предназначен в качестве документа, сопутствующего ИСО/МЭК 27002. Он не предназначен для замены ИСО/МЭК 27002 или ИСО/МЭК 27001. Он, скорее, является дополнением к этим более обобщенным стандартам.

Настоящий стандарт применяет ИСО/МЭК 27002 к области здравоохранения таким образом, чтобы тщательно рассмотреть вопрос о надлежащем применении мер безопасности в целях защиты персональной медицинской информации. Эти соображения, в некоторых случаях, привели авторов к выводу, что применение определенных целей контроля, указанных в ИСО/МЭК 27002, необходимо, если персональная медицинская информация должна быть защищена надлежащим образом. Поэтому настоящий стандарт устанавливает ограничения на применение определенных мер безопасности, указанных в ИСО/МЭК 27002. Это в свою очередь привело к включению в раздел 7 нескольких нормативных актов, согласно которым применение данного контроля безопасности является обязательным. Например, в 7.2.1 определено следующее:

*«Организации, занимающиеся обработкой медицинской информации, в том числе личной медицинской информации, **должны** иметь политику по защите информации в письменном виде, одобрен-*

[1)] Это руководство отвечает требованиям пересмотренного варианта ИСО/МЭК 27002:2005.

ную руководством, опубликованную, а затем доведенную до всех сотрудников и соответствующих сторонних организаций».

В области здравоохранения организация (например, больница) может быть сертифицирована на соответствие ИСО/МЭК 27001, при этом не требуется сертификация или даже признание соответствия настоящему стандарту. Однако следует надеяться, что, ввиду того, что медицинские организации стремятся улучшить защиту персональной медицинской информации, а соответствие настоящему стандарту, как более строгому стандарту для здравоохранения, будет также иметь широкое распространение.

Все объекты контроля защиты, описанные в ИСО/МЭК 27002, имеют отношение к информатизации здоровья, но некоторые элементы управления требуют дополнительных разъяснений касательно того, каким образом они могут быть использованы, чтобы защитить конфиденциальность, целостность и доступность информации о состоянии здоровья. Существуют также дополнительные требования, характерные для сферы здравоохранения. Настоящий стандарт содержит дополнительные указания в формате, который лица, ответственные за защиту медицинской информации могут легко понять и применить.

Авторы настоящего стандарта не намереваются писать пособие по компьютерной безопасности или заново формулировать то, что уже было написано в ИСО/МЭК 27002 или ИСО/МЭК 27001. Существует много требований безопасности, которые являются общими для всех систем, связанных с применением компьютерной техники, используемых в финансовом обслуживании, производстве, управлении производственными процессами или в любой другой организованной области деятельности. Были предприняты объединенные усилия для того, чтобы сосредоточиться на требованиях безопасности, необходимость которых вызвана уникальными задачами по предоставлению электронной медицинской информации, которая поддерживает оказание помощи.

Кому адресован настоящий стандарт?

Настоящий стандарт предназначен для тех, кто отвечает за контроль защиты медицинской информации, и для медицинских организаций и других хранителей медицинской информации, которым необходимо руководство по данной теме, а также для их советников по безопасности, консультантов, аудиторов, продавцов и третьих лиц, оказывающих услуги.

Преимущества использования настоящего стандарта

ИСО/МЭК 27002 является широким комплексным стандартом, и его рекомендации не адаптированы специально под требования здравоохранения. Настоящий стандарт позволяет последовательно применить ИСО/МЭК 27002 в условиях здравоохранения и при этом особое внимание уделить специальным задачам, поставленным сферой здравоохранения. Соответствие настоящему стандарту помогает медицинским организациям сохранять конфиденциальность и целостность вверенных им данных, обеспечивать доступность к основным информационным системам здравоохранения и распределять ответственность за медицинскую информацию.

Принятие настоящего стандарта медицинскими организациями в пределах одной юрисдикции и между юрисдикциями поможет взаимодействию и позволит безопасно внедрить новые совместные технологии оказания медицинской помощи. Безопасный и конфиденциальный обмен информацией может значительно улучшить результаты предоставления медицинских услуг.

Благодаря настоящему стандарту медицинские организации могут отметить снижение количества и тяжести инцидентов в системе безопасности, позволяя перераспределить ресурсы для более продуктивной деятельности. Защита IT позволит распределить ресурсы здравоохранения рентабельно и продуктивно. На самом деле, исследование, проведенное Форумом по защите информации и аналитиками рынка, показало, что хорошая разносторонняя защита может увеличить эффективность организации на целых 2 %.

Наконец, последовательный подход к защите IT, понятный всем лицам и организациям, относящимся к здравоохранению, улучшит моральное состояние коллектива и повысит доверие общества к системам, хранящим персональную медицинскую информацию.

Как использовать настоящий стандарт

Читателям, еще не знакомым с ИСО/МЭК 27002, настоятельно рекомендуется ознакомиться с вводными разделами настоящего стандарта, прежде чем продолжить его изучение. Специалисты по внедрению настоящего стандарта должны сначала внимательно прочитать ИСО/МЭК 27002, так как в тексте ниже будут неоднократно делаться ссылки на соответствующие разделы этого стандарта. Настоящий стандарт не может быть полностью понят без знакомства с полным текстом ИСО/МЭК 27002.

Читателям, не знакомым с защитой медицинской информации и ее целями, задачами, и полным контекстом, будет полезно прочитать краткое введение, которое можно найти в разделе 5.

Читатели, интересующиеся руководством по внедрению ИСО/МЭК 27002 в область здравоохранения, найдут в разделе 6 применяемый на практике план действий. Данный раздел не содержит обязательных требований. Вместо этого даны общие советы и рекомендации о том, как лучше приступить к внедрению ИСО/МЭК 27002 в здравоохранение. Раздел выстроен вокруг цикла деятельности (планирование/действие/проверка/улучшение), который описан в ИСО/МЭК 27001, и который, в случае его выполнения, приведет к надежному внедрению системы менеджмента информационной безопасности.

Читатели, нуждающиеся в конкретных советах по одиннадцати разделам управления защитой и 39 основным категориям управления защитой, описанным в ИСО/МЭК 27002, смогут найти их в разделе 7. Этот раздел рассматривает каждый из одиннадцати разделов ИСО/МЭК 27002 по управлению защитой. При необходимости указываются минимальные требования, а в некоторых случаях изложены нормативные руководства по надлежащему применению определенных видов управления защитой для защиты медицинской информации, указанных в ИСО/МЭК 27002.

В конце настоящего стандарта даны три приложения. Приложение А описывает общие угрозы медицинской информации. Приложение В кратко описывает задачи и сопутствующие документы системы менеджмента информационной безопасности. В приложении С рассматриваются преимущества средств поддержки для оказания помощи при внедрении. В библиографии перечислены соответствующие стандарты в области защиты медицинской информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информатизация здоровья

МЕНЕДЖМЕНТ ЗАЩИТЫ ИНФОРМАЦИИ В ЗДРАВООХРАНЕНИИ ПО ИСО/МЭК 27002

Health informatics. Information security management in health using ISO/IEC 27002

Дата введения — 2016—11—01

1 Область применения

1.1 Общие положения

Настоящий стандарт определяет руководства для помощи при толковании или внедрении ИСО/МЭК 27002 в информатизацию здоровья и является дополнением настоящему стандарту[1)].

Настоящий стандарт устанавливает подробный набор элементов управления для управления защитой медицинской информации и предоставляет руководства по лучшим практикам для защиты медицинской информации. Внедряя настоящий стандарт, медицинские организации и другие хранители медицинской информации смогут обеспечить минимальный необходимый уровень защиты, соответствующий условиям организации и способный поддерживать конфиденциальность, целостность и доступность персональной медицинской информации.

Настоящий стандарт распространяется на информацию о здоровье во всех ее аспектах, независимо от формы представления информации (слова и цифры, звукозаписи, рисунки, видео и медицинские снимки), средств, используемых для ее хранения (напечатанная или написанная на бумаге или в электронном виде) и средств, используемых для ее передачи (вручную, по факсу, через компьютерные сети или по почте), так как информация всегда должна быть соответствующим образом защищена.

Настоящий стандарт и ИСО/МЭК 27002 в своей совокупности определяют, *что* требуется в рамках защиты информации в области здравоохранения; но не определяют то, *как* эти требования должны быть выполнены. Иными словами, настоящий стандарт в максимально возможной степени является технологически нейтральным. Нейтральность по отношению к внедрению технологий является важной особенностью. Технология защиты по-прежнему переживает бурное развитие, и темп этих изменений теперь измеряется в месяцах, а не в годах. В противоположность этому, ожидается, что стандарты в целом останутся в силе в течение многих лет, при том, что они подлежат периодическому пересмотру. Не менее важно и то, что технологическая нейтральность оставляет продавцам и поставщикам услуг возможность предлагать новые или развивающиеся технологии, отвечающие необходимым требованиям, которые описывает настоящий стандарт.

Как отмечалось во введении, для понимания настоящего стандарта необходимо сначала ознакомиться с содержанием ИСО/МЭК 27002.

1.2 Исключения из области применения

Следующие области защиты информации выходят за рамки настоящего стандарта:

a) методики и статистические испытания для эффективной анонимизации персональной медицинской информации;

b) методики псевдонимизации персональной медицинской информации (см. [10] для примера технической спецификации ИСО, непосредственно касающиеся данной темы);

c) качество работы сети обслуживания и методы измерения доступности сетей, используемых для информатизации здоровья;

d) качество данных (в отличие от целостности данных).

[2)] Данное руководство отвечает требованиям пересмотренного варианта ИСО/МЭК 27002:2005.

Издание официальное

2 Нормативные ссылки

Следующие нормативные документы являются обязательными для применения настоящего документа. Для датированных ссылок применяется только цитированное издание. Для недатированных ссылок применяется последнее издание ссылочного документа (включая все поправки).

ISO/IEC 27002:2005, Информационные технологии. Технологии безопасности. Практические правила менеджмента информационной безопасности (Information technology — Security techniques — Code of practice for information security management)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 Термины здравоохранения

3.1.1 **информатизация здоровья** (health informatics): Научная дисциплина, которая занимается когнитивными задачами, задачами по обработке информации и коммуникационными задачами практики здравоохранения, задачами образования и исследованиями, в том числе в области информатики и информационных технологий, обеспечивающих выполнения этих задач.

[ИСО/ТР 18307:2001, определение 3.73]

3.1.2 **информационная система здравоохранения** (health information system): Хранилище информации о здоровье субъекта оказания медицинской помощи в удобном для машинной обработки виде, которая безопасно хранится и передается и является доступной для нескольких уполномоченных пользователей.

Примечание — Основано на определении 2.25, ИСО/ТР 20514:2005.

3.1.3 **здравоохранение** (healthcare): Любой вид услуг, предоставленных медицинскими работниками или средним медицинским персоналом и оказывающих влияние на состояние здоровья.

[Европейский парламент, 1998, согласно цитате ВОЗ]

3.1.4 **медицинская организация** (healthcare organization): Общий термин, используемый для описания многих видов организаций, предоставляющих медицинские услуги.

[ИСО/ТР 18307:2001, определение 3.74]

3.1.5 **работник здравоохранения** (health professional): Лицо, которое уполномоченные органы признали квалифицированным для выполнения определенных медицинских служебных обязанностей.

Примечание — Основано на определении 3.18, ИСО/ТС 17090-1:2002.

3.1.6 **поставщик медицинской помощи** (healthcare provider): Лица или организации, которые каким-либо образом вовлечены в оказание медицинской помощи клиенту, или заботящиеся о благополучии клиента.

3.1.7 **идентифицируемое лицо** (identifiable person): Лицо, которое может быть прямо или косвенно идентифицировано, в частности по идентификационному номеру или одному или нескольким факторам, характерным для его физической, физиологической, психической, экономической, культурной или социальной идентичности.

[ИСО 22857:2004, определение 3.7]

3.1.8 **пациент** (patient): Субъект оказания медицинской помощи. (См. 3.1.10.)

3.1.9 **персональная медицинская информация** (personal health information): Информация об идентифицируемом человеке, которая относится к физическому или психическому здоровью человека или к оказанию медицинской помощи человеку, которая может включать в себя:

a) информацию о регистрации физического лица для предоставления медицинских услуг;

b) информацию о платежах или основаниях для включения человека в список лиц, получающих медицинские услуги;

c) номер, символ или особенность, приписываемая конкретному человеку для того, чтобы однозначно установить его личность в целях предоставления медицинских услуг;

d) любую информацию о человеке, собранную в ходе предоставления ему медицинской помощи;

e) сведения, полученные во время проверок или экспертизы части тела или физической субстанции;

f) идентификацию человека (например, работника здравоохранения) в качестве поставщика медицинской помощи для человека.

Примечание — Персональная медицинская информация не включает в себя информацию саму по себе или в сочетании с другой информацией, имеющейся в распоряжении владельца, которая является анонимизированной, то есть по информации невозможно установить личность человека, который является субъектом информации.

3.1.10 **субъект оказания медицинской помощи** (subject of care): Один или несколько человек, которым должны предоставить, предоставляют или уже предоставили медицинское обслуживание.
[ИСО/ТС 18308:2004, определение 3.40]

3.2 Термины по защите информации

3.2.1 **актив** (asset): Все, что имеет ценность для организации.
[ИСО/МЭК 13335-1:2004, определение 2.2]

Примечание — В контексте информационной безопасности в медицине, информационные активы включают:
a) медицинскую информацию;
b) IT-сервисы;
c) аппаратные средства;
d) программное обеспечение;
e) коммуникационные средства;
f) средства информации;
g) IT-средства;
h) медицинские приборы, которые записывают данные или формируют отчеты данных.

3.2.2 **подотчетность** (accountability): Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.
[ИСО 7498-2:1989, определение 3.3.3]

3.2.3 **доверие** (assurance): Результат серии процессов установления соответствия, посредством которых организация достигает уверенности в статусе менеджмента информационной безопасности.

3.2.4 **доступность** (availability): Свойство данных или ресурсов быть доступными и пригодными к использованию по запросу авторизованного логического объекта.
[ИСО 7498-2:1989, определение 3.3.11]

3.2.5 **оценка соответствия** (compliance assessment): Процессы, посредством которых организация подтверждает, что задействованные средства управления информационной безопасности остаются исправными и эффективными.

Примечание — Нормативно-правовое соответствие относится непосредственно к элементам управления безопасностью, задействованным в целях выполнения требований соответствующего законодательства, такого как Директива Европейского союза о защите персональных данных.

3.2.6 **конфиденциальность** (confidentiality): Свойство данных, позволяющее не давать права доступа к информации или не раскрывать ее неавторизованным лицам, процессам или другим логическим объектам.
[ИСО 7498-2:1989, определение 3.3.16]

3.2.7 **целостность данных** (data integrity): Способность данных не подвергаться изменению или уничтожению при несанкционированном доступе.
[ИСО 7498-2:1989, определение 3.3.21]

3.2.8 **управление информацией** (information governance): Процессы, посредством которых организация получает гарантию того, что риски для ее информации, а потому и работоспособность и целостность организации эффективно идентифицируются и управляются.

3.2.9 **защита информации** (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 защиты информации, но также могут рассматриваться как производные от трех основных свойств в определении.

3.2.10 **риск** (risk): Сочетание вероятности события и его последствий.
[Руководство ИСО 73:2002, определение 3.1.1]

3.2.11 **оценка рисков** (risk assessment): Общий процесс анализа риска и оценивания рисков.
[Руководство ИСО 73:2002, определение 3.3.1]

3.2.12 **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, принятие риска и информирование о рисках.

[Руководство ИСО 73:2002, определение 3.1.7]

3.2.13 **работа с рисками** (risk treatment): Процесс выбора и осуществления мер по изменению (обычно снижению) риска.

Примечание — Основано на определении 3.4.1, Руководстве ИСО 73:2002.

3.2.14 **целостность системы** (system integrity): Свойство, показывающее, что система выполняет предусмотренную для нее функцию в нормальном режиме, свободном от преднамеренного или случайного несанкционированного воздействия на систему.

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

[ИСО/МЭК 13335-1:2004, определение 2.25]

3.2.16 **уязвимость** (vulnerability): Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

[ИСО/МЭК 13335-1:2004, определение 2.26]

4 Сокращения

ISMF — Форум по менеджменту защиты информации (ISMF — Information Security Management Forum);

СМИБ — Система менеджмента информационной безопасности (ISMS — Information Security Management System);

IT — Информационная технология (IT — Information Technology);

SLA — Соглашение о качестве предоставляемых услуг (SLA — Service Level Agreement);

SOA — Заявление о применимости (SOA — Statement of Applicability).

5 Защита медицинской информации

5.1 Цели защиты медицинской информации

Сохранение конфиденциальности, доступности и целостности (включая подлинность, подотчетность и контролируемость) информации является главнейшей целью защиты информации. В здравоохранении конфиденциальность объектов оказания медицинской помощи зависит от сохранения конфиденциальности персональной медицинской информации. Чтобы сохранить конфиденциальность, также должны быть приняты меры по сохранению целостности данных, если это может являться единственной причиной, по которой может быть нарушена целостность данных управления доступом, журналов аудита и других системных данных способами, которые позволяют нарушениям конфиденциальности происходить или оставаться незамеченными. Кроме того, безопасность пациентов зависит от поддержания целостности персональной медицинской информации; неспособность сделать это может также привести к болезни, травме или даже смерти. Точно так же, высокий уровень доступности является особенно важным атрибутом системы здравоохранения, где лечение часто строго ограничено во времени. Действительно, стихийные бедствия, которые могут привести к перебоям в других, не связанных со здоровьем, информационных системах, могут происходить именно в то время, когда информация, содержащаяся в системе здравоохранения, наиболее необходима. Кроме того, атаки на сетевые системы типа «отказ в обслуживании» становятся все более распространенным явлением.

Элементы управления, описанные в разделе 7, это элементы, которые обозначены как подходящие для здравоохранения в целях защиты конфиденциальности, целостности и доступности персональной медицинской информации и обеспечения того, что доступ к такой информации может быть проверен и обеспечен. Эти элементы управления помогают предотвратить ошибки в медицинской практике, которые могут быть вызваны неспособностью поддерживать целостность медицинской информации. Кроме того, они помогают гарантировать поддержание непрерывности предоставления медицинских услуг.

Существуют дополнительные факторы, формирующие цели защиты медицинской информации. Они включают в себя:

a) соблюдение законодательных обязательств, закрепленных в действующих законах и положениях о защите данных, защищающих права объектов оказания медицинской помощи на неприкосновенность частной жизни[2)];

b) поддержание установленных в области информатизации здоровья рекомендованных методов конфиденциальности и защиты;

c) поддержание подотчетности на уровне отдельного человека и организации среди медицинских организаций и медицинских работников;

d) поддержка осуществления систематического управления рисками в медицинских организациях;

e) удовлетворение требований защиты, выявленных в общих ситуациях сферы здравоохранения;

f) снижение эксплуатационных расходов за счет содействия более широкому использованию технологии в безопасной, надежной, и хорошо управляемой манере, которая поддерживает, но не ограничивает, текущую деятельность в сфере здравоохранения;

g) поддержание общественного доверия к медицинским организациям и информационным системам, на которые эти организации полагаются;

h) поддержание профессиональных стандартов и этики, установленных для здоровья, профессиональными организациями, связанными со здравоохранением (в такой мере, что защита информации сохраняет конфиденциальность и целостность медицинской информации);

i) управление электронными информационными системами в области здравоохранения в среде, надлежащим образом защищенной от угроз;

j) содействия возможности взаимодействия медицинских систем, так как медицинская информация все чаще циркулирует между организациями и через границы юрисдикций (особенно в связи с этим совместимость благоприятствует надлежащему обращению с медицинской информацией для обеспечения ее постоянной конфиденциальности, целостности и доступности).

5.2 Защита информации в рамках управления информацией[3)]

В последние годы управление организацией стало одним из важнейших вопросов для организаций всех типов, в ответ на нормативные тенденции, закрепленные в таких законодательных инициативах, как американский закон Сарбейнса-Оксли о борьбе с корпоративным и бухгалтерским мошенничеством и Закон о непрерывности действия и прозрачности медицинского страхования, Европейский Базель II, доклад Тернбулла в Великобритании и Закон о контроле и прозрачности компаний (KonTraG) в Германии. Кроме того, растущая зависимость организаций от информации и обеспечивающих ей технологий, делает управление информацией важным компонентом менеджмента операционных рисков.

Многие области управления информацией, такие как аккредитации и защита данных, можно считать попадающими в область применения управления информацией. Очень важен тот факт, что область применения управления информацией охватывает и помогает непрерывному развитию защиты информации так, чтобы всегда уделялось должное внимание конфиденциальности, целостности и доступности. Защита информации, очевидно, является наиболее важным элементом, делающим возможным более широкий спектр управления информацией.

5.3 Управление информацией в рамках управления организацией и клинической практикой

В то время как медицинские организации могут отличаться в своих взглядах на управление клинической практикой и организацией, важность интеграции и заинтересованность в управлении информации должны быть выше всяких разногласий, будучи крайне важной поддержкой для обоих. Так как медицинские организации становятся все более зависимыми от информационных систем для поддержки предоставления медицинских услуг (например, путем использования технологий и тенденций поддержки принятия решений в отношении «основанной на фактических данных», а не «основанной на

[2)] В дополнение к правовым обязательствам, огромное количество информации доступно по этическим обязательствам, связанным с медицинской информацией, например этический кодекс Всемирной организации здравоохранения. Эти этические обязательства в определенных обстоятельствах могут также иметь влияние на политику защиты медицинской информации.

[3)] Следует отметить, что в некоторых странах управление информацией называют обеспечением безопасности информации.

опыте» медицинской помощи), становится все более очевидным, что события, при которых происходит потеря целостности, доступности и конфиденциальности, могут оказать существенное клиническое воздействие, и что проблемы, связанные с такими воздействиями, будут представлять собой неспособность придерживаться этических и правовых обязательств, присущих для «обязанности проявлять внимание».

Все страны и юрисдикции, несомненно, будут проводить тематические исследования, в которых будут рассматриваться случаи, когда такие нарушения привели к неверно поставленным диагнозам, смерти или затянутому выздоровлению. Поэтому рамочные основы управления клинической практикой должны рассматривать эффективное управление рисками защиты информации, как равное по значению с планами предоставления медицинских услуг, стратегиями управления инфекциями и другими «ключевыми» вопросами управления клинической практикой.

5.4 Медицинская информация, подлежащая защите

Существует несколько типов информации, конфиденциальность, целостность и доступность[4)] которой должны быть защищены:

a) персональная медицинская информация;

b) псевдонимизированные данные, полученные из персональной медицинской информации посредством определенной методики для идентификации по псевдониму;

c) статистические и научные данные, включая анонимизированные данные, взятые из персональной медицинской информации посредством удаления персонально идентифицирующих данных;

d) клинические/медицинские знания, не связанные с каким-либо отдельным объектом оказания медицинской помощи, включая клинические данные поддержки принятия решения (например, данные о нежелательной лекарственной реакции);

e) данные о работниках здравоохранения, персонале и волонтерах;

f) информация, связанная с надзором в сфере состояния здоровья населения;

g) данные журналов аудита, создаваемых медицинскими информационными системами, которые содержат персональную медицинскую информацию или псевдонимизированные данные, полученные из персональной медицинской информации, или содержащие данные о действиях пользователей в отношении персональной медицинской информации;

h) данные безопасности системы для информационных систем здравоохранения, в том числе данные контроля доступа и другие связанные с безопасностью данные о конфигурации системы для информационных систем здравоохранения.

Степень защиты конфиденциальности, целостности и доступности зависит от типа информации, целей, для которых она указывается, и рисков, которым она подвергается. Например, статистические данные [перечисление c) выше] могут не быть конфиденциальными, но защита их целостности может быть очень важна. Аналогично, для данных аудита [перечисление g) выше] может не потребоваться высокий уровень доступности (частого архивирования со временем поиска, измеряемым в часах, а не секундах, может быть достаточно в данном приложении), но их содержание может быть строго конфиденциальным. Оценка риска может правильно определить количество усилий, необходимых для защиты конфиденциальности, целостности и доступности (см. 6.4.4). Результаты регулярной оценки рисков должны соответствовать приоритетам и ресурсам организации-исполнителя.

5.5 Угрозы и уязвимости защиты медицинской информации

Виды угроз и уязвимостей защиты информации, как и их описания, широко варьируются. Хотя никто не является действительно уникальным с точки зрения здравоохранения, уникальным в здравоохранении *является* комплекс факторов, которые будут учитываться при оценке угроз и уязвимостей.

По своей природе, организации здравоохранения функционируют в среде, где никогда нельзя полностью исключить наличие посетителей и посторонних лиц в целом. В больших организациях здравоохранения само количество людей, передвигающихся в оперативных зонах, является значительным. Эти факторы повышают уязвимость систем к физическим угрозам. Вероятность того, что такие угрозы будут возникать, может увеличиться в случае присутствия эмоциональных или психически больных объектов оказания медицинской помощи или родственников.

Многие медицинские организации испытывают постоянную нехватку финансирования, и их сотрудники иногда вынуждены работать в условиях значительного стресса. Это часто может привести к

[4)] Степень доступности зависит от целей, для которых информация будет указываться.

частым ошибкам, в том числе выполнению неправильных процедур. Другие последствия таких ограничений в ресурсах, включают в себя системы, к разработке, внедрению и эксплуатации которых отнеслись крайне несерьезно, или системы, используемые в течение долгого времени после того, как их следовало снять с эксплуатации. Эти факторы могут увеличить возможность возникновения отдельных видов угроз и усугубить уязвимость. С другой стороны, клиническое лечение по-прежнему является процессом, который включает в себя большое количество профессиональных, технических, административных, подсобных и добровольных сотрудников, многие из которых рассматривают свою работу как призвание. Их преданность и разнообразие опыта часто может уменьшить подверженность уязвимостям. Высокий уровень профессиональной подготовки, полученный многими работниками здравоохранения, также отличает здравоохранение от многих других отраслей промышленности в снижении возникновения внутренних угроз.

Решающее значение правильного определения объектов оказания медицинской помощи и правильного их сопоставления с медицинскими картами приводит медицинские организации к необходимости собирать подробную идентифицирующую информацию. Региональные или юрисдикционные регистры пациентов (то есть регистры объекта оказания медицинской помощи) иногда являются наиболее полными и современными хранилищами идентифицирующей информации, доступной в юрисдикции. Эта идентифицирующая информация имеет большую потенциальную ценность для тех, кто хотел бы использовать ее для совершения кражи персональных данных, и поэтому должна быть строго защищена.

Поэтому следует с особой тщательностью рассматривать среду здравоохранения с ее специфическими угрозами и уязвимостями. Приложение А содержит информационный список видов угроз, которые должны быть рассмотрены медицинскими организациями при оценке рисков для конфиденциальности, целостности и доступности медицинской информации и для целостности и доступности соответствующих информационных систем.

6 Практический план действий по внедрению ИСО/МЭК 27002

6.1 Систематизация стандартов ИСО/МЭК 27002 и ИСО/МЭК 27001

ИСО/МЭК 27002 предоставляет стандартный перечень целей контроля в 11 областях, содержащих в общей сложности 39 основных категорий безопасности, каждая с описанием одного или нескольких средств контроля защиты. Специалисты по внедрению ИСО/МЭК 27002 в среде здравоохранения могут отметить, что большинство целей контроля применимо почти во всех ситуациях. Тем не менее, пользователям стандартов в здравоохранении также необходимо распознавать ситуации, в которых может возникнуть необходимость в дополнительных целях управления. Это часто происходит, когда клинические процессы пересекаются со специализированными устройствами, такими как сканеры, машины для инфузий и т. д., даже если средства контроля защиты относятся только к поддержанию целостности данных устройства. В разных юрисдикциях также имеются различные правовые системы, которые могут изменить требуемую область применения деятельности по согласованию.

ИСО/МЭК 27001 вводит понятие «Система менеджмента информационной безопасности (СМИБ)» и описывает необходимость этой подробной системы элементов управления, когда прилагаются усилия по достижению целей защиты, применимые согласно оценке рисков. Международный опыт и признанные передовые практические принципы защиты информации показывают, что постоянное соблюдение ИСО/МЭК 27002 может быть наилучшим образом обеспечено посредством внедрения системы управления, как показано на рисунке 1.

При наличии возможности медицинские организации должны объединять свои СМИБ с процессами управления информацией, описанными в 5.2 и 5.3, а также принять во внимание рекомендации, приведенные в 6.2—6.7.

Распространенная ошибка, в особенности среди медицинских организаций, у которых обычно отсутствуют основные требования, предъявляемые к официальной аккредитации или сертификации, заключается в том, что соответствие с ИСО/МЭК 27002 описано как основание для утверждения перечня. Для полного соответствия организации должны быть в состоянии продемонстрировать работающую СМИБ, содержащую соответствующие процессы проверки соответствия. Это соответствие хорошо вписывается в нормативно-правовую базу, в соответствии с которой обычно работают медицинские организации. См. также 7.12.

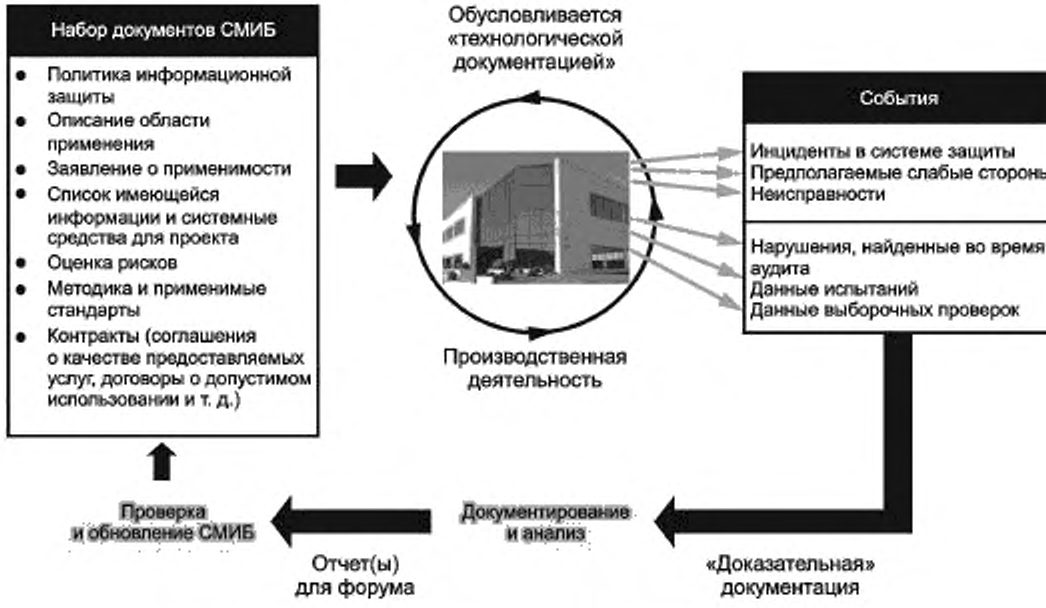

Рисунок 1 — Система менеджмента информационной безопасности

6.2 Обязательство руководства по внедрению ИСО/МЭК 27002

Прежде чем предпринимать попытки добиться соответствия с ИСО/МЭК 27002, очень важно убедиться в том, что медицинская организация имеет поддержку руководства. Очевидно, что активная приверженность и поддержка руководства необходимы для успеха. Эта приверженность должна включать в себя письменные и устные заявления о важности защиты медицинской информации и признания ее преимуществ.

Оценка рисков приносит с собой возможность обнаружения серьезных рисков, что, в свою очередь, требует существенных изменений в существующих процессах для снижения этих рисков. Должна быть явно показана личная готовность руководства к тому, чтобы подвергнуть себя и организацию изменениям в процессах и стать инициаторами этих изменений.

Если эти шаги не будут предприняты, приверженность других будет до конца полной. Могут появиться ненужные подозрения среди заинтересованных сторон о «реальной цели» программы (например, делается ли это для того, чтобы повысить эффективность защиты информации, или же для того, чтобы уменьшить количество необходимых сотрудников?).

Кроме того, руководство должно быть готово к вероятности того, что, возможно, в краткосрочной перспективе увеличение расходов, возникающее из-за перехода к новому режиму, особенно в области здравоохранения, вызовет отрицательные отзывы. Такие отзывы могут также возникнуть из ряда представлений о затрагиваемых целях и планах. Явная приверженность руководства может минимизировать подобные проблемы.

6.3 Создание, эксплуатация, обслуживание и улучшение СМИБ

6.4—6.7 настоящего стандарта дают рекомендации относительно создания и последующей эксплуатации СМИБ в области здравоохранения. Для этого требуется провести цикл мероприятий, как показано на рисунке 2.

В приложении В даны информативные примеры шагов, обычно имеющихся в каждом этапе жизненного цикла, а также примеры видов документов, связанных с каждой фазой.

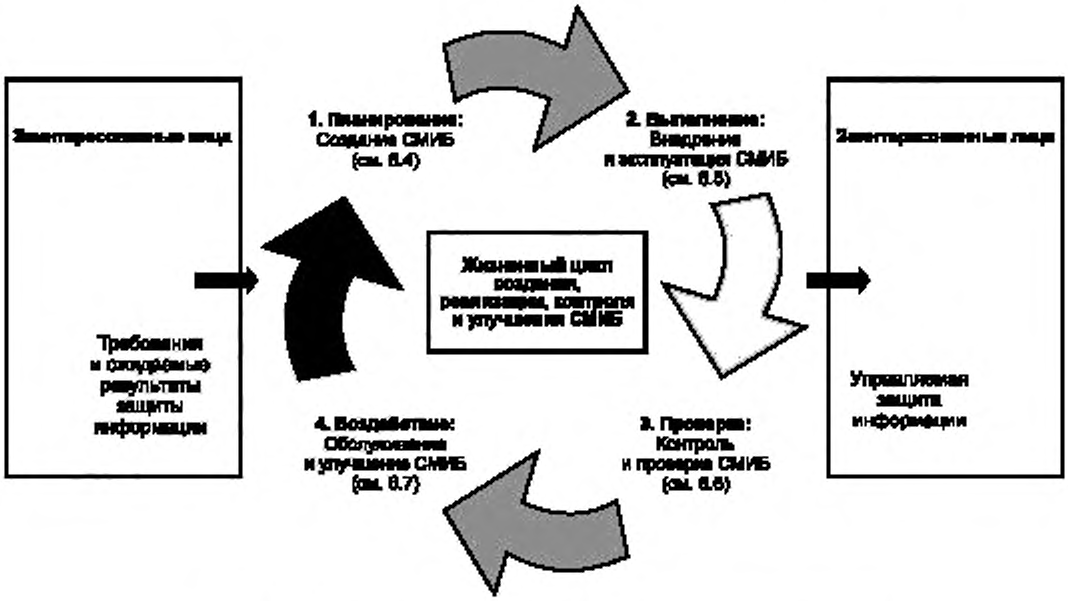

Рисунок 2 — Обзор системы менеджмента информационной безопасности

6.4 Планирование. Создание СМИБ

6.4.1 Выбор и определение области применения соответствия

6.4.1.1 Общие сведения

Теоретически, ИСО/МЭК 27002 может быть применен к целой организации. Однако опыт внедрения в Великобритании и других странах показал, что очень большим компаниям сложно с первого раза добиться того, чтобы завершить необходимую работу и предоставить необходимый уровень соответствия.

Было выявлено, что области применения соответствия, которые охватывают не более 2 или 3 участков, или около 50 сотрудников, или около десяти процессов, работают очень хорошо. По этой причине, все организации по оказанию первичной медицинской помощи, клиники, группы для предоставления медицинских услуг на дому, специалисты и отделения в больницах и т. д. сами устанавливают действующие области применения. Таким образом, для достижения полного распространения и максимальной выгоды обычно следуют пошаговому и итеративному процессу. Перспективы достижения таких результатов не должны быть подорваны выбором чрезмерно обширной области применения соответствия. Однако там, где привлечены сторонние поставщики IT-услуг, в качестве области применения для соответствия широко и с большим успехом применяется «Управление предоставлением IT-услуг».

В медицинских организациях, как и везде, в последние годы защита информации перестала быть технической или «конторской» функцией, и стала важной обязанностью корпораций.

В здравоохранении обширная взаимозависимость функций усложняет определение области применения. По этой причине очень важно правильно ее определить.

6.4.1.2 Критерии определения области применения соответствия

Чтобы надлежащим образом уравновесить «продуктивность» соответствия с корпоративной выгодой, многие организации государственного сектора, в том числе медицинские организации, определили начальную область применения «Безопасного предоставления IT-услуг». Хотя эта область применения больше связана с инфраструктурой, чем производственной деятельностью, она дает реальную корпоративную выгоду, поскольку выполняет задачи первостепенной важности, в том числе защиту инфраструктуры в целом, поощряя внедрение любых необходимых обновлений для процессов корпоративной безопасности и улучшения управления идентификационной информацией, осведомленности о защите информации и управления непрерывностью бизнеса. Как правило, во многих из этих областей корпоративная выгода выходит за рамки выбранной области применения.

Поэтому важно, чтобы для определения сферы использовались некие критерии. Критерии, как правило, являются «мягкими» и охватывают такие темы, как:

a) Желаемая степень видимости;

b) Предполагаемый баланс вовлечения техники и бизнеса;

c) Желаемая степень регионального или центрального значения;

d) Степень управляемости, представляемая областью применения.

6.4.1.3 Анализ пробелов возможного обобщенного уровня при определении области применения соответствия

Прежде чем сделать окончательное определение области применения, может быть целесообразным провести анализ пробелов на выборочной основе, чтобы таким образом получить «ощущение» того, сколько работы в различных областях может потребоваться до принятия окончательного решения. Выбор «легкой» или «сложной» области остается за организацией, хотя, по логике вещей, при выборе «тяжелых» аспектов области применения можно получить соизмеримо бóльшую корпоративную выгоду.

6.4.1.4 Контролируемое вовлечение/включение третьих сторон

Другой типичной областью, в которой допускаются ошибки, является толкование области применения. Область применения включает в себя услуги, предоставляемые третьими сторонами, и проведение необходимых вспомогательных процессов, но не определение того, как эти вспомогательные процессы проводятся.

6.4.1.5 Соглашения о качестве предоставляемых услуг (SLA) и контракты, помогающие установить область применения

SLA и контракты могут также помочь при определении области применения в той мере, в которой эти инструменты эффективно определяют границы области применения. Даже если в некоторых случаях они не делают этого явно, рассмотрение этих документов все равно будет полезным для выяснения вероятных приоритетов улучшения.

6.4.1.6 Подготовка и распространение описания области применения

Необходимо подготовить официальное описание области применения, особенно если желательна сертификация по ИСО/МЭК 27001. Описание должно быть широко обнародовано в рамках организации. Очень важно, чтобы в описании области применения были определены границы деятельности по согласованию в плане людей, процессов, мест, платформ и приложений.

В случае медицинских организаций, это описание должно быть широко обнародовано, рассмотрено и принято группами управления информацией, клиническими практиками и компаниями организации. В самом деле, известно, что некоторые медицинские учреждения ищут отзывы на заявления, сделанные профессиональными органами надзора за практикующими врачами, которые могут быть в курсе других организаций, следующих соответствию или сертификации.

См. 7.3.2.1 для информации о минимальных требованиях по описанию области применения.

6.4.2 Анализ пробелов

После того, как была выбрана область применения, следующим этапом процесса планирования является анализ пробелов, при котором осуществляется общая оценка соответствия. Передовая практика показала, что этот анализ должен быть сфокусирован на структурной организации, внедрении, документировании практической деятельности по обеспечению безопасности и свидетельств, используемых в качестве опоры для анализа. Это явно согласуется с практиками здравоохранения, где важны соответствующие навыки, записи и процедуры.

Общий сбой во время таких анализов заключается в невозможности получения сравнительных точек зрения и подтверждения дополнительными фактами. Существует вероятность, что аналитик получит отзывы, которые лишь отражают желания отдельных лиц, а не общую точку зрения, имеющуюся в существующей практике. Для того чтобы опросить специалистов и руководителей в сфере здравоохранения с целью получить разностороннее представление о вопросе, нужно время.

Целью анализа пробелов является предоставление первоначальных рекомендаций для требуемых улучшений, до получения подробной оценки рисков (см. 6.4.5.1) и обработки рисков (см. 6.4.5.2). Кроме того, анализ пробелов может предложить первоначальный порядок очередности для таких улучшений.

6.4.3 Создание или усовершенствование форума по защите медицинской информации

В основе СМИБ должен быть создан соответствующий форум по управлению защитой информации (ISMF) для контроля и управления защитой информации. И то, что является «соответствующим» в этом контексте, варьируется в зависимости от организаций, а также в зависимости от области здравоохранения.

Структурирование форума будет сложным, так как его придется приспособить к взглядам многих заинтересованных сторон, и настроить для соответствия многим нормативным обязательствам. Как функции ISMF нельзя передать или распределить без потери эффективности, так и создание ISMF нельзя воспринимать как полномочие на создание «еще одного комитета». Как правило, лучше расширить направленность существующего комитета, такого, например, как тот, который занимается рассмотрением рисков или управлением информацией.

Форум должен состоять из представителей всех служб защиты информации и управления информацией, а также представителей различных групп пользователей и представителей ключевых функций поддержки. Также туда обычно включены представители службы внутреннего аудита и управления персоналом.

Ответственный за защиту информации организации (виртуальный или реальный) должен, кроме всего прочего, делать доклады на форуме и предоставлять на нем услуги секретариата, а также должен быть ответственным за проверку, публикацию и комментирование сообщений, получаемых участниками форума.

Как описано в 5.2 и 5.3, центральный характер защиты информации в рамках управления информацией делает размещение ISMF в структуре управления информации очень разумным, но только если последняя группа, в свою очередь, связана со структурой управления клинической практикой. Управление клинической практикой затрагивает вопросы безопасности пациента, а они часто тесно связаны с защитой медицинской информации, в чем и заключается управление информацией.

Использование подхода управления информацией подчеркивает критический характер защиты информации, а также делает возможным интегрированный процесс при содействии анализа рисков, что напрямую поддерживает управление клинической практикой. Отказ от замкнутого мышления, разделяющего защиту информации, защиту данных, свободу информации, и т. д. может только помочь избежать двойных затрат и обеспечить повышенную уверенность в целостности процесса.

6.4.4 Оценка рисков медицинской информации

6.4.4.1 Общие положения

Оценка рисков является механизмом, посредством которого должна идентифицироваться система элементов управления, которая выполняет задачи ИСО/МЭК 27002. Этот процесс хорошо отображен в ИСО/МЭК/ТО 13335-3.

Существует ряд особых соображений в сфере здравоохранения, которые следует обсудить.

6.4.4.2 Роль оценки рисков защиты информации в здравоохранении

Очевидно, что здравоохранение подвержено относительно высоким рискам, особенно в таких областях, как лаборатории, отделения неотложной помощи и операционные. Поэтому наличие низких рисков в действиях, связанных с медицинской информацией, поддерживающих вышеуказанные области, следовало бы поставить под вопрос, хотя было бы ошибкой предполагать, что любая деятельность, напрямую связанная с медицинской информацией имеет отношение к предоставлению медицинских услуг.

Оценка рисков защиты информации в здравоохранении должна включать в себя рассмотрение как качественных, так и количественных факторов. Финансовые потери не должны быть одной из основных рассматриваемых проблем, но могут быть приняты во внимание там, где есть доказательства выплаты крупных сумм за халатность. Потребуется тщательная разработка рекомендаций по оценке, имеющих отношение к здравоохранению, например, руководств, признающих важность безопасности пациентов, непрерывной доступности аварийных служб, профессиональной аттестации и регулирования клинической практики.

6.4.4.3 Свойства оценки рисков с примерами из здравоохранения и ссылками на ИСО/МЭК 13335

Риск состоит из причинно-следственной связи между несколькими источниками риска. На рисунке 3 показана взаимосвязь между рисками и источников риска в ИСО/МЭК 13335, показывающая, что значение риска определяется исходя из окружающих значений активов, угроз и уязвимостей.

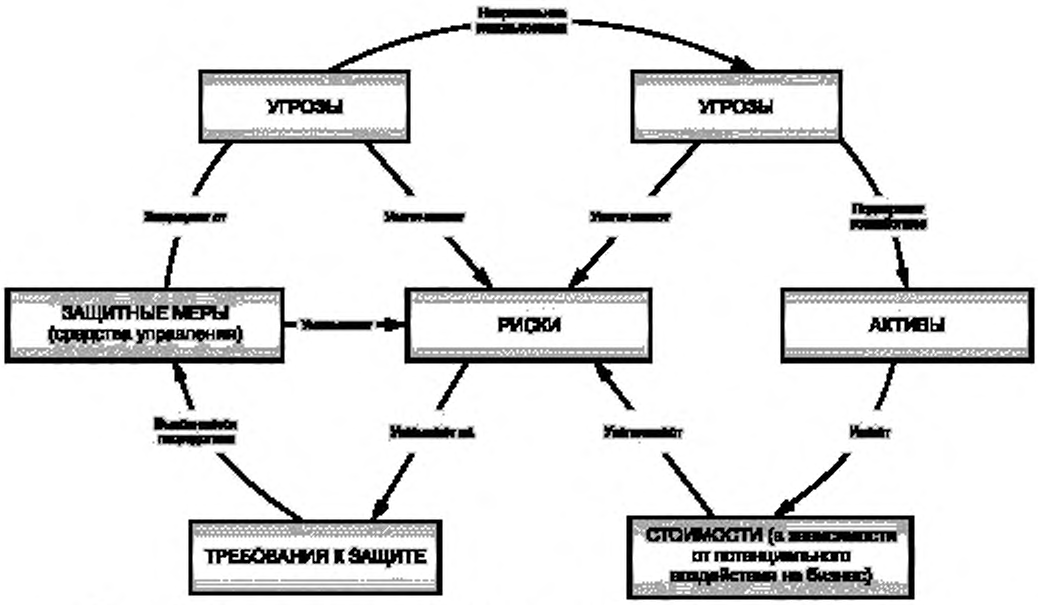

Рисунок 3 — Отношения между рисками и источниками рисков в упрощенной модели риска

Оценка рисков защиты информации и последующее управление ими, как правило, представлено так, как показано на рисунке 4.

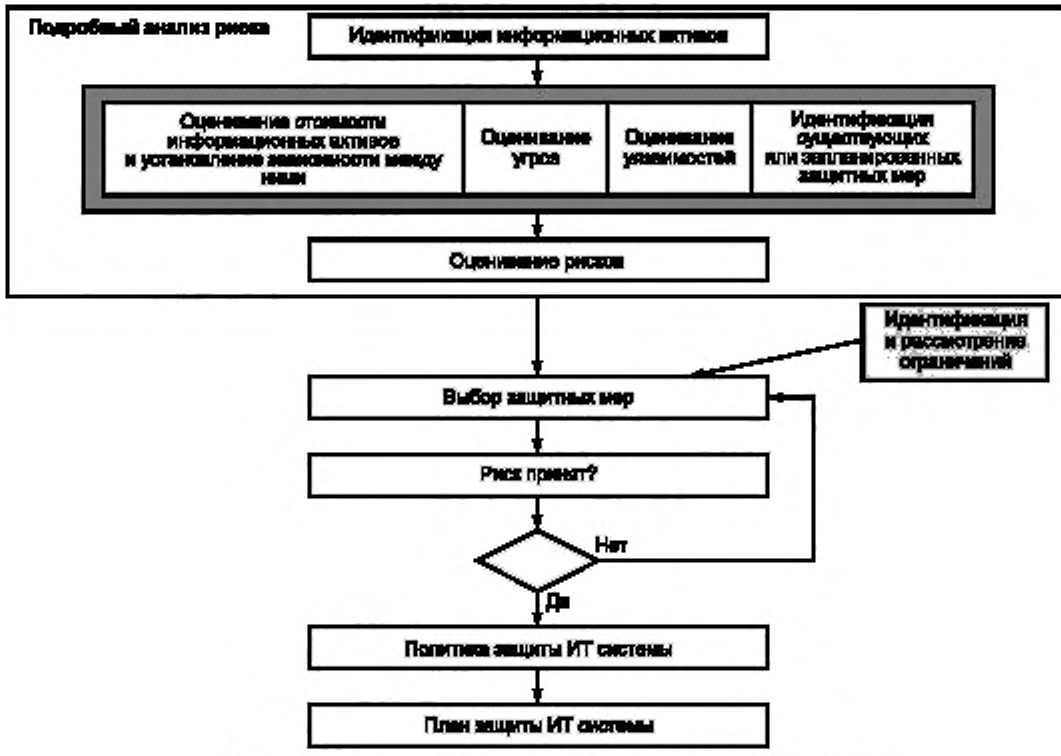

Рисунок 4 — Управление рисками с использованием анализа рисков

И ИСО/МЭК 27001, и ИСО/МЭК/ТО 13335-3 определяют компоненты риска и управление риском как:

a) идентификацию бизнес-активов, угроз и уязвимостей;

b) оценку последствий для бизнеса;

c) вероятность угроз и оценку уязвимостей;

d) определение уровней риска;

e) идентификацию рекомендованных средств контроля защиты;

f) сравнение с существующими средствами контроля, что позволяет определить области остаточного риска;

g) возможности для обработки рисков, включая прямое управление, принятие рисков, исключение рисков, управляемый перенос и т. д.;

h) планы по оценке и обработке рисков;

i) отображение решений, выбранных согласно списку в руководствах ИСО/МЭК 27002.

Все это применимо к здравоохранению, хотя «оценка последствий для бизнеса» явно должна включать в себя много различных медицинских профессий. Оценка рисков защиты информации, выполняемая медицинскими организациями, принесет выгоду, если будет следовать этой модели.

В дополнение к вышеуказанному списку, важно также сформировать представление о зависимости бизнес-процессов от IT-услуг, оборудования, программного обеспечения, мультимедиа и места. Без этого представления, следующего за оценкой последствий для бизнеса, понимание соответствующих сценариев неудачи будет почти невозможно. В свете возможного сильного воздействия на медицинские организации, понимание этих зависимостей имеет большое значение.

6.4.4.4 Требуемые навыки и вклады

Как правило, анализ рисков не может быть проведен любым человеком в одиночку, за исключением тех случаев, когда лицо выражает свое собственное мнение. Скорее, это деятельность, направленная на достижение договоренности, так что все точки зрения собираются и действительно учитываются. В действительности все люди имеют разные точки зрения и разные взгляды на допустимость риска. Для того, чтобы добиться реалистичных «сценариев наихудших случаев» воздействий, вероятностей угрозы и уязвимостей, скорее всего, будет необходимо учитывать проблемы, даже гипотетические и маловероятные.

Естественно, реальные случаи из прошлого по умолчанию являются реалистичными, но они могут не быть худшими. Для определения наихудших случаев могут потребоваться специалисты в этой области. Однако сценарии с несколькими условными операторами вряд ли будут реалистичными. Работники здравоохранения, скорее всего, извлекут выгоду из работы IT-персонала, который будет в состоянии идентифицировать виды отказов и сценарии, требующие оценки.

Эффективная оценка рисков защиты информации в сфере здравоохранения требует наличия следующих знаний и навыков:

a) знания в области ухода за больным и клинической практики, в том числе ведение записей и составление направлений для предоставления медицинских услуг;

b) знание форматов клинических данных и возможность злоупотребления этими данными;

c) знание факторов внешней среды, что может усилить или смягчить любой или все уровни компонентов риска, описанных выше;

d) информация об атрибутах IT и медицинского прибора и характеристики работоспособности / отказа медицинского оборудования;

e) знание предыдущих происшествий и сценариев реальных случаев воздействия;

f) детальное знание системной архитектуры;

g) знание программ по контролю над изменениями, которые могут внести изменения в любой уровень компонентов риска или во все сразу.

6.4.4.5 Требуемые результаты

ИСО/МЭК ТР 13335-3 определяет следующие обычные результаты:

a) отчет об оценке рисков;

b) план обработки рисков.

Кроме того, медицинские организации должны также выполнять:

c) модели активов/зависимостей (в поддержку оценки рисков);

d) отчеты о состоянии средств управления;

e) итоговые отчеты по обработке рисков (в поддержку анализа пробелов и заявлений о применимости).

Поскольку здравоохранение — это сектор, имеющий обязательства (как юридические, так и профессиональные) по соблюдению соответствия и ответственности по управлению рисками, результат, который отображает все связанные оценки риска, выполненные специалистами разных направлений или функциональных групп, следует рассматривать как помощь в эффективном управлении информацией и обеспечении целостности отдельных оценок риска.

6.4.5 Управление рисками

6.4.5.1 Оценка рисков

Оценка рисков предназначена быть средством достижения цели. Она не должна быть самоцелью, но часто именно так и оказывается. Это особенно относится к средам с ограничениями по ресурсам, как, например, во многих медицинских организациях. Управление рисками реагирует на оценку выявлением того, какие элементы управления следует усилить, какие элементы управления уже эффективно размещены и какие дополнительные элементы управления организация должна внедрить для того, чтобы снизить остаточный уровень риска до приемлемого уровня.

Возрастающая взаимосвязь информационных систем здравоохранения делает управление рисками в здравоохранении особенно сложным, так как немногие медицинские организации могут работать так, как будто их системы информации являются изолированными. Оценка рисков в здравоохранении часто затрагивает вопросы о безопасном хранении информации, праве собственности на информацию и ответственности за информацию. Действенное управление рисками должно обеспечивать регулировку ответственности за защиту информации и полномочий на принятие решений по управлению рисками.

6.4.5.2 Обработка рисков

Чтобы четко отличать процесс управления рисками в целом от управления выявленными рисками, в стандарте Австралии и Новой Зеландии AS/NZ 4360 было введено понятие «обработка рисков». Это понятие впоследствии было принято стандартом ИСО/МЭК 27001.

«Обработка рисков» обозначает деятельность по снижению риска до приемлемого уровня (признавая, нельзя предоставить достаточный объем ресурсов для того, чтобы даже попытаться полностью предотвратить риски). Обработка рисков особенно уместна для медицинских организаций, фактически принося с собой понятия «обрабатывать, передавать или допускать» по отношению к рискам.

Определение того, что является приемлемым, является и должно оставаться специфичным для организации и работающего в ней персонала. Оно должно отражать склонность организации к рискам и должна быть использована для обеспечения того, что расходы на улучшение защиты информации оправданы, и представляет собой явно хорошее использование ограниченных финансовых ресурсов.

6.4.5.3 Критерии приемлемости рисков

Медицинские организации должны определить и задокументировать свои критерии приемлемости рисков. Факторов, которые следует учитывать, множество и они являются переменными, однако следует рассмотреть для включения следующее:

a) стандарты сектора здравоохранения, промышленности или организации;
b) клинические или другие приоритеты;
c) соответствие корпоративной культуре;
d) реакции объектов оказания медицинской помощи;
e) согласованность со стратегией приемлемости рисков IT, клиники и компании;
f) стоимость;
g) эффективность;
h) тип защиты;
i) количество охватываемых угроз;
j) уровень риска, при котором элементы управления становятся оправданными;
k) уровень риска, который привел к созданию рекомендаций;
l) уже действующие альтернативы;
m) дополнительные полученные выгоды.

Взятые вместе, эти факторы дадут оценку рентабельности, которая может подкрепить необходимое экономическое обоснование для поиска финансирования.

Решение, как правило, принятое ISMF, согласно которому определенный элемент управления не должен быть внедрен, имеет полную силу, но должно быть официально зарегистрировано для периодического обзора и переоценки. Медицинские организации должны документировать принятые риски.

6.4.5.4 Планы по управлению особыми областями рисков

Вышеуказанный процесс должен включать в себя соглашение о том, когда (хотя для него приемлемо и «никогда») будут приняты меры по снижению выявленного риска посредством внедрения элемента(ов) управления.

Планы по будущему внедрению должны быть отражены в плане по улучшению защиты организации.

6.4.6 Планирование улучшения защиты

Полномочия по плану улучшения защиты по поручению ISMF должны получить лица, ответственные за защиту информации организации, лица, ответственные за защиту данных, специалисты по управлению рисками, или аналогичные ответственные лица организации.

Часто выполненные в формате диаграммы Гантта, планы должны быть доступны для персонала медицинского учреждения и других сотрудников, так как они, как правило, не являются конфиденциальным документом. На самом деле, они часто могут быть полезны для демонстрации прогресса и улучшения процесса.

Такие планы будут наиболее эффективны при сведении к минимуму перерывов в работе, если они объединяют внесение улучшений в обеспечение защиты информации с планируемыми изменениями в IT-средствах и предоставлением медицинских услуг. Они также должны отражать признанные периоды необычной активности в здравоохранении, такие как поступление новой группы врачей-интернов или студентов-практикантов.

6.4.7 Заявление о применимости

Заявление о применимости можно рассматривать как краткий обзор состояния защиты информации в организации, трактовки организацией требований защиты и ее стратегии для реализации решений в области защиты. Этот документ ведется лицом, ответственным за защиту информации, или аналогичным ответственным лицом по поручению ISMF, и он должен быть предоставлен службам по управлению организацией и клинической практикой с целью формирования основной части пакета документов по управлению. Также его формат, как правило, подходит для использования в качестве инструмента для оценки или подтверждения для поддержки внешнего аудита, клинического обеспечения и других надзорных проверок.

6.4.8 Набор документов СМИБ

Модель СМИБ, указанная в 6.1, описывает требуемую документацию (см. рисунок 1). Основные документы это:

a) политика компании в области защиты информации;

b) описание области применения;

c) заявление о применимости;

d) перечень информационных активов и бизнес-активов, которые необходимо защищать;

e) планы и отчеты по оценке рисков;

f) принятые методики и стандарты;

g) соглашения, основанные на договорах (включая соглашение о качестве предоставляемых услуг и соглашение о допустимом использовании).

Кроме того, работа СМИБ и ее успехи в соответствии потребностям и приоритетам клинической практики может значительно облегчиться, если эти приоритеты оформляются службами управления клинической практики и компании, а затем хранятся СМИБ как часть набора документов. Затем этот документ предоставляет вспомогательный материал для поддержки решений о принятии рисков, принятых СМИБ.

Приложение В содержит набор документов СМИБ и связанные с ним документы по различным этапам создания или улучшения СМИБ.

6.4.9 Потенциальная возможность упрощения посредством использования инструментов

Процесс приведения в соответствие с ИСО/МЭК 27002 предполагает ряд этапов, в ходе которых создается значительное количество информации и документации. Тем не менее, медицинские организации существуют в изменчивой окружающей среде, в которой меняются риски и внедряются новые элементы управления. Поэтому необходимо поддерживать общую целостность этой информации и документации.

Кроме того, ступенчатый, составной, расширяющийся и цикличный характер задействованных процессов свидетельствует о том, что информация неоднократно обрабатывается и повторно используется в нескольких процессах, при этом результаты последнего процесса часто требуют внесения поправок на более раннем этапе. Наконец, решения будут принимаются в свете целого ряда факторов, которые требуют множества перекрестных ссылок.

Медицинские организации должны рассмотреть вопрос о применении инструментов для поддержки соответствия ИСО/МЭК 27002. Приложение С содержит подробное обсуждение потенциальной пользы и необходимых атрибутов таких инструментов.

6.5 Действие. Внедрение и эксплуатация СМИБ

Внедрение СМИБ включает в себя несколько этапов.

a) **Создание плана обработки рисков:** после выявления рисков в ходе анализа, они должны быть рассмотрены и либо приняты высшим руководством, либо минимизированы, если риск считается неприемлемым. План обработки рисков разъясняет мероприятия, которые необходимо провести для снижения неприемлемых рисков. Он включает в себя план внедрения средств контроля защиты, выбранный (на основе результатов оценки рисков) для снижения или смягчения этих недопустимых рисков. ISMF несет ответственность за осуществления этого плана. Теоретически, план обработки рисков будет включать в себя расписания, приоритеты и подробные планы работы, а также будет распределять обязанности по внедрению средств контроля защиты. В сфере здравоохранения утверждение таких планов может задействовать как службы управление информацией, так и службы управления клинической практики.

b) **Распределение ресурсов:** важная роль управления заключается в обеспечении необходимыми ресурсами (людьми, системами и финансированием) для защиты активов медицинской информации.

c) **Выбор и внедрение средств контроля защиты:** раздел 7 рассматривает каждый из одиннадцати пунктов о защите ИСО/МЭК 27002 и дает советы и рекомендации по правильному выбору средств контроля защиты в среде здравоохранения.

d) **Подготовка и обучение:** в 7.5.2.2 обсуждаются требования по подготовке и обучению всех сотрудников, подрядчиков, специалистов здравоохранения и других лиц, имеющих доступ к информационным системам здравоохранения и персональной медицинской информации.

e) **Управление работой:** надлежащая непрерывная работа СМИБ является существенным фактором, если необходимо поддерживать конфиденциальность, целостность и доступность медицинской информации и информационных систем. В 7.7 говорится об аспектах управления работой, связанных со здоровьем.

f) **Управление ресурсами:** эффективное обеспечение защиты информации может быть дорогим и может быть недостаточно компетентных человеческих ресурсов. Действенное определение приоритетов посредством ISMF и тщательное управление людьми и ресурсами необходимы для обеспечения эффективной непрерывной работы.

g) **Управление инцидентами в системе безопасности:** для минимизации последствий инцидентов в системе безопасности, важно, чтобы инцидент был надлежащим образом обнаружен, а корректирующие действия предприняты. Методическое руководство по инцидентам в системе безопасности должно быть подготовлено и подлежит регулярной проверке. Это особенно важно для определения обязанностей и шагов действия на начальном этапе реагирования, так как события могут разворачиваться быстро, а критический характер информационных систем здравоохранения дает мало времени на размышления в то время, когда в системе безопасности возникает инцидент. Четкие процедуры отчетности для инцидентов в системе безопасности также имеют важное значение для того, чтобы сохранялось доверие заинтересованных сторон системы здравоохранения и чтобы лица, ответственные за управление клинической практикой и компанией, были в курсе важных событий и их последствий. В 7.10 содержится подробное обсуждение управления инцидентами в системе безопасности.

6.6 Проверка. Мониторинг и проверка СМИБ

6.6.1 Необходимость в постоянной гарантии

Организации, СМИБ и ISMF в рамках СМИБ требуют гарантии его эффективности при поддержании нынешнего уровня защиты и при ее постоянном улучшении в соответствии со стратегией обеспечения защиты информации в соответствии с целями организации.

Для обеспечения данной гарантии доступен ряд вариантов. Эти варианты могут быть использованы в комбинации друг с другом. Менее дорогие возможности предоставляют соразмерно меньшую гарантию, отражающую предлагаемые ими ограниченную строгость и независимость. Медицинские организации должны создавать программы для проверки соответствия, которые используют комбинацию технологии и подходы.

6.6.2 Оценка соответствия

6.6.2.1 Самостоятельная оценка

На базовом уровне, особенно там, где внедрение ИСО/МЭК 27001 проводится исключительно для внутренних целей, оценка, выполненная небольшой группой из других подразделений организации,

даст некоторое представление об эффективности СМИБ. Тем не менее такой подход часто может быть скомпрометирован лояльностью и личными и организационными обязательствами коллег.

6.6.2.2 Рецензирование

Очень похожим, но альтернативным вариантом является проведение рецензирования, при котором различные организационные связи рецензентов способны привести к росту объективности и, следовательно, обеспечению гарантии.

Этот вариант также может быть осуществлен бесплатно, если он организован на взаимной основе, например, между лицами, ответственными за защиту информации. Тем не менее, это, конечно, может означать, что присутствует возможность договоренности о взаимно положительных отчетах.

6.6.2.3 Независимый аудит

Независимые аудиты могут быть по определенной стоимости проведены различными организациями, такими как аудиторские и консалтинговые компании или собственные внутренние аудиторы организации. Вероятно, итоговый отчет будет надежным и более высокого качества, отражая, как правило, более высокий уровень компетентности. Такие проверки дают «сравнительную оценку», поскольку вовлеченный персонал, скорее всего, уже проводил другие подобные независимые аудиты, на основе которых они могут проводить сравнения.

6.6.2.4 Сертификационный аудит на соответствие ИСО/МЭК 27001

Сертификационные аудиты обычно включают в себя совещание по определению объемов работ, обзор документа, а затем саму проверку соответствия.

Основываясь на опыте, накопленном другими сертифицированными организациями, медицинские организации должны привлекать аудиторов этих организаций, сразу после принятия решения о проведении сертификации. Затем аудитор становится скорее партнером по проведению аудита, а соответствие может быть достигнуто постепенно, например, по предварительной договоренности о том, что описание области применения, оговоренное в 6.4.1, правильно сформулировано и может быть предоставлено. Тем не менее, также стоит рассмотреть возможность проведения рецензирования или независимого аудита на промежуточном этапе для дальнейшего предотвращения любой возможности возникновения сбоя.

Распространенным заблуждением является то, что сертификация осуществляется, только если наблюдаемая защита информации, так или иначе, является «идеальной». Требованием является лишь наличие уже функционирующей СМИБ, четкое понимание рисков и воздействий, и план управления для снижения этих воздействий до приемлемого уровня. На самом деле, в процессе аудита может быть выявлено ограниченное число неисправностей, которые, в зависимости от их значимости, не помешают успешному проведению сертификации.

Существует также ошибочное мнение, что сертификация требует много времени. Тем не менее, опыт показывает, что сертификационные аудиты медицинских организаций не занимают у аудитора по сертификации более 5—6 рабочих дней.

Окончательным независимым аудитом является аудит, проведенный компетентным, независимым аудиторским органом в соответствии с руководствами ИСО 27001, как это установлено во многих странах. Данный вид аудита является наилучшим из перечисленных здесь вариантов, так как он осуществляется профессиональным аудитором. Такой аудитор должен также быть компетентен в области IT и защиты информации. Следовательно, уровень тщательности проведенного аудита и сравнительной оценки методик, которые можно ожидать от такого аудита, высок. Тем не менее, опыт показывает, что стоимость такого аудита все равно является приемлемой.

Пользователям настоящего международного стандарта, которые решили использовать этот вариант, настоятельно рекомендуется привлекать таких аудиторов при запуске своей программы так, чтобы их поддержка и участие проявлялись постепенно и так, чтобы их окончательное утверждение было более вероятным, учитывая, что не возникнет никаких «неожиданностей» на заключительном этапе аудита.

6.7 Улучшение. Обслуживание и улучшение СМИБ

Результаты мониторинга, описанного в 6.6, должны быть переданы ISMF для дальнейшего рассмотрения, так как именно ISMF отвечает за обеспечение исправления недостатков, и за то, что СМИБ остается эксплуатационно-эффективным.

SOA, описанное в 6.4.7, может быть эффективным инструментом для информирования лиц, ответственных за управление клинической практикой и компанией, о текущем состоянии СМИБ. Формат,

используемый для SOA, также обычно подходит для использования в качестве инструмента оценки или подтверждения в поддержку внешнего аудита, клинического обеспечения и других надзорных проверок.

План по улучшению защиты, описанный в 6.4.6, также является важным инструментом в демонстрации прогресса и усовершенствования процессов.

7 Использование ИСО/МЭК 27002 в здравоохранении

7.1 Общие положения

Данный раздел содержит конкретные рекомендации по одиннадцати пунктам управления защитой и 39 основным категориям управления защитой, описанным в ИСО/МЭК 27002.

Основным принципом, указанным в ИСО/МЭК 27002, является то, что каждая организация может рассматривать и трактовать данный документ в своем собственном контексте и с учетом нормативных и бизнес-требований. Тем не менее, опыт, накопленный в ряде стран, включая Австралию, Канаду, Францию, Нидерланды, Новую Зеландию, Южную Африку и Великобританию, показал необходимость включения определенных разделов и категорий управления, если речь идет о защите персональной медицинской информации. Основываясь на этом опыте, в соответствующих случаях указаны минимальные требования, а в некоторых случаях изложены нормативные руководства, описывающие надлежащее применение определенных элементов контроля защиты, описанных в ИСО/МЭК 27002, для защиты медицинской информации. Эти минимальные требования имеют настолько большое значение для обеспечения защиты персональной медицинской информации, что любые медицинские организации, которые не соответствуют им, не могут считаться соответствующими этому стандарту.

В каждом последующем подразделе даны руководства в дополнение к руководствам, имеющимся в ИСО/МЭК 27002, но не в качестве замены для них.

7.2 Политика защиты информации

7.2.1 Документы по политике защиты информации

Контроль

Организации, занимающиеся обработкой медицинской информации, в том числе личной медицинской информации, **должны** иметь политику по защите информации в письменном виде, одобренную руководством, опубликованную, а затем доведенную до всех сотрудников и соответствующих сторонних организаций.

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, касательно того, что должен содержать документ о политике по защите информации, этот документ **должен** содержать заявления:

a) о необходимости защиты медицинской информации;

b) целях защиты информации;

c) области применения соответствия, как описано в 6.4.1.6;

d) законодательных, нормативных и контрактных требованиях, включая те, которые касаются защиты персональной медицинской информации, а также юридических и этических обязанностей работников здравоохранения для защиты этой информации;

e) средствах для оповещения об инцидентах в системе защиты информации, в том числе канал связи для поднятия вопроса о конфиденциальности, не опасаясь обвинений или взаимных упреков.

Теоретически пересмотр содержания этой политики будет зависеть от результатов оценки рисков организации, хотя сама политика должна только задавать направление, устанавливать принципы и указывать на другие документы, где следует найти (чаще меняющиеся) особенности.

При создании своего документа о политике по защите информации, медицинские организации должны будут специально учитывать следующие факторы, которые являются специфичными для сектора здравоохранения:

f) объем медицинской информации;

g) права и этические обязанности персонала, как оговорено в законе и принято членами профессиональных организаций;

h) где возможно, права объектов оказания медицинской помощи на неприкосновенность частной жизни и на доступ к записям о ней;

i) обязанности практикующих врачей касательно получения согласия на получение информации от объектов оказания медицинской помощи и сохранения конфиденциальности персональной медицинской информации;

j) законные основания практикующих врачей и медицинских организаций при необходимости не следовать протоколам системы безопасности, если приоритеты здравоохранения, часто связанные с неспособностью отдельных объектов оказания медицинской помощи выразить свои предпочтения, требуют подобное несоблюдение протокола; также процедуры, которые необходимо осуществлять для достижения этой цели;

k) обязанности соответствующих медицинских организаций и объектов оказания медицинской помощи в случае, когда оказание медицинских услуг происходит на основе «совместного ухода» или «стационарной помощи с реабилитацией»;

l) протоколы и процедуры, которые должны применяться при обмене информацией с целью проведения исследования и клинических испытаний;

m) средства и пределы полномочий для временных работников, таких как временные заместители врачей, студенты и персонал, являющийся на работу «по вызову»;

n) средства и установленные ограничения на доступ к персональной медицинской информации для волонтеров и вспомогательного персонала, такого как священники и персонал, работающий на благотворительной основе.

Многие организации здравоохранения посчитали полезным сделать документ о политике доступным для сотрудников в электронном виде посредством использования области защиты информации во внутренней сети организации здравоохранения.

Если медицинская организация получает поддержку от сторонних организаций или сотрудничает с третьими сторонами, в частности в случаях, когда она получает услуги от других юрисдикций, структура политики **должна** включать в себя задокументированную политику, средства контроля и процедуры, которые охватывают эти взаимодействия и указывают обязанности всех сторон. В случаях, когда личные данные передаются за пределы страны, **должны** применяться положения ИСО 22857.

7.2.2 Проверка документа о политике защиты информации

Контроль

Политика защиты информации медицинской организации **должна** подлежать постоянной поэтапной проверке, так чтобы вся совокупность политики подлежала ежегодному рассмотрению. Эту политику **следует** пересмотреть после возникновения серьезного инцидента в системе безопасности.

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, такая проверка **должна** охватывать:

a) изменчивый характер работы медицинских организаций и сопутствующие изменения, вносимые в профили рисков и управление рисками;

b) изменения, вносимые в IT-инфраструктуру организации, и сопутствующие изменения в профиле рисков организации;

c) изменения, обнаруженные во внешней среде, которые схожим образом влияют на профиль рисков организации;

d) новейшие средства контроля, требования по соответствию и обеспечению соответствия, а также средства, установленные органами здравоохранения юрисдикции или новыми законодательными актами или постановлениями в качестве обязательных;

e) новейшие руководства и рекомендации в отношении персональной медицинской информации от профессиональных ассоциаций здравоохранения и от комиссий по конфиденциальности информации;

f) результаты судебных дел, проверенные в судах, которые установили или опровергли прецеденты или общепринятые практики;

g) задачи и вопросы касательно политики, поставленные перед организацией ее персоналом, объектами оказания медицинской помощи, а также их партнерами и медработниками, исследователями и органами государственного управления (например, представителями комиссий по обеспечению конфиденциальности).

7.3 Организация защиты информации

7.3.1 Общие сведения

Руководство медицинской организации несет ответственность за защиту персональной медицинской информации и других защищенных данных о здоровье, обрабатываемых организацией. На это

особенно стоит обратить внимание организациям, которые полагаются на услуги внешнего управления, предоставляемые третьими сторонами. Эффективное взаимодействие также является важным элементом в поддержании защиты информации. И то, и другое требуют явной и четкой инфраструктуры менеджмента информационной безопасности.

7.3.2 Внутренняя организация

7.3.2.1 Направленность руководства на защиту информации, согласование защиты информации и распределение ответственностей за защиту информации

Контроль

Организации, занимающиеся обработкой персональной медицинской информации, **должны**:

a) четко определять и распределять ответственность за защиту информации;

b) иметь ISMF для уверенности в том, что существует четкое управление и ощутимая поддержка руководства в мероприятиях по обеспечению защиты, затрагивающих защиту медицинской информации, как указано в 6.4.3.

Минимум один человек **должен** нести ответственность за защиту медицинской информации в организации.

Форум по защите медицинской информации **должен** проводить собрания минимум раз в месяц. (Как правило, наиболее эффективно собираться в промежутке между собраниями руководящего органа, во время которого Форум предоставляет отчеты. Это позволяет обсудить неотложные вопросы на собрании за небольшое время.)

Должно быть составлено официальное описание области применения, которое определяет границы мероприятий по обеспечению соответствия в отношении людей, процессов, мест, платформ и приложений.

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, важно отметить существенный характер ответственности руководства в организациях, которые являются хранителями персональной медицинской информации, как описано в 6.2. Подотчетность и согласование можно обеспечить только в долгосрочной перспективе, если организация имеет явную инфраструктуру менеджмента информационной безопасности.

Независимо от утвержденной организационной структуры, очень важно, чтобы она была спроектирована и структурирована таким образом, чтобы облегчить доступ объектов оказания медицинской помощи (например, чтобы сделать запросы на получение персональной медицинской информации), чтобы облегчить отчетность в рамках организационной структуры и обеспечить своевременное предоставление информации.

Как отмечалось в 6.4.3, ответственный за защиту информации организации (виртуальный или реальный) **должен**, кроме всего прочего, делать доклады на форуме и предоставлять услуги секретаря. Он **должен** быть ответственным за проверку, публикацию и комментирование сообщений, получаемых участниками форума.

Медицинские организации **должны** обнародовать описание области применения в пределах организации, затем пересмотреть его и убедиться, что оно принято информацией организации, группами управления клинической практикой и организацией.

7.3.2.2 Процесс авторизации средств обработки информации

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.3.2.3 Соглашения о конфиденциальности

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** иметь соглашение о конфиденциальности, определяющее конфиденциальный характер этой информации. Соглашение **должно** быть применимо к персоналу, имеющему доступ к медицинской информации.

Руководство по внедрению

Вышеуказанное соглашение **должно** включать в себя ссылки на взыскания, возможные при обнаружении нарушения политики защиты информации.

7.3.2.4 Связь с властями, связь со специальными группами по интересам и независимый обзор защиты информации

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.3.3 Третьи стороны

7.3.3.1 Идентификация рисков, связанных со сторонними организациями

Контроль

Организации, занимающиеся обработкой медицинской информации, **должны** оценивать риски, связанные с доступом третьих сторон к этим системам или содержащимся в них данным, а затем внедрять элементы контроля защиты, подходящие для определенного уровня риска и для использованных технологий.

Руководство по внедрению

Оценка рисков необходима для эффективного управления доступом третьих сторон к системам, содержащим медицинскую информацию, а в особенности персональную медицинскую информацию. Должны защищаться права субъектов оказания медицинской помощи, даже когда сторонняя организация, имеющая возможность доступа к персональной медицинской информации, располагается в юрисдикции, отличной от той, которая руководит субъектом оказания медицинской помощи или медицинской организацией.

7.3.3.2 Решение вопросов безопасности при работе с клиентами

Нет дополнительных руководств по менеджменту защиты информации в сфере здравоохранения.

7.3.3.3 Решение вопросов безопасности при соглашениях с третьими сторонами

Контроль

Медицинские организации, пользующиеся услугами третьих сторон, при которых сервисы третьих сторон обрабатывают персональную медицинскую информацию, **должны** использовать официальные контракты, в которых оговаривается:

a) конфиденциальный характер и ценность персональной медицинской информации;

b) меры по защите, которые должны быть применены и/или требования которых должны быть соблюдены;

c) ограничения доступа третьих сторон к этим сервисам;

d) качество предоставляемых услуг, которого нужно достигнуть в случае предоставления этих услуг;

e) формат и частота предоставления отчетов в ISMF медицинской организации;

f) организация участия третьей стороны на соответствующих собраниях медицинской организации, а также в рабочих группах;

g) средства для осуществления надзорного аудита третьих сторон;

h) взыскания, производимые в случае несоблюдения любого из вышеуказанных условий.

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, вышеуказанные требования должны гарантировать то, что когда медицинская организация перестает напрямую контролировать поток информации, конфиденциальность, целостность и доступность персональной медицинской информации будут сохранены. Для информации, пересекающей границы юрисдикций, существуют инструкции, указанные в ИСО 22857.

В случаях, когда третья сторона не занимается обработкой персональной медицинской информации, все равно может быть уместна соответствующая подгруппа вышеуказанных элементов контракта. Во всех случаях предоставления услуг третьей стороной должно быть внедрено соглашение, оговаривающее минимальный набор элементов управления защитой, который должен быть применен.

7.4 Управление активами

7.4.1 Ответственность за активы медицинской информации

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны**:

a) отвечать за активы медицинской информации (т.е., поддерживать уровень таких активов);

b) иметь назначенного хранителя этих активов медицинской информации;

c) иметь правила для надлежащего применения этих активов, которые идентифицированы, задокументированы и внедрены.

Руководство по внедрению

Организации, занимающиеся обработкой медицинской информации, **должны** иметь правила для поддержания актуальности этих активов (например, актуальность баз данных по лекарствам) и целостности этих активов (например, функциональная целостность медицинских приборов, записывающих или сообщающих данные).

Медицинские приборы, записывающие или сообщающие данные, могут потребовать особых мер предосторожности в связи со средой, в которой они функционируют, а также в связи с электромагнитным излучением, происходящим во время их работы. Такие приборы **должны** быть особенным образом идентифицированы.

7.4.2 Классификация медицинской информации

7.4.2.1 Руководства по классификации

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** единообразно классифицировать такие данные как конфиденциальные.

Руководство по внедрению

Определение уровней защиты информационных активов в здравоохранении является комплексным, а сравнение с классификацией правительственной или военной информации может ввести в заблуждение. Ниже указаны важные характеристики информационных активов в рамках здравоохранения.

a) Конфиденциальность персональной медицинской информации всегда скорее субъективна, чем объективна. Другими словами, в целом только субъект данных (т.е., объект оказания медицинской помощи) может надлежащим образом определить относительную конфиденциальность различных областей или групп данных. Например, человек, избегающий насильственных отношений, может посчитать свой новый адрес и номер телефона конфиденциальной информацией, в отличие от клинических данных о состоянии его сломанной руки;

b) Конфиденциальность персональной медицинской информации зависит от контекста. Например, имя и адрес объекта оказания медицинской помощи в списке допуска к отделению неотложной помощи больницы может расцениваться им как не особо конфиденциальная информация, а его имя и адрес в списке допуска к лечению импотенции может расцениваться им как в крайней степени конфиденциальная информация;

c) Конфиденциальность персональной медицинской информации в медицинской карте пациента может со временем меняться. Например, изменение общественных мнений за последние 20 лет привело к тому, что многие объекты оказания медицинской помощи не стремятся скрыть свою сексуальную ориентацию. И наоборот, отношение к наркотической и алкогольной зависимости привело к тому, что на данный момент многие объекты оказания медицинской помощи расценивают данные о прохождении консультации у врача по вопросам зависимости в большей степени конфиденциальными, чем это было 20 лет назад.

Поскольку нельзя предсказать чувствительность данного элемента персональной медицинской информации в отношении всех его применений и всех этапов его жизненного цикла, персональная медицинская информация **должна** всегда подлежать соответствующему уровню защиты. Обратите внимание, что в то время как вся персональная медицинская информация должна быть в равной степени классифицирована как конфиденциальная, из практических соображений может потребоваться идентификация записей об объекте оказания медицинской помощи, которые подвержены повышенному риску доступа неуполномоченными лицами. Среди них работники самой организации (особенно если их состояние влечет за собой эмоциональное поведение), главы правительства, знаменитости, политики, работники СМИ и участники групп, подвергающиеся особенно высоким рискам (например, люди с заболеваниями, передающимися половым путем или те, чья персональная медицинская информация содержит записи о предрасположенности к серьезным заболеваниям). Может потребоваться особая маркировка записей о таких людях, так чтобы можно было четко контролировать доступ. Однако, при применении таких схем нужно быть крайне осторожными, так как такая маркировка может обострить проблему, для решения которой она создается, например, она может привлечь внимание к определенным частям информации, которые промаркированы. Также стоит подчеркнуть, что в то время как некоторые лица подвержены повышенным рискам, их персональная медицинская информация изначально не является в большей степени конфиденциальной, чем информация других объектов оказания медицинской помощи. *Вся* персональная медицинская информация является конфиденциальной и с ней следует обращаться надлежащим образом. См. также обсуждение в 7.5.2.1.

Выявление и (в случае необходимости) нанесение защитной маркировки о конфиденциальности информационных активов может стать важным инструментом в подготовке кадров и в соответствии политике. Это лучше всего работает, когда классификация действует в качестве индикатора необходимых методик обработки информации. Классификация также может быть важным компонентом соглашений

о защите данных между юрисдикциями и со сторонними организациями и их сотрудниками. Идентификация и маркировка информационных активов также является важным компонентом ИСО/МЭК 27002.

В дополнение к традиционной классификации данных на основе их чувствительности к раскрытию, в классификации также нуждается критичность информации, т.е. насколько большое значение имеют наличие и целостность информации для непрерывного предоставления медицинской помощи. Факторы времени, вовлеченные в процессы клинической практики, часто играют решающую роль в определении требований к доступности для персональной медицинской информации. Классификация в отношении доступности, целостности и критичности также должна применяться к методикам, IT-устройствам, программному обеспечению, расположению и персоналу. Критичность **должна** быть идентифицирована с помощью оценки рисков.

7.4.2.2 Маркировка и обработка информации

Контроль

Все информационные системы здравоохранения, занимающиеся обработкой персональной медицинской информации, **должны** информировать пользователей о конфиденциальности персональной медицинской информации, к которой система имеет доступ (например, при запуске или входе в систему) и должны маркировать печатную копию как конфиденциальную, когда она содержит персональную медицинскую информацию.

Руководство по внедрению

Не вся медицинская информация является конфиденциальной, и не все информационные системы здравоохранения предоставляют пользователям доступ к персональной медицинской информации. Пользователи информационных систем здравоохранения должны знать, когда данные, к которым они имеют доступ, содержат персональную медицинскую информацию.

7.5 Безопасность человеческих ресурсов

7.5.1 До поступления на работу

7.5.1.1 Роли и ответственности

Руководство по внедрению

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, все организации, чей персонал участвует в обработке персональной медицинской информации, **должны** документировать факты такого участия в соответствующих должностных инструкциях. Роли и ответственности по защите, как указано в политике защиты информации организации, должны также оговариваться в соответствующих должностных инструкциях.

Стоит обратить особое внимание на роли и ответственности временного или работающего по краткосрочным контрактам персонала, такого как временные заместители, студенты, врачи-интерны и т. д.

7.5.1.2 Отбор

Контроль

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, все организации, чей персонал, подрядчики или волонтеры обрабатывают (или должны обрабатывать) персональную медицинскую информацию, **должны**, **по меньшей мере**, проверять личность, действующий адрес и место предыдущей работы такого персонала, подрядчиков и волонтеров при подаче заявления о приеме на работу.

Руководство по внедрению

Важно знать, как и где связываться с медицинским персоналом, хотя, так как некоторые медицинские работники постоянно перемещаются, адрес может иметь ограниченную ценность. Поэтому медицинские организации должны рассматривать возможность сбора необходимого количества ссылок и использования других форм проверки, например, профессиональными органами и академическими учреждениями.

По возможности **должны** осуществляться проверки криминального прошлого. См. также 7.8.2.1.

7.5.1.3 Условия приема на работу

Руководство по внедрению

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, все организации, занимающиеся обработкой персональной медицинской информации, **должны** включать в условия приема на работу персонала, который обрабатывает или будет обрабатывать персональную медицинскую информацию, заявление об ответственности персонала за защиту информации.

Условия приема на работу **должны**:

a) Включать в себя ссылки на взыскания, возможные при обнаружении нарушения политики защиты информации,

b) Гарантировать, что условия, связанные с конфиденциальностью персональной медицинской информации, сохранятся при приеме на работу на неограниченный срок.

По отношению к персоналу клиники условия приема на работу **должны** указывать, какие права на доступ к записям об объектах оказания медицинской помощи и к связанным информационным системам здравоохранения в случае заявлений третьих сторон будет иметь этот персонал.

Если между приемом на работу и датой начала работы сотрудника прошло много времени, **следует** серьезно задуматься о повторе процесса отбора или его основных элементов.

7.5.2 В период работы

7.5.2.1 Ответственности руководства

Руководство по внедрению

В дополнение к руководствам, данным в ИСО/МЭК 27002, важно отметить, что стоит сделать акцент на обеспокоенность объектов оказания медицинской помощи, которые не хотят, чтобы к их персональной медицинской информации имели доступ медицинские работники, которые являются их соседями, коллегами или родственниками. Такие опасения часто составляют большой процент жалоб от тех, кто опасается за конфиденциальность своей персональной медицинской информации. Точно так же, сотрудники часто не хотят сталкиваться с обзором информации о друзьях, родственниках или соседях. Эффективное управление информационных систем здравоохранения необходимо для решения этих проблем.

7.5.2.2 Осведомленность, обучение и подготовка в области защиты информации

Контроль

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, все организации, занимающиеся обработкой персональной медицинской информации, **должны** гарантировать предоставление обучения и подготовки в области защиты информации при введении в курс обязанностей, а также то, что регулярные обновления в политике безопасности и методиках организации доводятся до персонала и, где это уместно, до сторонних подрядчиков, исследователей, студентов и волонтеров, занимающихся обработкой персональной медицинской информации.

7.5.2.3 Дисциплинарный процесс

Руководство по внедрению

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, дисциплинарные процессы организации здравоохранения по отношению к нарушениям защиты информации **должны** следовать методикам, отраженным в политике и, следовательно, известным объекту дисциплинарного процесса. В дополнение к соответствию применимым законам, такие процессы должны соответствовать соглашениям, достигнутым между работниками здравоохранения и профессиональными органами здравоохранения.

7.5.3 Окончание срока работы или смена работы

7.5.3.1 Ответственности при окончании срока работы и возврат активов

Руководство по внедрению

В дополнение к руководствам, данным в ИСО/МЭК 27002, важно отметить, что в здравоохранении многие виды сотрудников, например, доктора и медсестры обычно развиваются посредством обучающих программ и других «перемещений», при которых их права доступа могут значительно измениться. Для обеспечения прекращения предыдущих прав, которые в их новой должности не требуются, процесс смены работы должен проходить по тому же алгоритму, что и в случае с людьми, прекращающими работу в организации.

7.5.3.2 Лишение прав на доступ

Контроль

Все организации, занимающиеся обработкой персональной медицинской информации, **должны** как можно скорее лишить пользовательских прав на доступ к этой информации увольняющихся постоянных или временных сотрудников, сторонних подрядчиков или волонтеров по окончанию срока работы, контракта или волонтерской деятельности.

Руководство по внедрению

В дополнение к руководствам, данным в ИСО/МЭК 27002, важно отметить, что в здравоохранении существует множество примеров студентов, временных заместителей, у которых после окончания работы остались права на доступ. Особенно в больших больницах, большое количество временных

работников имеет краткосрочный доступ к персональной медицинской информации. Необходимо тщательно контролировать прекращение прав таких работников на доступ. В то же время, в здравоохранении многие действия выполняются после времени предоставления медицинских услуг (например, окончание расшифровки медицинских записей). Это может значительно усложнить процесс своевременного прекращения прав, и эти действия должны учитываться при проектировании и внедрении процедур прекращения прав на доступ.

Медицинские организации должны серьезно задуматься над немедленным прекращением прав доступа после получения заявления об увольнении по собственному желанию или уведомления об увольнении и т. д., в случае, если существует возможность рисков при сохранении этих прав на доступ.

7.6 Физическая безопасность и безопасность среды

7.6.1 Безопасные зоны

7.6.1.1 Периметр физической безопасности

Контроль

Организации, занимающиеся обработкой персональной медицинской информации, **должны** использовать периметры безопасности для защиты зон, содержащих средства обработки, поддерживающие эти применения в здравоохранении. Эти безопасные зоны должны защищаться соответствующими мерами по контролю доступа для обеспечения того, что только уполномоченные сотрудники имеют доступ.

Руководство по внедрению

В дополнение к руководствам, данным в ИСО/МЭК 27002, важно осознавать, что во многих ситуациях здравоохранения установка периметров безопасности особенно сложна. Многие рабочие области заполняются объектами оказания медицинской помощи. На самом деле, возможно, нет такого промышленного сектора, где люди имеют такой доступ к рабочим областям, кроме как в здравоохранении. В то же время, необходимо поддерживать безопасную среду, сохраняющую физическую безопасность и безопасность объектов оказания медицинской помощи, а также безопасность данных и систем, которые могут быть доступны в этой среде.

В отличие от клиентов в других промышленных секторах, клиенты в здравоохранении часто физически не имеют возможности обеспечить личную защиту и безопасность. Меры по обеспечению физической безопасности для информации **должны** быть согласованы с мерами по обеспечению физической безопасности и защиты для объектов оказания медицинской помощи. Медицинские организации обязаны защищать и то, и то.

7.6.1.2 Средства управления физическим доступом; обеспечение безопасности офисов, помещений и сооружений; защита от внешних угроз и угроз внутри среды; работа в безопасных зонах

Руководство по внедрению

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** делать целесообразные шаги по обеспечению того, что люди имеют доступ к IT-оборудованию (серверам, устройствам хранения, терминалам и экранам) в той степени, в которой этого требуют физические преграды и клинические процессы.

7.6.1.3 Публичный доступ, области доставки и загрузки

Руководство по внедрению

В дополнение к инструкциям, указанным в ИСО/МЭК 27002, важно осознавать, что оказание медицинской помощи включает в себя различные обстоятельства, при которых общество (объекты оказания медицинской помощи и поддерживающие их лица) имеет физический допуск в области, где хранится огромное количество конфиденциальной информации (например, лабораторные испытания, где рабочий процесс может потребовать сбора информации по объектам оказания медицинской помощи в той же области, в которой в настоящее время обрабатываются данные предыдущих объектов; зоны терапии с отделениями оказания неотложной помощи, где близкие или родственники потенциально могут столкнуться со значительным количеством защищаемой вербальной и визуальной информации о других объектах оказания медицинской помощи, рабочие места для ухода за больным с использованием вычислительной техники, расположенные рядом с палатами пациентов). Это все физические области в сфере здравоохранения, которые собирают медицинскую информацию через опросы и которые содержат системы, где данные отображаются на экране, и, следовательно, **должны** быть предметом дополнительного изучения.

Чтобы убедиться в том, что поддерживается конфиденциальность объектов оказания медицинской помощи, здравоохранение часто требует того, чтобы в лифтах, на дверях помещений, в которых могут проводиться опросы, и в других областях были размещены уведомления. Такие уведомления служат напоминанием о воздержании от обсуждения случаев, связанных с пациентами, в зонах общественного пользования.

7.6.2 Безопасность оборудования

7.6.2.1 Размещение и защита оборудования

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** располагать все рабочие места так, чтобы иметь доступ к персональной медицинской информации таким образом, чтобы избежать случайного разглашения или доступа объектов оказания медицинской помощи или посторонних людей.

Медицинские приборы, которые записывают или передают данные, могут также потребовать специальных мер обеспечения безопасности по отношению к среде, в которой они функционируют, а также в связи с электромагнитным излучением, происходящим во время их работы. Медицинские организации, а особенно больницы, **должны** обеспечить то, что руководства по размещению и защите для IT-оборудования минимизируют контакты с такими излучениями.

7.6.2.2 Вспомогательные энергетические системы, безопасность кабельной системы и обслуживание оборудования

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, медицинские организации должны серьезно отнестись к защите сети и других кабельных систем в областях с излучением от медицинских приборов.

7.6.2.3 Безопасность наружного оборудования

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** гарантировать, что любое использование медицинских приборов, которые записывают или передают данные, за ее пределами, разрешено. Это **должно** распространяться на оборудование, используемое удаленными работниками, даже если это использование непрерывно (например, когда оно формирует ключевую особенность работы таких сотрудников, как сотрудники, работающие на машине скорой помощи, терапевты и т. д.)

7.6.2.4 Безопасная утилизация или повторное использование оборудования

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** безопасно переписать или же уничтожить все средства, содержащие прикладное ПО для работы с медицинской информацией или персональную медицинскую информацию, когда эти средства становятся не нужны.

7.6.2.5 Уничтожение собственности

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, предоставляющие или использующее оборудование, данные или программное обеспечение в поддержку программ здравоохранения, **не должны** допускать, чтобы это оборудование, данные или программное обеспечение были удалены с участка или перемещены в его пределах без разрешения организации.

7.7 Управление коммуникациями и деятельностью

7.7.1 Производственная деятельность и эксплуатационная ответственность

7.7.1.1 Документально оформленные технологические инструкции

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.1.2 Контроль изменений

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** посредством официального структурированного процесса контроля изменений, контролировать изменения в средствах, обрабатывающих информацию, и система, обрабатывающих персональную медицинскую информацию обработки информации, для обеспечения надлежащего контроля программ управляющей системы и систем, а также непрерывного ухода за пациентами.

Руководство по внедрению

Важно отметить, что неподходящие, неправильно протестированные или некорректные изменения в обработке персональной медицинской информации могут привести к катастрофическим последствиям для ухода за больным и для его безопасности. Внесение изменений в процесс обработки **должно** явным образом фиксировать и оценивать риски изменений.

7.7.1.3 Распределение обязанностей

Руководство по внедрению

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны**, при наличии возможности, распределять обязанности и области ответственности с целью снижения возможности неправомерного внесения изменений или злоупотребления персональной медицинской информацией.

Организации, занимающиеся обработкой персональной медицинской информации, **должны** гарантировать, что задействованные IT-системы содержат функциональность применимости, которая обеспечит поддержку клинических процессов различными должностными лицами, где это требуется.

7.7.1.4 Разделение средств разработки, испытания и эксплуатации

Контроль

В дополнение к следованию руководствам, данным в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** разделять (физически или виртуально) среды разработки и испытания для информационных систем здравоохранения, обрабатывающих такую информацию из эксплуатационной среды, управляющей этими информационными системами здравоохранения. Правила смены статуса информации с разработки на эксплуатацию **должны** быть определены и задокументированы организацией, управляющей затронутыми сферами применения.

7.7.2 Управление предоставлением услуг третьими сторонами

Руководство по внедрению

Управление предоставлением услуг третьими сторонами значительно упрощается, когда принято официальное соглашение, которое определяет минимальный набор средств управления, которые необходимо внедрить

7.7.3 Планирование и приемка системы

7.7.3.1 Управление производительностью

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.3.2 Приемка системы

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** установить критерии приемлемости для запланированных новых информационных систем, обновлений и новых версий. Они **должны** производить подходящие испытания системы перед ее приемкой.

Руководство по внедрению

Объем и строгость этих испытаний должны быть на уровне, соответствующем обозначенным рискам изменений. См. также 7.7.1.2.

7.7.4 Защита от враждебного программного или мобильного кода

7.7.4.1 Средства управления против враждебного программного кода

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** внедрить соответствующие средства управления предотвращения, обнаружения и реагирования для защиты от вредоносного программного обеспечения, и **должны** внедрять соответствующую подготовку для осведомленности пользователя.

7.7.4.2 Средства управления против мобильного кода

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.5 Резервное копирование информации

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** осуществлять резервное копирование всей персональной медицинской информации и хранить ее в физически защищенной среде для обеспечения ее последующей доступности.

Для защиты конфиденциальности персональной медицинской информации, она должна быть скопирована в зашифрованном виде.

7.7.6 Управление безопасностью сетей

7.7.6.1 Средства управления сетью

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.6.2 Безопасность сетевых служб

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** тщательно продумать, какое влияние может оказать потеря доступности сетевых служб на клиническую практику. См. также 7.11.

7.7.7 Обработка носителей

7.7.7.1 Управление съемными электронными носителями

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** гарантировать, что вся персональная медицинская информация, хранящаяся на съемных носителях,

a) зашифрована, пока ее носитель находится в процессе перемещения, или

b) защищена от кражи, пока ее носитель находится в процессе перемещения.

7.7.7.2 Утилизация носителей

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, вся персональная медицинская информация **должна** быть безопасно переписана, или же носитель **должен** быть уничтожен, когда перестанет быть нужным.

Руководство по внедрению

Несоответствующая утилизация носителей продолжает быть источником серьезных нарушений конфиденциальности пациента. Особенно важно отметить, что эти меры контроля должны быть применены перед ремонтом или утилизацией любого связанного оборудования. Это требование также применимо к медицинским приборам, записывающим или сообщающим данные.

7.7.7.3 Процедура обработки информации

Контроль

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, носители, содержащие персональную медицинскую информацию, **должны** быть физически защищены, или же данные должны быть зашифрованы. Состояние и местоположение носителей, содержащих персональную медицинскую информацию, **должно** контролироваться.

7.7.7.4 Безопасность системной документации

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.8 Обмен информацией

7.7.8.1 Политика и процедуры обмена медицинской информацией и соглашения об обмене медицинской информацией

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, в ИСО 22857 можно найти особые руководства по политике обмена медицинской информацией. Хотя этот международный стандарт явно ссылается на перемещение персональной медицинской информации через границы юрисдикций (где в данном контексте границы обозначают юрисдикции учреждений здравоохранения, а не обязательно границы стран), большая часть его рекомендаций может быть использована, где необходимо, для работы с обменом данными между организациями.

Организации **должны** гарантировать, что безопасность таких обменов информацией является предметом развития политик и надзорного аудита (см. 7.12).

Безопасности обмена информацией может значительно поспособствовать использование соглашений об обмене информацией, которые определяют минимальный набор элементов управления, который необходимо применить.

7.7.8.2 Физические носители в процессе перемещения

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.8.3 Электронный обмен сообщениями

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся передачей персональной медицинской информации посредством электронного обмена сообщениями, **должны** предпринимать меры по обеспечению его конфиденциальности и целостности. Важно отме-

тить, что обеспечение безопасности обмена электронными и мгновенными сообщениями может вовлекать процедуры для медицинского персонала, которые нельзя переложить на объекты оказания медицинской помощи и посторонних людей.

Электронная переписка между медицинскими работниками, которая содержит персональную медицинскую информацию, **должна** быть зашифрована в процессе передачи. Один из подходов к этому включает в себя использование цифровых сертификатов. См. элемент «Библиография» для получения информации о списке стандартов, связанных с использованием цифровых сертификатов в среде здравоохранения.

См. также 7.12.2.2 для обсуждения получения разрешения перед общением за пределами организации.

7.7.8.4 Информационные системы здравоохранения

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.9 Электронное обслуживание медицинской информации

7.7.9.1 Электронная торговля и сетевые транзакции

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, важно отметить осторожность, с которой следует определять, содержат ли данные, используемые при электронной торговле и сетевых транзакциях, персональную медицинскую информацию. Если это так, эта информация должна быть надлежащим образом защищена. Особенно в здравоохранении следует обратить внимание на данные, связанные с выставлением счетов, заявлениями о выплате страхового возмещения за получение медицинских услуг, рядом инвойсов, требованиями и другими данными электронной торговли, из которых можно получить персональную медицинскую информацию.

7.7.9.2 Общедоступная медицинская информация

Контроль

Общедоступная медицинская информация (в отличие от персональной медицинской информации) **должна** архивироваться.

Целостность общедоступной медицинской информации **должна** сохраняться для предотвращения несанкционированного внесения изменений.

Источник (авторство) общедоступной информации **должен** быть указан, а его целостность **должна** быть защищена.

7.7.10 Мониторинг

7.7.10.1 Общие положения

Среди всех требований по защите персональной медицинской информации, одними из самых главных являются те требования, которые связаны с аудитом и ведением протоколов. Они гарантируют подотчетность объектов оказания медицинской помощи, доверяющих свою информацию системам электронных медицинских карт, а также дают пользователям стимул для соответствия политикам надлежащего использования этих систем. Эффективный аудит и ведение протоколов могут помочь обнаружить злоупотребление информационными системами здравоохранения или персональной медицинской информацией. Эти процессы также могут помочь организациям и объектам оказания медицинской помощи получить компенсацию от пользователей, нарушающих права доступа.

7.7.10.2 Ведение контрольных журналов

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** создавать безопасные протоколы аудита каждый раз, когда пользователь осуществляет доступ, создает, обновляет или архивирует персональную медицинскую информацию через систему. Журнал аудита **должен** однозначно распознавать пользователя, однозначно распознавать субъект данных (т. е. объект оказания медицинской помощи), распознавать функцию, выполняемую пользователем (создание записи, доступ к ней, обновление записи и т. д.), и отмечать дату и время, когда функция была выполнена.

Когда обновляется персональная медицинская информация, **должна** быть сохранена запись о предыдущей версии содержания данных и связанный с ней протокол аудита (т. е. информация о том, кто вводил данные и когда).

Системы обмена сообщениями, используемые для передачи сообщений, содержащих персональную медицинскую информацию, **должны** вести журнал обмена сообщениями (такой журнал **должен** содержать время, дату, отправителя и получателя сообщения, но не его содержание).

Организация должна тщательно оценить и установить время сохранения этих журналов аудита с определенными ссылками на клинические профессиональные стандарты и правовые обязательства, с целью сделать возможным проведение расследований при необходимости и представить доказательства злоупотребления персональной медицинской информацией.

7.7.10.3 Использование системы мониторинга

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, средство составления протоколов информационной системы здравоохранения **должно** быть функционирующим каждый раз, когда используется информационная система здравоохранения, подвергаемая аудиту.

Информационные системы здравоохранения, содержащие персональную медицинскую информацию, **должны** быть снабжены средствами для анализа протоколов и журналов аудита, которые:

a) позволяют идентифицировать всех пользователей системы, которые получали доступ к записям об указанном объекте оказания медицинской помощи или вносили в них изменения за определенный период времени;

b) позволяют идентифицировать все объекты оказания медицинской помощи, к чьим данным получали доступ или вносили в них изменения определенные пользователи системы за определенный период времени.

7.7.10.4 Защита информации в журналах

Контроль

Протоколы аудита **должны** быть защищенными от несанкционированного доступа. Доступ к инструментам аудита системы должен быть защищен для предотвращения злоупотребления или несанкционированного доступа.

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, важно отметить, что доказательная целостность протоколов аудита может сыграть важную роль при расследованиях коронеров, расследованиях касательно врачебной ошибки и других судебных и квазисудебных расследованиях. В таких расследованиях действия медицинских работников и временные привязки событий иногда обусловлены изучением изменений и обновлений в персональной медицинской информации пациента.

7.7.10.5 Журналы регистрации администратора и оператора

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.10.6 Регистрация отказов

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.7.10.7 Синхронизация часов

Контроль

Информационные системы здравоохранения, поддерживающие критическую по времени деятельность по совместному уходу, **должны** предоставлять сервисы для синхронизации времени для помощи при прослеживании и воссоздании временных рамок действий, когда это необходимо.

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, важно отметить, что хронометраж событий, зарегистрированных в электронном виде в персональной медицинской информации и в журналах аудита, может сыграть важную роль при таких процессах, как расследования коронеров, расследования врачебной ошибки и другие судебные и квазисудебные расследования, где важно точно определить клиническую последовательность событий.

7.8 Контроль доступа

7.8.1 Требования к контролю доступа в здравоохранении

7.8.1.1 Общие положения

Контроль

Организации, занимающиеся обработкой персональной медицинской информации, **должны** осуществлять контроль доступа к такой информации. Обычно пользователи информационных систем здравоохранения **должны** иметь доступ к персональной медицинской информации только в случаях, когда:

a) существуют отношения в области здравоохранения между пользователем и субъектом данных (объектом оказания медицинской помощи, чья персональная медицинская информация оценивается);

b) пользователь выполняет действие от лица субъекта данных;

c) есть необходимость в особых данных для поддержки этой деятельности.

7.8.1.2 Политика контроля доступа

Контроль

Организации, занимающиеся обработкой персональной медицинской информации, **должны** иметь доступ к управлению политикой контроля доступа к этим данным.

Политика организации касательно контроля доступа **должна** быть установлена на основе предопределенных ролей со связанными органами, которые отвечают требованиям, но ограничены нуждами этой роли.

Политика контроля доступа как компонент основных принципов политики защиты информации, описанной в 7.2.1, **должна** отражать профессиональные, этические, нормативные требования, а также требования, связанные с объектом оказания медицинской помощи, и **должна** учитывать задания, выполняемые медицинскими работниками, а также процесс выполнения задания.

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, важно отметить, что для предотвращения задержки или отказа предоставления медицинских услуг существуют более строгие, чем обычно, требования для четкого понимания политики и процесса с соответствующими разрешениями на отмену действия «обычных» правил контроля доступа в аварийных ситуациях.

Медицинские организации побуждают к рассмотрению возможности внедрения федеративной идентификационной информации и решений для управления доступом с учетом возможности дополнительной поддержки и снижения административных расходов, которое оно даст политике контроля доступа. Кроме того, это будет поддерживать процессы доступа с более высоким уровнем безопасности, такие как доступ, основанный на интеллектуальных карточках, и возможность «однократного предъявления пароля».

7.8.2 Управление доступом пользователей

7.8.2.1 Регистрация пользователей

Контроль

Доступ к информационным системам здравоохранения, которые занимаются обработкой персональной медицинской информации, **должен** подлежать процедуре регистрации пользователей. Процедура регистрации пользователей **должна** гарантировать, что уровень аутентификации, предъявляющий идентификационную информацию пользователя, соответствует уровню(ям) доступа, которые будут доступны для пользователя.

Данные регистрации пользователя **должны** периодически проверяться для того, чтобы гарантировать, что они полные, точные и что доступ все еще требуется.

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, важно понять, что задача по идентификации и регистрации пользователей информационных систем здравоохранения включает в себя все нижеуказанное:

a) точное определение личности пользователя (например, Джоан Смит, родилась 26 марта 1982 года, сейчас проживает по такому адресу);

b) точное определение, после проверки, надежных документов о профессиональной подготовке (например, доктор Джоан Смит, кардиолог) и/или занимаемой должности (например, Сьюзен Джонс, секретарь приемной больницы);

c) назначение однозначного идентификатора пользователя.

Обратите внимание, что объекты оказания медицинской помощи, как правило, не являются пользователями системы, хотя те, кто может иметь доступ ко всем своим персональным данным или к их части (например, через сетевой портал), на самом деле могут считаться пользователями (хотя и имеющими ограниченный доступ). Стоит также обратить внимание, что существуют такие медицинские сферы применения, когда пользователь ищет общий совет или информацию касательно здоровья. И хотя этот запрос на информацию будет внесен в протокол, имя пользователя остается неизвестным. Многие сайты, предоставляющие информацию по беременности, СПИДу, или другим темам касательно здоровья, работают в такой манере. Пользователи сайтов с такой общей медицинской информацией, как правило, не нуждаются в регистрации и поэтому исключены из рассмотрения в последующем обсуждении. См. также 7.5.1.2.

7.8.2.2 Регистрация пользователей

В последующем обсуждении обозначено несколько стратегий контроля доступа, которые могут очень помочь при обеспечении конфиденциальности и целостности персональной медицинской информации:

a) контроль доступа, основанный на ролях, который полагается на документы о профессиональной подготовке и занимаемой должности пользователей, установленные во время регистрации для ограничения доступа только для тех, кто должен выполнять одну или несколько четко определенных ролей;

b) контроль доступа, основанный на рабочей группе, который полагается на принадлежность пользователей к рабочим группам (таким как клинические группы) для определения того, к каким записям они могут иметь доступ;

c) произвольный контроль доступа, который позволяет пользователям информационных систем здравоохранения, связанным с персональной медицинской информацией объекта оказания медицинской помощи на законных основаниях (например, семейный врач), предоставлять доступ другим пользователям, которые ранее установили связь с персональной медицинской информацией объекта оказания медицинской помощи (например, специалист).

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, информационные системы здравоохранения, содержащие персональную медицинскую информацию, **должны** поддерживать контроль доступа, основанный на ролях, способный присвоить каждому пользователю одну или несколько ролей, а каждой роли — одну или несколько функций.

Пользователь информационной системы здравоохранения, содержащей персональную медицинскую информацию, **должен** получать доступ к ее сервисам по одной роли (то есть, пользователи, которые были зарегистрированы с несколькими ролями, **должны** указывать одну из ролей во время каждого сеанса доступа к информационной системе здравоохранения).

Информационные системы здравоохранения должны объединять пользователей (включая медицинских работников, вспомогательного персонала и других) с записями об объектах оказания медицинской помощи, что позволяет в дальнейшем иметь доступ на основе этого объединения.

Дополнительные руководства по управлению полномочиями в здравоохранении можно найти в ИСО/ТС 22600-1 и ИСО/ТС 22600-2.

7.8.2.3 Управление паролями пользователей

Дополнительных руководств по менеджменту защиты информации в здравоохранении нет, однако стоит отметить, что ограниченность во времени, обнаруженная в ситуациях оказания медицинской помощи, может помешать эффективно использовать пароли. Многие медицинские организации предпочли внедрить альтернативные технологии аутентификации для решения данной проблемы

7.8.2.4 Проверка прав доступа пользователей

Помимо инструкций, указанных в ИСО/МЭК 27002, необходимо обратить особое внимание на пользователей, от которых разумно ожидать предоставления неотложной помощи, так как им может потребоваться доступ к персональной медицинской информации в экстренных ситуациях, когда объект оказания медицинской помощи не может сообщить о своем согласии.

7.8.3 Обязанности пользователя

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, при определении обязанностей пользователя **должны** уважать права и этические обязанности медицинских работников, как указано в законе и как принято членами профессиональных медицинских организаций.

7.8.4 Контроль доступа к сети и контроль доступа к операционной системе

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.8.5 Контроль доступа к приложениям и информации

7.8.5.1 Ограничение доступа к информации

Контроль

Информационные системы здравоохранения, занимающиеся обработкой персональной медицинской информации, **должны** аутентифицировать пользователей и **должны** делать это посредством аутентификации с использованием, по крайней мере, двух факторов.

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, необходимо обратить особое внимание на технические мероприятия, по которым объект оказания медицинской помощи точно аутентифицируется при доступе ко всей личной информации или к ее части (в тех системах информации, где это допустимо). Такое же внимание стоит уделить простоте использования таких мероприятий, особенно для объ-

ектов оказания медицинской помощи с физическими недостатками, а также предоставлению доступа заменяющими лицами, ответственными за принятие решений.

7.8.5.2 Изоляция зависимой системы

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.8.6 Мобильные компьютерные среды и дистанционный режим работы

7.8.6.1 Мобильные компьютерные среды и связи

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны**:

a) иметь особый доступ к рискам, имеющимся в мобильных компьютерных средах здравоохранения;

b) подготовить политику по мерам предосторожности при использовании мобильных устройств, включая беспроводные устройства;

c) требовать от мобильных пользователей следовать этой политике.

Как отмечено в ИСО/МЭК 27002, беспроводные соединения мобильных сетей, хоть и похожи на соединения проводных сетей, имеют несколько существенных отличий, с точки зрения защиты информации. Некоторые беспроводные протоколы шифрования, такие как эквивалент конфиденциальности проводных сетей (WEP), до сих пор применяются, несмотря на известные уязвимости, которые показывают их неэффективность. Кроме того, информация, хранящаяся на мобильных устройствах, не всегда может быть скопирована (резервное копирование) (например, из-за ограниченной пропускной способности сети или из-за того, что устройства не всегда подключены во время запланированного резервного копирования).

7.8.6.2 Дистанционный режим работы

Руководство по внедрению

Помимо соблюдения инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны**:

a) подготовить политику по мерам предосторожности при дистанционном режиме работы;

b) убедиться, что пользователи, работающие в дистанционном режиме, следуют этой политике.

Некоторые национальные юрисдикции (например, Германия) уже установили ограничения для медицинских работников на дистанционный режим работы.

Важно обратить внимание на то, что в здравоохранении дистанционный режим работы может пересекать юрисдикционные границы и даже может происходить на борту самолета или корабля, находящегося в данный момент вне каких-либо национальных юрисдикций. Терапевты уже давно на постоянной основе обмениваются снимками и т. д. через электронную почту, пересекая юрисдикционные границы, для получения мнения специалиста. Международные группы, участвующие в помощи при стихийных бедствиях, смогут в будущем полагаться на информационные системы здравоохранения в юрисдикциях, отличающихся от их юрисдикции. Нужно учитывать правовые и этические соображения по данному вопросу при разработке и внедрении информационных систем здравоохранения (особенно национальных систем), которые могут использоваться подобным образом. См. также 7.7.7.1 и 7.7.8.3.

7.9 Заказ, проектирование и обслуживание информационных систем

7.9.1 **Требования безопасности для информационных систем**

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.2 Правильная обработка в приложениях

7.9.2.1 Однозначное распознавание объектов оказания медицинской помощи

Контроль

Организации, занимающиеся обработкой персональной медицинской информации, **должны**:

a) гарантировать то, что каждый объект оказания медицинской помощи будет однозначно распознан;

b) быть в состоянии объединить два или несколько протоколов, если предусмотрено произвольное создание нескольких протоколов для того же объекта оказания медицинской помощи или во время возникновения неотложного состояния.

Руководство по внедрению

Оказание неотложной помощи и другие ситуации, при которых могло не существовать возможности надлежащим образом распознать объекты оказания медицинской помощи, неизбежно приведут к созданию нескольких карт по одному и тому же пациенту. В пределах каждой информационной системы

здравоохранения должна существовать возможность объединения нескольких карт пациентов в одну. Такое объединение требует внимательности, и поэтому потребуется не только персонал, обученный для такого объединения, но, возможно, и технические средства для упрощения объединения информации из исходных карт в объединенную.

Организации, занимающиеся обработкой персональной медицинской информации, **должны** гарантировать, что данные, исходя из которых можно установить личность, сохранятся только там, где это необходимо, и что методики удаления, анонимизации и псевдонимизации используются надлежащим образом в максимально возможной мере для сведения к минимуму рисков непреднамеренного разглашения персональной информации.

7.9.2.2 Проверка входных данных

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.2.3 Контроль внутренней обработки

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.2.4 Целостность сообщения

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.2.5 Проверка выходных данных

Контроль

Информационные системы здравоохранения, занимающиеся обработкой персональной медицинской информации, **должны** предоставлять идентифицирующие личность сведения для помощи медицинским работникам в подтверждении того, что найденные электронные медицинские карты относятся к объекту оказания медицинской помощи, проходящему лечение.

Руководство по внедрению

В дополнение к руководствам, указанным в ИСО/МЭК 27002, необходимо учитывать некоторые дополнительные важные факторы. Прежде чем полагаться на персональную медицинскую информацию, предоставленную информационной системой здравоохранения, медицинским работникам должно быть предоставлено достаточно информации для того, чтобы убедиться в том, что объект оказания медицинской помощи соответствует полученной информации. Соответствие объекта оказания медицинской помощи, проходящего лечение, существующей записи может стать нетривиальной задачей. Некоторые системы повышают уровень безопасности путем добавления фотографии в медицинскую карту каждого объекта оказания медицинской помощи. Такие улучшения могут сами по себе создавать проблемы с конфиденциальностью, так как они делают возможным случайное запоминание характеристик, таких как расовая принадлежность, которые не включены в поля данных. Требования по идентификации объектов оказания медицинской помощи и наличию данных, используемых для ее поддержки, также могут варьироваться от юрисдикции к юрисдикции. Большое внимание необходимо проявлять при проектировании информационных систем здравоохранения, для того чтобы работники здравоохранения могли доверять системе в обеспечении информацией, необходимой для подтверждения того, что каждая найденная карта соответствует объекту оказания медицинской помощи, проходящему лечение.

Информационные системы здравоохранения должны делать возможной проверку того, что бумажные распечатки являются полными (например, посредством записи «страница 3 из 5»).

7.9.3 Контроль доступа с использованием криптографии

7.9.3.1 Политика использования контроля доступа с использованием криптографии и управление ключами

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, в ИСО 17090-3 можно найти руководства по размещению и использованию цифровых сертификатов здравоохранения и по управлению ключами.

7.9.3.2 Управление ключами

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.4 Безопасность системных файлов

7.9.4.1 Контроль оперативного программного обеспечения

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.4.2 Защита данных испытания системы

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **не должны** использовать реальную персональную медицинскую информацию в качестве данных испытания.

7.9.4.3 Контроль доступа к исходному коду программы

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.9.5 Безопасность в процессах разработки и поддержки и контроль технической уязвимости

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.10 Управление инцидентами защиты информации

7.10.1 События и слабости в системе безопасности отчетной информации

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** установить ответственности и процедуры касательно инцидентов в системе безопасности, для того чтобы:

a) обеспечить быстрый, эффективный и последовательный отклик на инциденты в системе безопасности;

b) гарантировать то, что существует действенный иерархический порядок для таких инцидентов, так чтобы можно было использовать управление в кризисных ситуациях и планы по управлению непрерывности бизнеса при подходящих условиях и в нужное время;

c) собирать и сохранять данные по инциденту, такие как протоколы и журналы аудита, а также другие свидетельства.

Инциденты в системе безопасности включают коррупцию или непреднамеренное разглашение персональной медицинской информации, или потерю доступности информационных систем здравоохранения, где такая потеря отрицательно сказывается на уходе за больным или способствует неблагоприятным клиническим событиям.

Организации **должны** уведомлять объект оказания медицинской помощи каждый раз, когда персональная медицинская информация была непреднамеренно разглашена.

Организации **должны** уведомлять объект оказания медицинской помощи каждый раз, когда отсутствие доступности информационных систем здравоохранения, возможно, неблагоприятно сказалось на их лечении.

В медицинских организациях существует тенденция искусственно отделять инциденты защиты информации от других типов инцидентов как в обращении, так и в отчетности. Учитывая тот факт, что проникновение в систему могло привести к краже IT-оборудования (что приводит к нарушению конфиденциальности) или что пожар мог быть устроен преднамеренно, чтобы скрыть факт злоупотребления IT-оборудованием, или что определенное злоупотребление или неправильное использование системы могло иметь клинические последствия, оценка защиты информации **должна** быть проведена в отношении всех подобных инцидентов или инцидента-образца для дальнейшей оценки эффективности установленных элементов управления и оценки рисков, которые привели к их внедрению.

7.10.2 Управление инцидентами и улучшениями

7.10.2.1 Обязанности и процедуры

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.10.2.2 Извлечение уроков из инцидентов

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.10.2.3 Сбор свидетельств

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, могут подумать о полезности сбора и свидетельств с целью выявления врачебной ошибки, а также им может потребоваться учесть между-юрисдикционные требования в случае, когда информационные системы здравоохранения доступны за пределами границ юрисдикции.

7.11 Аспекты защиты информации в управлении непрерывностью бизнеса

Руководство по внедрению

Помимо инструкций, указанных в ИСО/МЭК 27002, следующие соображения важны в условиях среды здравоохранения. Управление непрерывностью бизнеса, которое включает в себя аварийное восстановление, все чаще признается в качестве требования для медицинских организаций, и приоритет, которое оно имеет, продолжает расти. Отражая строгие требования к доступности в здравоохранении, основные усилия должны быть направлены на отказоустойчивость и исправление избыточного

кода, и не только для самой технологии, но и для обучения медицинских кадров смежным специальностям.

Планирование непрерывности бизнеса в здравоохранении является особенно сложной задачей для специалистов защиты информации, так как любые планы должны быть соответствующим образом объединены с планами по организации исправления сбоев питания, реализации инфекционного контроля и работе с другими чрезвычайными ситуациями клинической практики. Действительно, запуск любого из них, вероятно, приведет непосредственно к запуску плана управления непрерывностью бизнеса, если только обеспечить дополнительную поддержку к той, которая имеется обычно. Тем не менее, недавние инциденты, такие как вспышки атипичной пневмонии, показали, что серьезные инциденты могут привести к нехватке персонала, которая затем может серьезно ограничить возможность успешной реализации планов управления непрерывностью бизнеса.

Медицинские организации здравоохранения должны гарантировать то, что их планирование непрерывности бизнеса управления включает в себя планирование управления в кризисных ситуациях здравоохранения.

Медицинские организации также должны гарантировать то, что планы, которые они разрабатывают, регулярно тестируются на «программной» основе. Испытания, включенные в эту программу, должны выстраиваться друг на друге, от стационарных испытаний к модульным испытаниям, от них — к обобщению вариантов вероятного времени восстановления, а затем, наконец, к генеральной репетиции. Таким образом, подобная программа имеет низкий уровень риска и обеспечивает действительное улучшение общего уровня осведомленности среди ее пользователей.

7.12 Соответствие

7.12.1 Общие положения

Руководство по внедрению

Помимо соблюдения инструкций, указанных ИСО/МЭК 27002, медицинские организации **должны** запустить программу проверки соответствия, которая учитывала бы весь жизненный цикл действий, т.е. не только процессы, в которых имеются проблемы, но и те, что делают обзор результатов и принимают решения об обновлениях в СМИБ.

Программы аудита медицинских организаций должны быть формально выстроены так, чтобы охватить все элементы настоящего международного стандарта, все области риска и все внедренные элементы управления, в пределах 12—18-месячного цикла.

В строго управляемой и проверяемой среде многих медицинских организаций ISMF должен поставить перед собой цель создать основу для аудита градуированного соответствия, нижним слоем которой является внутренняя проверка, осуществляемая квалифицированными рабочими и руководителями. После этого аудит СМИБ от лица ISMF, внутренний аудит, оценка работы элементов управления и внешний аудит должны быть определены таким образом, чтобы каждый слой черпал уверенность из всех нижележащих.

7.12.2 Соответствие законодательным требованиям

7.12.2.1 Определение применимого законодательства, прав на интеллектуальную собственность и защиту организационной документации

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.12.2.2 Защита данных и конфиденциальности персональной информации

Контроль

Помимо инструкций, указанных в ИСО/МЭК 27002, организации, занимающиеся обработкой персональной медицинской информации, **должны** контролировать согласие объектов оказания медицинской помощи на предоставление информации.

По возможности, согласие объектов оказания медицинской помощи на предоставление информации должно быть получено до того, как персональная медицинская информация будет передана по электронной почте, по факсу или по телефону, или разглашена иным способом сторонам, не входящим в медицинскую организацию.

Руководство по внедрению

Примером законодательства или предписания, требующего согласия объектов оказания медицинской помощи на предоставление информации, является *Рекомендация Совета Европы R (97)5 «О защите медицинской информации», Совет Европы, Страсбург, 12 февраля 1997 (Council of Europe Recommendation, R (97)5 On the Protection of Medical Data, Council of Europe, Strasbourg, 12 February 1997):*

Перед осуществлением генетического анализа субъект данных должен быть проинформирован о целях анализа и возможности неожиданных результатов.

Он должен быть проинформирован о неожиданных результатах, если:

a) это не запрещено национальным законом;

b) человек сам запросил эту информацию;

c) маловероятно, что информация нанесет серьезный вред:

i. его/ее здоровью,

ii. его/ее единокровным или единоутробным родственникам, члену его/ее семьи, или человеку, который имеет с ним/ней прямую генетическую связь;

d) эта информация имеет непосредственное значение для его/ее лечения или предотвращения болезни.

Примером профессиональных рекомендаций, требующих согласия объектов оказания медицинской помощи, является Хельсинкская декларация по медицинским исследованиям на людях.

7.12.2.3 Предотвращение злоупотребления средств обработки информации и регулирование контроля доступа с использованием криптографии

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

7.12.3 Соответствие политике и стандартам безопасности и техническое соответствие

Руководство по внедрению

Особое внимание уделяется соблюдению соответствия с целью технической возможности взаимодействия, так как крупные информационные системы здравоохранения, как правило, состоят из большого количества взаимодействующих систем.

7.12.4 Рекомендации по аудиту информационных систем в среде здравоохранения

Нет дополнительных руководств по менеджменту защиты информации в здравоохранении.

Приложение А
(справочное)

Угрозы защиты медицинской информации

Угрозы конфиденциальности, целостности и доступности активов медицинской информации включают в себя все нижеследующее.

1) **Имитация другого лица сотрудником организации** (включая имитацию другого лица медицинскими работниками и вспомогательным персоналом)

Имитация другого лица сотрудниками организации заключается в использовании системы теми, кто извлекает выгоду из учетных записей, не принадлежащих им. Она представляет собой сбой в надежной аутентификации пользователей. Многие случаи имитации другого лица сотрудниками организации были совершены просто потому, что это облегчает людям работу. Например, когда один медицинский работник может заменить другого на рабочей станции и продолжает работать по уже открытой карте объекта оказания медицинской помощи, существует сильное искушение пропустить процедуру выхода первого пользователя из системы и входа второго пользователя. Тем не менее, имитация другого лица сотрудниками организации также является источником серьезных нарушений конфиденциальности. В самом деле, большая часть нарушений конфиденциальности совершается сотрудниками организации. Имитация другого лица сотрудниками организации также может осуществляться с целью сокрытия случаев причинения вреда.

2) **Имитация другого лица поставщиками услуг** (включая сотрудников по обслуживанию, работающих на договорной основе, таких как разработчики системного программного обеспечения, сотрудников по ремонту оборудования и других лиц, которые могут иметь *формальное* законное основание на доступ к системе и данным)

Имитация другого лица поставщиками услуг заключается в использовании сотрудниками, работающими на договорной основе, привилегированного доступа к системам (например, во время испытания на месте и ремонта неисправного оборудования) для получения несанкционированного доступа к данным. Само по себе это является нарушением, или неспособностью должным образом обеспечить безопасное использование внешних источников. Хотя и реже, чем в случае с имитацией другого лица членами организации, имитация другого лица поставщиками услуг также может быть источником серьезных нарушений конфиденциальности персональной медицинской информации.

3) **Имитация другого лица посторонними лицами** (включая хакеров)

Имитация другого лица посторонними лицами происходит, когда третьи лица получают доступ к данным или ресурсам системы, выдав себя за уполномоченного пользователя или обманным путем став уполномоченным пользователем (например, через так называемый «социальный инжиниринг»). В дополнение к хакерам, имитацию другого лица посторонними лицами также совершают журналисты, частные детективы и «хактивисты» (хакеры, которые работают от имени или в поддержку политических группировок). Имитация другого лица посторонними лицами представляет собой отказ одной или нескольких нижеуказанных мер безопасности:

i) идентификация пользователя;

ii) аутентификация пользователя;

iii) аутентификация источника;

iv) контроль доступа и управление полномочиями.

4) Несанкционированное использование приложения для доступа к медицинской информации

Получить несанкционированный доступ к приложению для доступа к медицинской информации может быть на удивление легко (например, объектом оказания медицинской помощи, проникнувшим в незанятую рабочую станцию в рабочем кабинете терапевта и включившим монитор). Уполномоченные пользователи также могут выполнять несанкционированные действия, такие как изменение данных со злым умыслом. В Великобритании доктор Гарольд Шипман пытался скрыть скандальное убийство десятков своих пациентов путем изменения записей в своей компьютерной системе.

Критическая важность правильной идентификации объектов оказания медицинской помощи и правильное установление соответствия с их медицинской картой приводит медицинские организации к сбору подробных идентификационных данных по пациентам, проходящим лечение. Эти идентификационные данные имеют большую потенциальную ценность для того, кто может использовать ее для хищения персональных данных, и поэтому они должны быть строго защищены.

В общем, несанкционированное использование приложений медицинской информации представляет собой сбой в одной или нескольких нижеуказанных мерах безопасности:

i) контроль доступа рабочей группы (например, позволяя пользователю получать доступ к картам объектов оказания медицинской помощи, с которыми он не имеет никаких законных отношений);

ii) подотчетность и контроль аудита (например, позволяя неподходящим действиям пользователя оставаться незамеченными);

iii) безопасность персонала (например, предоставляя сотрудникам недостаточный уровень обучения или не объясняя, что их доступ к записям подлежит аудитам и проверкам).

5) Попадание вредоносного или разрушительного программного обеспечения (включая вирусы, червей и другое вредоносное программное обеспечение)

Большая часть инцидентов защиты IT представлена компьютерными вирусами. Попадание вредоносного или разрушительного программного обеспечения представляет собой сбой в антивирусной защите или в управлении изменениями программного обеспечения. В то время как обычно они находятся в пределах должностных полномочий сетевых операторов, распространение червей электронной почты и вирусов, а также использование хакерами слабых мест в программном обеспечении сервера объединились, чтобы в значительной степени осложнить меры, которые необходимо принять для предотвращения попадания вредоносного или разрушительного программного обеспечения.

6) Злоупотребление системными ресурсами

Эта угроза представляет собой пользователей, использующих информационные системы здравоохранения и сервисы для собственной работы; пользователей, скачивающих с Интернета не связанную с работой информацию на компьютеры, предназначенные исключительно для поддержки информационных систем здравоохранения; пользователей, создающих базы данных или другие приложения для вопросов, не связанных с работой, или пользователей, ухудшающих доступность информационных систем здравоохранения, например, используя пропускную способность сети для загрузки потокового видео или аудио для личного пользования. Такое злоупотребление представляет собой сбой в исполнении соглашений о надлежащем использовании или обучении пользователей важности поддержания целостности и доступности источников медицинской информации.

7) Несанкционированный доступ к передаче данных

Несанкционированный доступ к передаче данных по электронным коммуникациям происходит, когда человек (хакер, например) вмешивается в нормальное перемещение данных по сети. Наиболее распространенным результатом является атака типа отказ в обслуживании (при которой серверы или сетевые ресурсы эффективно выводятся из строя), но возможны и другие формы несанкционированного доступа к передаче данных (например, атака повторного воспроизведения, при которой реальное, но устаревшее сообщение передается повторно таким образом, что создается впечатление, что оно новое). Несанкционированный доступ к передаче данных представляет собой сбой в обнаружении вторжений и/или управления доступа к сети, и/или анализа рисков (в частности, анализа уязвимости), и/или архитектуры системы (которая должна быть разработана с защитой от атаки типа отказ в обслуживании).

8) Перехват информации в каналах связи

Если не шифруется во время передачи конфиденциальность информации, содержащейся в сообщении, может быть аннулирована посредством перехвата информации в каналах связи. Это проще, чем кажется, так как любой пользователь локальной сети может установить на своей рабочей станции так называемый «анализатор пакетов» и контролировать большую часть сетевого трафика в их локальной сети, в том числе читать электронную почту во время ее передачи. Хакерские инструменты помогают автоматизировать и упростить большую часть этого процесса. Перехват информации в каналах связи представляет собой сбой в защищенной связи.

9) Отказ от авторства

Эта угроза представляет собой пользователей, отрицающих, что они послали сообщение (отказ от авторства) и пользователей, отрицающих, что они получили сообщение (отказ от получения). Однозначное установление того, имел ли место факт перехода персональной медицинской информации от одного врача или медицинского учреждения к другому, может быть основным признаком расследований врачебной ошибки. Отказ от авторства может представлять собой сбой в применении элементов управления, таких как цифровые подписи на электронных рецептах (пример отказа от авторства) или элементов управления, таких как уведомления о прочтении сообщений электронной почты (пример отказа от получения).

10) Сбой подключения (включая сбои в сетях медицинской информации)

Все сети подвержены периодическим отключениям. Качество обслуживания является одним из основных факторов в предоставления сетевых услуг в сфере здравоохранения. Сбой подключения может быть также результатом неправильного направления сетевых услуг (например, злонамеренного изменения таблиц маршрутизации, которое приводит к переадресации сетевого трафика). Отказы подключения могут облегчить раскрытие конфиденциальной информации, заставляя пользователей отправлять сообщения с помощью менее безопасных механизмов, например по факсу или через Интернет.

11) Встраивание вредоносного кода

Эта угроза включает в себя вирусы электронной почты и враждебный мобильный код. Хотя это и не является специфичной угрозой для информационных систем здравоохранения, более широкое использование беспроводных и мобильных технологий среди медицинских работников увеличивает возможность угрозы нанесения повреждений. Встраивание вредоносного кода представляет собой сбой в эффективном применении программного управления антивирусом или средств управления для предотвращения вторжений.

12) Случайная неправильная маршрутизация

Эта угроза включает в себя возможность того, что информация доставлена по неправильному адресу, в случае передачи по сети. Случайная неправильная маршрутизация может представлять собой сбой в образовании пользователя или неспособность поддерживать целостность каталогов врачей или медицинских учреждений (или и то, и другое).

13) Техническая неисправность ведущего компьютера, накопителей или инфраструктуры сети

Эти угрозы включают в себя отказ оборудования, сбои сети или сбои в работе накопителей информации. Такие отказы обычно представляют собой сбой одного или нескольких элементов управления операциями, перечисленными в разделе 10 ИСО/МЭК 27002:2005. Хотя это и не является специфичным для информационных систем здравоохранения, потеря доступности таких систем может впоследствии представлять угрозу жизни пациентов.

14) Сбой в системе жизнеобеспечения (включая перебои в подаче электроэнергии и перебои с обслуживанием, связанные со стихийными бедствиями или техногенными катастрофами)

Информационные системы здравоохранения могут иметь решающее значение во время стихийных бедствий и других событий, которые могут угрожать жизни большого числа людей. Эти же бедствия могут нанести ущерб системам жизнеобеспечения, необходимым для проведения операций. Надлежащая оценка угроз и рисков медицинской информации о состоянии здоровья будет включать в себя оценку того, насколько важны такие системы в случае стихийных бедствий, и насколько устойчивой будет их работа при таких сценариях бедствия.

15) Сбой системы или сетевого программного обеспечения

Атаки типа отказ в обслуживании значительно облегчаются слабостью или неверной настройкой операционной системы или программного обеспечения сетевой операционной системы. Сбой системы или сетевого программного обеспечения представляет собой сбой в проверке целостности программного обеспечения, испытаний системы или элементы управления сопровождения программного обеспечения.

16) Сбой прикладного программного обеспечения (например, приложения для доступа к медицинской информации)

Сбои прикладного программного обеспечения могут быть использованы в атаках типа отказ в обслуживании, а также могут быть использованы для того, чтобы скомпрометировать конфиденциальность защищенных данных. Сбой прикладного программного обеспечения представляет собой сбой в испытании программного обеспечения, контроле над внесением изменений в программное обеспечение или проверке целостности программного обеспечения.

17) Ошибка оператора

Счета об ошибках оператора образуют небольшую, но ощутимую часть непреднамеренных разглашений конфиденциальной информации и значительную часть непреднамеренных раскрытий данных. Ошибка оператора представляет собой сбой в одном или нескольких следующих действиях:

i) управление работой.

ii) безопасность персонала (включая эффективную подготовку).

iii) аварийное восстановление (включая резервное копирование и восстановление данных).

18) Ошибка технического обслуживания

Ошибки технического обслуживания это ошибки, допущенные теми, кто отвечает за техническое обслуживание систем аппаратного и программного обеспечения. Ошибки технического обслуживания могут быть совершены сотрудниками, а также сторонними сотрудниками, работающими на договорной основе и выполняющими обязанности по техническому обслуживанию. Такие ошибки могут, в свою очередь, поставить под угрозу конфиденциальность защищенных данных. Неправильная настройка программного обеспечения во время установки является частой причиной возникновения уязвимостей, позже используемых хакерами. Ошибки обслуживания представляют собой сбой в средствах управления аппаратного обеспечения технического обслуживания, в средствах управления программного обеспечения технического обслуживания, средствах контроля изменений в программном обеспечении или комбинацию вышеперечисленных сбоев.

19) Ошибка пользователя

Ошибка пользователями может, например, привести к тому, что конфиденциальная информация будет отправлена к неправильному получателю. Ошибка пользователя иногда может представлять собой сбой в:

i) элементах управления пользователя.

ii) безопасности персонала (включая подготовку).

20) Нехватка персонала

Угроза нехватки персонала включает в себя возможность отсутствия ключевого персонала и сложность его замены. Уязвимость к этой угрозе зависит от степени, в которой нехватка персонала будет влиять на бизнес-процессы. В здравоохранении эпидемия, которая значительно увеличивает спрос на своевременный доступ к медицинской информации, может также создать нехватку персонала, что ставит под угрозу наличие таких систем. Сбой подобного рода представляет собой сбой в управления непрерывностью бизнеса (см. раздел 14 ИСО/МЭК 27002:2005).

21) Кража сотрудниками организации (включая кражу оборудования или данных)

Сотрудники организации, как правило, имеют более широкий доступ к конфиденциальной информации, чем посторонние, и поэтому находятся в выгодном положении для кражи информации для того, чтобы продать ее или раскрыть ее другим лицам. Хотя угроза кражи персональной медицинской информации сотрудниками организации является сравнительно редкой, она увеличивается вместе со славой или скандальной известностью субъекта данных (например, знаменитости или главы государства) и уменьшается с потенциальной угрозой последующего наказания (например, потери врачом его лицензии на врачебную практику). Кража сотрудниками организации представляет собой отказ одного из многих возможных элементов управления, в том числе управления выхода печатной копии, документов или информации, физической безопасности или физической защиты оборудования.

22) Кража посторонними лицами (включая кражу оборудования или данных)

Кража данных и оборудования посторонними лицами является серьезной проблемой в некоторых больницах. Кража может привести к нарушению конфиденциальности, потому что конфиденциальные данные находятся на сервере или украденном ноутбуке, или потому, что сами данные являются целью кражи. Кража посторонними лицами может представлять собой отказ одного из многих элементов управления, в том числе элементов управления мобильных компьютерных сред, безопасного перемещения в среде, обработки последствий происшествия, проверок соответствия или физической защиты от кражи.

23) Умышленное причинение вреда сотрудниками организации

Умышленное причинение вреда сотрудниками организации включает акты вандализма и другие случаи нанесения физического вреда IT-системам или их поддерживающей среде людьми, которым было предоставлено право доступа. Пользователями информационных систем здравоохранения, как правило, являются преданные делу работники здравоохранения, и умышленное причинение встречается редко. Умышленное причинение вреда сотрудниками организации представляет собой отказ безопасности людских ресурсов (см. раздел 8 ИСО/МЭК 27002:2005).

24) Умышленное причинение вреда посторонними лицами

Угроза умышленного причинения вреда посторонними лицами включает в себя акты вандализма и другие случаи нанесения физического вреда IT-системам или их поддерживающей среде людьми, которые не имеют доступа к таким системам. В то время как в большинстве отраслей промышленности акты такого рода представляют собой неспособность эффективно применять физические средства безопасности, доступ объектов оказания медицинской помощи и их близких и родственников в операционные зоны больниц, клиник и других медицинских организаций значительно усложняет устранение таких угроз по сравнению с большинством других операционных зон. Элементы управления безопасности в разделе 9 ИСО/МЭК 27002:2005 должны быть тщательно отобраны и применены для минимизации подобных угроз.

25) Терроризм

Угроза терроризма включает в себя действия экстремистских групп, желающих повредить или нарушить работу медицинских организаций или навредить медицинским работникам, или сорвать работу информационных систем здравоохранения. Хотя таких масштабных атак еще не происходило, планировщики должны рассмотреть вероятность угроз терроризма, особенно когда спроектированы крупномасштабные информационные системы здравоохранения, так как атаки на такие системы могут повысить эффективность биотерроризма и других атак, которые вызывают кризис, связанный с состоянием здоровья.

Приложение В
(справочное)

Задачи и сопутствующие документы СМИБ

В.1 Задачи и сопутствующие документы для установки СМИБ (планирование)

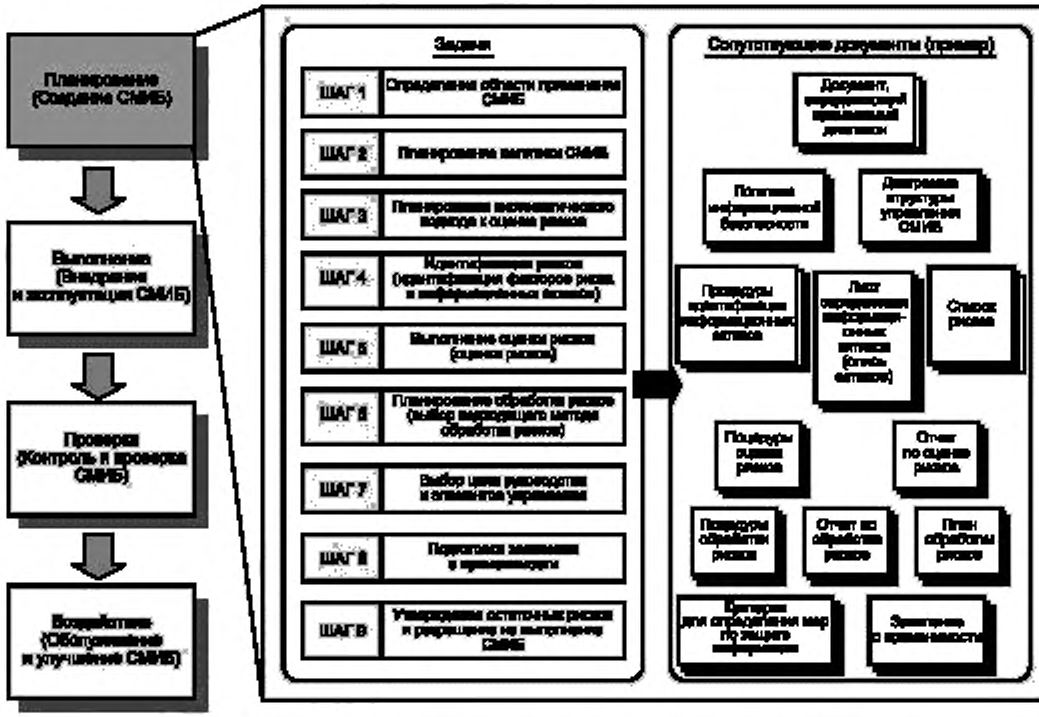

Рисунок В.1 — Задачи и сопутствующие документы для установки СМИБ

В.2 Задачи и сопутствующие документы для внедрения и эксплуатации СМИБ (действие)

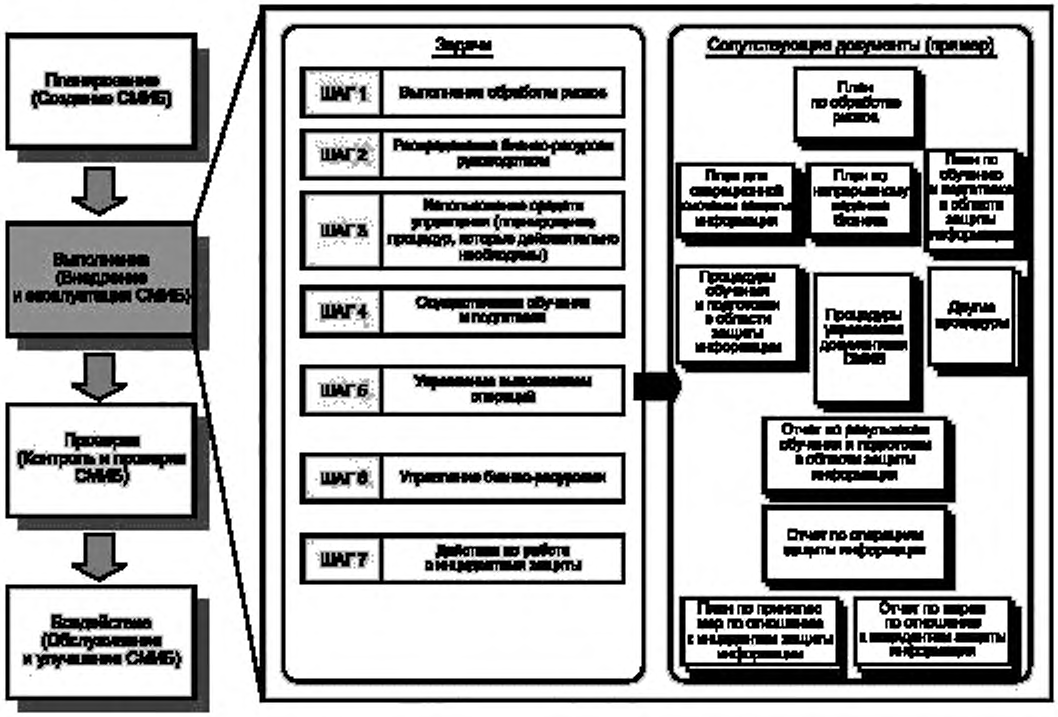

Рисунок В.2 — Задачи и сопутствующие документы для внедрения и эксплуатации СМИБ

В.3 Задачи и сопутствующие документы для мониторинга и проверки СМИБ (проверка)

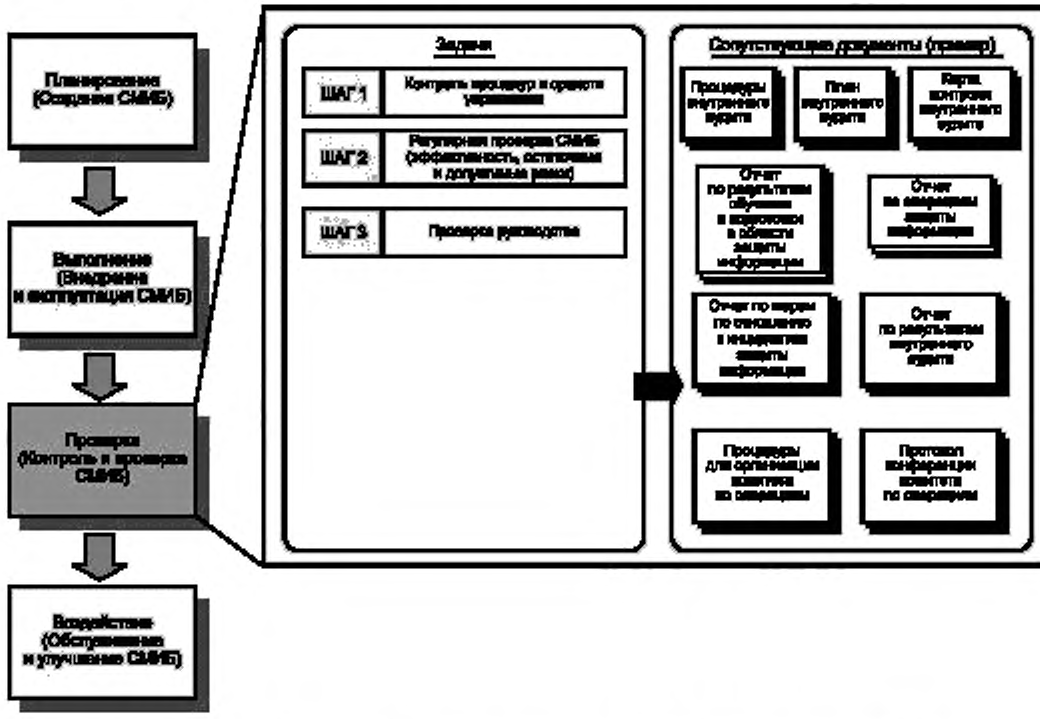

Рисунок В.3 — Задачи и сопутствующие документы для мониторинга и проверки СМИБ

В.4 Задачи и сопутствующие документы для обслуживания и улучшения СМИБ (улучшение)

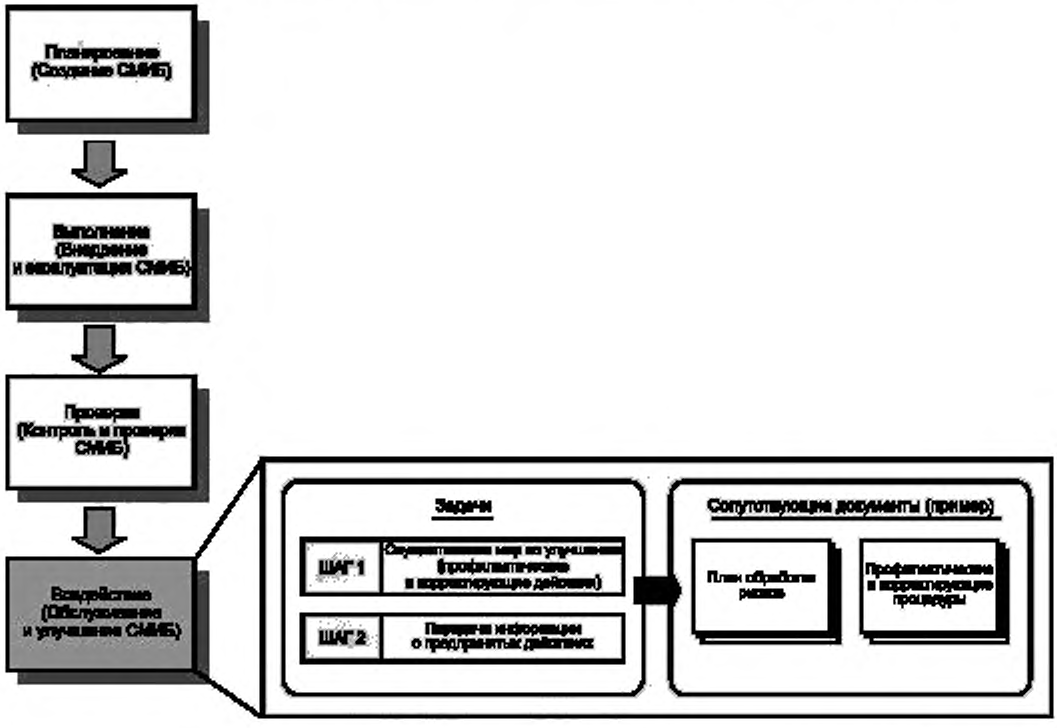

Рисунок В.4 — Задачи и сопутствующие документы для обслуживания и улучшения СМИБ

Приложение С
(справочное)

Потенциальная польза и требуемые свойства инструментов поддержки

С.1 Потенциальная польза инструментов поддержки

Хотя инструменты для баз данных никоим образом не являются обязательными, свидетельства неоднократно показали, что они приносят значительную пользу.

Существует широкий спектр доступных инструментов, от простых и дешевых до сложных и более дорогих. При рассмотрении вопроса о внедрении инструментов медицинские организации должны искать свидетельства успешного использования инструмента другими организациями и должны тщательно обдумать связанные с этим расходы на подготовку персонала и техническое обслуживание, хотя это вряд ли будет основным критерием.

Вероятно, национальные медицинские организации захотят максимально усилить соответствие при минимизации затрат. Очевидно, что для сотни больниц не является необходимым выполнять в целом те же самые оценки риска. Для решения этой проблемы Национальная служба здравоохранения Великобритании, например, разработала пакет, охватывающий универсальные модели рисков в типичных средах здравоохранения. Впоследствии использование инструмента в местном масштабе фокусируется на создании индивидуального решения в соответствии с местными условиями, сохраняя соответствие с центрально определенной моделью. Аналогичный подход также может быть использован для этапов процесса ИСО/МЭК 27002.

Потенциальной пользой инструментальной поддержки является:

a) упрощенный ввод данных и ведение данных;

b) отчеты в заданном формате и другие выходные данные;

c) упрощенное управление версиями;

d) оптимизированное повторное использование данных во время процесса;

e) последовательность подхода;

f) возможность повторного использования данных и результатов в последующих задачах;

g) возможность сравнения результатов;

h) всесторонний подход;

i) надежность третьих сторон, в особенности аудиторов;

) видимость последствий от принятия решений;

k) поддержка принятия решений и другие процессы управления;

l) способность предпринимать поиск и делать запросы;

m) значительно сниженные затраты, связанные с человеческими ресурсами;

n) относительно легкая передача материала последователям.

С.2 Требуемые свойства инструментов поддержки

Требуемыми свойствами таких инструментов являются:

a) обладающий хорошей репутацией производитель;

b) доступность поддержки и подготовки персонала;

c) поддержание содержания в соответствии с изменениями в стандарте;

d) эффективное объединение с другими офисными инструментами обеспечения производительности;

e) эффективное объединение с операционной системой;

f) эффективный, интуитивно понятный и типичный или графический веб-интерфейс;

g) возможность настройки содержания и выходных данных (в идеале);

h) многопользовательский вспомогательный процесс (в идеале).

С.3 Поддержка инструментов для процесса ИСО/МЭК 27002

Поддержка инструментов для процесса ИСО/МЭК 27002 должна распространяться:

a) на составление определения области применения и описания области применения;

b) анализ пробелов и отчеты по результатам анализа пробелов;

c) определение активов и отчет о состоянии и движении активов;

d) создание плана по безопасному улучшению, ведение записей о предоставлении отчетов и статусе внедрения;

e) ведение записей и создание отчетов по заявлению о применимости;

f) безопасное определение и предоставление отчетов по ресурсам.

Стоит отметить, что все эти процессы взаимодействуют и должны быть в состоянии функционировать между собой.

С.4 Поддержка инструментов для процесса анализа рисков

Функциональность анализа рисков и управления рисками, которые могут быть поддержаны инструментами, охватывают все минимальные процессы, определенные в С.3. Тем не менее более сложные средства дополнительно имеют одно или несколько следующих свойств:

a) библиотечная поддержка модели риска;

b) библиотека активов;

c) инструменты оценки активов;

d) поддержка моделирования зависимостей;

e) группирование активов для эффективности оценки;

f) методологии оценки угроз/активов/воздействия для высокой целостности в пределах оценки;

g) многоуровневая оценка угроз и уязвимостей для соответствия различным потребностям;

h) библиотеки контрмер;

i) функциональные средства назначения приоритетов;

j) оценка затрат масштабирования времени улучшений;

k) поддержка документации по безопасности;

l) функции поддержки принятия решений;

m) поддержка проведения аудита;

n) создание отчетов по обработке рисков;

o) возможность моделирования аварии при проектировании;

p) создание графических отчетов.

Опять же, стоит отметить, что многие из этих процессов взаимодействуют и должны быть в состоянии функционировать между собой.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002—2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO 17090-1 Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services

[2] ISO 17090-2 Health informatics — Public key infrastructure — Part 2: Certificate profile

[3] ISO 17090-3 Health informatics — Public key infrastructure — Part 3: Policy management of certification authority

[4] ISO 22857 Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health information

[5] ISO/TS 22600-1 Health informatics — Privilege management and access control — Part 1: Overview and policy management

[6] ISO/TS 22600-2 Health informatics — Privilege management and access control — Part 2: Formal models

[7] ISO/TS 22600-3 Health informatics — Privilege management and access control — Part 3: Implementations

[8] ISO/TS 21298 Health informatics — functional and structural roles

[9] ISO/TS 21091 Health informatics — Directory services for security, communications and identification of professionals and patients

[10] ISO/TS 25237 Health informatics — Pseudonymisation

УДК 004.61:006.354 ОКС 35.240.80

Ключевые слова: здравоохранение, информатизация здоровья, информация о здоровье, защита информации, менеджмент защиты, технология защиты, технологическая нейтральность

Редактор *А.Ф. Колчин*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 21.04.2016. Подписано в печать 04.05.2016. Формат 60 ×84 $^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 6,15. Тираж 30 экз. Зак. 1228.

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