ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27007— 2014

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по аудиту систем менеджмента информационной безопасности

ISO/IEC 27007:2011
Information technology -- Security techniques -- Guidelines for information security management systems auditing
(IDT)

Издание официальное

Москва
Стандартинформ
2015

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ФГУП «ВНИИНМАШ»), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от «11» июня 2014 г. № 563-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27007:2011 «Информационная технология. Методы обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности» (ISO/IEC 27007:2011 «Information technology – Security techniques – Guidelines for information security management systems auditing»)

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

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном 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 информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

Введение

ИСО/МЭК 27007 был подготовлен совместным техническим комитетом ИСО/МЭК СТК 1, «*Информационная технология*», Подкомитетом ПК 27, «*Методы и средства обеспечения безопасности ИТ*».

Настоящий стандарт предоставляет руководство по менеджменту программы аудита системы менеджмента информационной безопасности (СМИБ) и проведению внутренних или внешних аудитов на соответствие ИСО/МЭК 27001:2005, а также руководство по вопросу компетентности и оценки аудиторов СМИБ, которое следует использовать совместно с руководством, содержащимся в ИСО 19011.

Настоящий стандарт предназначен для всех пользователей, включая малые и средние организации.

В ИСО 19011, «*Руководящие указания по аудиту систем менеджмента*» представлено руководство по менеджменту программ аудита, проведению внутренних или внешних аудитов систем менеджмента, а также по вопросу компетентности и оценки аудиторов систем менеджмента.

Текст настоящего стандарта соответствует структуре ИСО 19011, а дополнительное, ориентированное на СМИБ, руководство по применению ИСО 19011 для аудита СМИБ обозначается буквами «ИБ».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по аудиту систем менеджмента информационной безопасности

Information technology – Security techniques – Guidelines for information security management systems auditing

Дата введения — 2015—06—01

1 Область применения

Настоящий стандарт в дополнение к указаниям, содержащимся в ИСО 19011, предоставляет руководство по менеджменту программы аудита системы менеджмента информационной безопасности (СМИБ), по проведению аудитов и по определению компетентности аудиторов СМИБ.

Настоящий стандарт применим для тех организаций, которые нуждаются в понимании или проведении внутренних или внешних аудитов СМИБ или осуществлении менеджмента программы аудита СМИБ.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок следует использовать только указанное издание. Для недатированных ссылок – последнее издание указанного документа (включая все его изменения).

ИСО 19011:2011 *Руководящие указания по аудиту систем менеджмента* (ISO 19011:2011, *Guidelines for auditing management systems*)

ИСО/МЭК 27001:2005[1)] *Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования* (ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*)

ИСО/МЭК 27000:2009[2)] *Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология* (ISO/IEC 27000:2009, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*)

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана

[1)] Отменен. Действует ИСО/МЭК 27001:2013. Для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только указанный ссылочный стандарт.

[2)] Отменен. Действует ИСО/МЭК 27000:2014. Для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только указанный ссылочный стандарт.

Издание официальное

ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины и определения, приведенные в ИСО 19011 и ИСО/МЭК 27000.

4 Принципы проведения аудита

Применять принципы проведения аудита, приведённые в разделе 4 ИСО 19011:2011.

5 Менеджмент программы аудита

5.1 Общие положения

Применять руководство подраздела 5.1 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.1.1 ИБ 5.1 Общие положения

Должна быть разработана программа аудита[1)] СМИБ, основанная на ситуации, связанной с риском информационной безопасности проверяемой организации.

5.2 Разработка целей программы аудита

Применять руководство подраздела 5.2 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.2.1 ИБ 5.2 Разработка целей программы аудита

Цели программы (программ) аудита должны быть установлены, для того чтобы руководить планированием и проведением аудитов и обеспечивать эффективную реализацию программы аудита. Цели могут зависеть от:

a) идентифицированных требований информационной безопасности;

b) требований ИСО/МЭК 27001;

c) уровня качества функционирования проверяемой организации, который отражает случаи возникновения сбоев и инцидентов информационной безопасности и эффективность измерений;

d) рисков информационной безопасности организации, подвергающейся аудиту.

Примеры целей программы аудита могут включать следующее:

1) проверку соответствия установленным правовым и договорным требованиям, а также иным требованиям и связанным с ними последствиям для безопасности;

2) достижение и поддержку уверенности в возможностях менеджмента риска проверяемой организации.

5.3 Разработка программы аудита

5.3.1 Роли и обязанности лица, осуществляющего менеджмент программы аудита

Применять руководство пункта 5.3.1 ИСО 19011:2011.

5.3.2 Компетентность лица, осуществляющего менеджмент программы аудита

Применять руководство пункта 5.3.2 ИСО 19011:2011.

5.3.3 Определение объема программы аудита

Применять руководство пункта 5.3.3 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.3.3.1 ИБ 5.3.3 Определение объема программы аудита

Объем программы аудита может меняться. Факторы, которые могут влиять на объем программы аудита:

a) масштаб СМИБ, включая:

1) общее количество сотрудников, работающих на каждом объекте, и взаимоотношения со сторонними организациями, регулярно работающими на проверяемом объекте;

[1)] Для целей данного документа использование термина «аудит» относится к аудитам СМИБ.

2) количество информационных систем;
3) количество объектов, охваченных СМИБ;
b) сложность СМИБ (включая количество и критичность процессов и видов деятельности);
c) значимость рисков информационной безопасности, идентифицированных для СМИБ;
d) важность информации и связанных с ней активов в области действия СМИБ;
e) сложность информационных систем, подлежащих аудиту на объекте, включая сложность использованной информационной технологии (ИТ);
f) наличие многих сходных объектов;
g) изменения сложности объектов, находящихся в области действия СМИБ.

В программе аудита следует уделить внимание установлению приоритетов на основе рисков информационной безопасности и требований бизнеса в отношении областей СМИБ, требующих более детального изучения.

Дополнительную информацию о выборке нескольких объектов можно найти в ИСО/МЭК 27006:2007[1)] и IAF MD 1:2007 [7], информация в которых относится только к сертификационным аудитам.

5.3.4 Идентификация и оценка рисков программы аудита

Применять руководство пункта 5.3.4 ИСО 19011:2011.

5.3.5 Разработка процедур по программе аудита

Применять руководство пункта 5.3.5 ИСО 19011:2011.

5.3.6 Идентификация ресурсов для программы аудита

Применять руководство пункта 5.3.6 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.3.6.1 ИБ 5.3.6 Идентификация ресурсов для программы аудита

Для всех существенных рисков, применяемых к проверяемой организации, аудиторам должно быть выделено достаточно времени для проверки эффективности соответствующих мер по уменьшению риска.

5.4 Реализация программы аудита

5.4.1 Общие положения

Применять руководство пункта 5.4.1 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.4.1.1 ИБ 5.4.1 Общие положения

В случае необходимости при реализации программы аудита должны рассматриваться требования конфиденциальности проверяемых и других заинтересованных сторон, включая возможные правовые или договорные требования.

5.4.2 Определение целей, области и критериев для каждого конкретного аудита

Применять руководство пункта 5.4.2 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.4.2.1 ИБ 5.4.2 Определение целей, области и критериев для каждого конкретного аудита

Область аудита должна отражать риски информационной безопасности, соответствующие требованиям бизнеса, и риски бизнеса проверяемой организации.

Дополнительно цели аудита могут включать следующее:

a) оценивание, достаточно ли определена область СМИБ и учтены ли все требования информационной безопасности;
b) оценивание актуальности целей СМИБ, определенных руководством; и
c) оценивание процессов поддержки и эффективного совершенствования СМИБ.

Практическая помощь – примеры критериев аудита

Ниже приведены темы, которые могут быть рассмотрены в качестве критериев аудита:

1) методика оценки риска информационной безопасности и результаты оценки и обработки риска проверяемой организации и учет ими всех соответствующих требований;
2) версия «Положения о применимости» и его связь с результатами оценки риска;
3) готовность к вводу в действие мер и средств контроля и управления для снижения риска;
4) параметры эффективности реализованных мер и средств контроля и управления и применение этих параметров, как определено для измерения эффективности мер и средств контроля и управления (см. ИСО/МЭК 27004);

[1)] Отменен. Действует ИСО/МЭК 27006:2011. Для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только указанный ссылочный стандарт.

5) деятельность по мониторингу и проверке процессов СМИБ и мер и средств контроля и управления;

6) внутренние аудиты и проводимые руководством проверки СМИБ и корректирующие меры, принимаемые организацией;

7) информация об адекватности и соблюдении политик, целей и процедур, принятых проверяемой организацией;

8) соответствие конкретным правовым и договорным требованиям, а также иным требованиям, важным для проверяемой организации, и их значение для информационной безопасности.

Аудиторская группа должна обеспечить уверенность, что область действия и границы СМИБ проверяемой организации четко определены с точки зрения характеристик деятельности организации, ее месторасположения, активов и технологий, включая детали и обоснование каких-либо недопущений в области действия. Аудиторская группа должна подтвердить, что проверяемая организация в области действия СМИБ учитывает требования, изложенные в пункте 1.2 ИСО/МЭК 27001:2005.

Следовательно аудиторы должны обеспечить уверенность, что оценка и обработка риска информационной безопасности проверяемой организации надлежащим образом отражают её деятельность и ограничены сферой деятельности. Аудиторы должны подтвердить, что это отражено в «Положении о применимости».

Аудиторы также должны обеспечить уверенность, что взаимодействие с услугами или видами деятельности, не полностью входящими в сферу действия СМИБ, рассматривается в рамках СМИБ и включено в оценку риска информационной безопасности проверяемой организации. Примером такой ситуации является коллективное использование средств (например, систем ИТ, баз данных и телекоммуникационных систем) вместе с другими организациями.

5.4.3 Выбор методов аудита

Применять руководство пункта 5.4.3 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.4.3.1 ИБ 5.4.3 Выбор методов аудита

В случае проведения совместного аудита особое внимание должно уделяться сообщению информации во время аудита. Соглашение об этом должно быть достигнуто со всеми заинтересованными сторонами до начала аудита.

5.4.4 Формирование группы по аудиту

Применять руководство пункта 5.4.4 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

5.4.4.1 ИБ 5.4.4 Формирование группы по аудиту

Общая компетентность аудиторской группы должна включать:

a) адекватные знания и понимание менеджмента риска информационной безопасности, являющиеся достаточными для оценки используемых проверяемой организацией методов; и

b) адекватные знания и понимание необходимости обеспечения информационной безопасности и менеджмента информационной безопасности, являющиеся достаточными для оценки комплекта мер и средств контроля и управления, а также планирования, реализации, поддержки и эффективности СМИБ.

При необходимости, следует позаботиться о том, чтобы аудиторы получили необходимый допуск к информации для получения свидетельств аудита.

5.4.5 Закрепление обязанностей по проведению конкретного аудита за руководителем аудиторской группы

Применять руководство пункта 5.4.5 ИСО 19011:2011.

5.4.6 Управление выходными данными программы аудита

Применять руководство пункта 5.4.6 ИСО 19011:2011.

5.4.7 Управление и поддержание записей программы аудита

Применять руководство пункта 5.4.7 ИСО 19011:2011.

5.5 Мониторинг программы аудита

Применять руководство подраздела 5.5 ИСО 19011:2011.

5.6 Анализ и улучшение программы аудита

Применять руководство подраздела 5.6 ИСО 19011:2011.

6 Проведение аудита

6.1 Общие положения

Применять руководство подраздела 6.1 ИСО 19011:2011.

6.2 Организация проведения аудита

6.2.1 Общие положения

Применять руководство пункта 6.2.1 ИСО 19011:2011.

6.2.2 Установление первоначального контакта с проверяемой организацией

Применять руководство пункта 6.2.2 ИСО 19011:2011.

6.2.3 Определение возможности проведения аудита

Применять руководство пункта 6.2.3 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

6.2.3.1 ИБ 6.2.3 Определение возможности проведения аудита

До начала аудита следует запросить проверяемую организацию о наличии записей СМИБ, недоступных для проверки аудиторской группой, например, содержащих конфиденциальную или критичную информацию. Лицо, отвечающее за менеджмент программы аудита, должно определить, возможно ли проведение аудита СМИБ в достаточной мере при отсутствии этих записей. Если делается вывод, что проведение аудита СМИБ в достаточной мере без анализа идентифицированных записей невозможно, ответственное лицо должно уведомить проверяемую организацию о невозможности проведения аудита, пока не будут предоставлены соответствующие права доступа или предложена альтернатива.

6.3 Подготовка к проведению аудита

6.3.1 Выполнение анализа документов при подготовке к аудиту

Применять руководство пункта 6.3.1 ИСО 19011:2011.

6.3.2 Подготовка плана аудита

Применять руководство пункта 6.3.2 ИСО 19011:2011.

6.3.3 Распределение работ между членами группы по аудиту

Применять руководство пункта 6.3.3 ИСО 19011:2011.

6.3.4 Подготовка рабочих документов

Применять руководство пункта 6.3.4 ИСО 19011:2011.

6.4 Проведение аудита

6.4.1 Общие положения

Применять руководство пункта 6.4.1 ИСО 19011:2011.

6.4.2 Проведение предварительного совещания

Применять руководство пункта 6.4.2 ИСО 19011:2011.

6.4.3 Выполнение анализа документов во время проведения аудита

Применять руководство пункта 6.4.3 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

6.4.3.1 ИБ 6.4.3 Выполнение анализа документов во время проведения аудита

Аудиторы должны проверить наличие документации и ее соответствие требованиям ИСО/МЭК 27001

Аудиторы должны подтвердить, что выбранные меры и средства контроля и управления связаны с результатом процесса оценки и обработки риска и могут быть впоследствии прослежены до политики и целей СМИБ.

Примечание – В приложении А настоящего стандарта представлено руководство по проведению аудита процессов СМИБ и документации СМИБ.

6.4.4 Обмен информацией в процессе проведения аудита

Применять руководство пункта 6.4.4 ИСО 19011:2011.

6.4.5 Роль и обязанности сопровождающих лиц и наблюдателей

Применять руководство пункта 6.4.5 ИСО 19011:2011.

6.4.6 Сбор и верификация информации

Применять руководство пункта 6.4.6 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

6.4.6.1 ИБ 6.4.6 Сбор и верификация информации

Сбор информации и свидетельств о реализации и эффективности процессов СМИБ, а также о мерах и средствах контроля и управления является важной частью аудита СМИБ. Возможные методы сбора соответствующей информации во время аудита включают:

a) проверку информационных активов и процессов СМИБ, а также мер и средств контроля и управления, реализуемых для них; и

b) использование автоматизированных инструментальных средств аудита.

Примечание – В приложении А настоящего стандарта представлено руководство по проведению аудита процессов СМИБ.

Аудиторы СМИБ должны обеспечивать надлежащее обращение со всей информацией, полученной от проверяемой организации в соответствии с соглашением между проверяемой организацией и аудиторской группой.

6.4.7 Формирование выводов аудита

Применять руководство пункта 6.4.7 ИСО 19011:2011.

6.4.8 Подготовка заключений по результатам аудита

Применять руководство пункта 6.4.8 ИСО 19011:2011.

6.4.9 Проведение заключительного совещания

Применять руководство пункта 6.4.9 ИСО 19011:2011.

6.5 Подготовка и рассылка отчета по аудиту

6.5.1 Подготовка отчета по аудиту

Применять руководство пункта 6.5.1 ИСО 19011:2011.

6.5.2 Рассылка отчета по аудиту

Применять руководство пункта 6.5.2 ИСО 19011:2011.

6.6 Завершение аудита

Применять руководство подраздела 6.6 ИСО 19011:2011.

6.7 Действия по результатам аудита

Применять руководство подраздела 6.7 ИСО 19011.

7 Компетентность и оценка аудиторов

7.1 Общие положения

Применять руководство подраздела 7.1 ИСО 19011:2011.

7.2 Определение компетентности аудитора для удовлетворения потребностей программы аудита

7.2.1 Общие положения

Применять руководство пункта 7.2.1 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

7.2.1.1 ИБ 7.2.1 Общие положения

При принятии решения об уровне владения аудитором соответствующими знаниями и навыками необходимо учитывать следующее:

a) сложность СМИБ (например, критичность информационных систем, специфика риска относительно СМИБ);

b) вид(ы) деятельности бизнеса, осуществляемой в области действия СМИБ;

c) уровень и разнообразие технологий, использованных при реализации различных компонентов СМИБ (например, реализованные меры и средства контроля и управления, контроль документации и/или процессов, корректирующие/превентивные действия и т. д.);

d) количество площадок;

e) ранее продемонстрированное функционирование СМИБ;

f) объем соглашений по аутсорсингу и с третьими сторонами, используемых в области действия СМИБ;

g) стандарты, правовые и иные требования, имеющие отношение к программе аудита.

7.2.2 Личные качества

Применять руководство пункта 7.2.2 ИСО 19011:2011.

7.2.3 Знания и навыки

7.2.3.1 Общие положения

Применять руководство подпункта 7.2.3.1 ИСО 19011:2011.

7.2.3.2 Общие знания и навыки аудиторов систем менеджмента

Применять руководство подпункта 7.2.3.2 ИСО 19011:2011.

7.2.3.3 Знания и навыки аудиторов систем менеджмента, касающиеся особенностей дисциплины и области ее применения

Применять руководство подпункта 7.2.3.3 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

7.2.3.3.1 ИБ 7.2.3.3 Знания и навыки аудиторов систем менеджмента, касающиеся дисциплины и областей ее применения

Аудиторы СМИБ должны обладать знаниями и навыками в следующих областях:

a) методы менеджмента информационной безопасности: это позволит аудитору исследовать СМИБ и сформировать соответствующие выводы аудита и рекомендации. Знания и практические навыки в этой области должны включать:

1) терминологию информационной безопасности;

2) принципы менеджмента информационной безопасности и их применение;

3) методы менеджмента риска информационной безопасности и их применение;

b) общие знания информационной технологии и методы обеспечения информационной безопасности, исходя из реальной ситуации (например, методы физического и логического контроля доступа; обеспечение защиты от вредоносной программы; методы менеджмента уязвимостей и т. д.) или доступ к ним;

c) существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления, а также основной организационный, правовой и договорной контекст СМИБ (например, меняющиеся процессы бизнеса и взаимоотношения, технологии или законы).

Если требуются дополнительные специальные знания и/или навыки, следует рассмотреть вопрос о привлечении экспертов по информационной безопасности (например, обладающих компетентностью в конкретной области деятельности, компетентностью в области обеспечения безопасности ИТ или менеджмента непрерывности бизнеса). В случае привлечения экспертов необходимо тщательно оценить их компетентность.

Примечание – Особые требования к аудиторам в отношении сертификации СМИБ приведены в ИСО/МЭК 27006.

7.2.3.4 Общие знания и навыки руководителя группы по аудиту

Применять руководство подпункта 7.2.3.4 ИСО 19011:2011.

7.2.3.5 Знания и навыки для аудита систем менеджмента по множеству дисциплин

Применять руководство подпункта 7.2.3.5 ИСО 19011:2011.

7.2.4 Достижение требуемого уровня компетентности аудиторов

Применять руководство пункта 7.2.4 ИСО 19011:2011. Дополнительно применять приведенное ниже руководство, ориентированное на СМИБ.

7.2.4.1 ИБ 7.2.4 Достижение требуемого уровня компетентности аудиторов

Аудиторы СМИБ должны обладать знаниями и навыками в области информационных технологий и информационной безопасности, подтвержденными, например, соответствующими сертификатами, а также должны быть способны понять соответствующие требования бизнеса. Опыт работы аудиторов СМИБ должен также способствовать развитию их знаний и навыков в области СМИБ.

7.2.5 Руководитель группы по аудиту

Применять руководство пункта 7.2.5 ИСО 19011:2011.

7.3 Определение критериев оценки аудитора

Применять руководство подраздела 7.3 ИСО 19011:2011.

7.4 Выбор соответствующего метода оценки аудитора

Применять руководство подраздела 7.4 ИСО 19011:2011.

7.5 Проведение оценки аудитора

Применять руководство подраздела 7.5 ИСО 19011:2011.

7.6 Поддержание и повышение компетентности аудитора

Применять руководство подраздела 7.6 ИСО 19011:2011.

Приложение А
(справочное)

Практическое руководство по аудиту СМИБ

В настоящем приложении представлено общее руководство по проведению аудита процессов СМИБ, согласно требованиям ИСО/МЭК 27001. При этом не принимаются во внимание какие-либо особые требования СМИБ, которые могут существовать у конкретной организации (например, правовые, нормативные и договорные требования, а также иные требования, относящиеся к реализации конкретных мер и средств контроля и управления информационной безопасностью).

Это руководство является справочным и предназначено для использования аудиторами, проводящими внутренний или внешний аудит СМИБ.

Необязательные дополнительные стандарты могут быть использованы как справочное руководство для проверяемой организации или аудитора. В приведенной таблице А.1 они перечислены как «Сопутствующие стандарты». Аудиторам следует помнить, что выводы о несоответствиях должны основываться исключительно на критериях аудита и требованиях ИСО/МЭК 27001.

Таблица А.1 – Практическое руководство по аудиту СМИБ

А.1 Сфера действия, политика и подход к оценке риска СМИБ (ИСО/МЭК 27001, подраздел 4.1, перечисления a)–c) пункта 4.2.1)	
Критерии аудита	ИСО/МЭК 27001[1)], подраздел 4.1, перечисления a), b) и c) пункта 4.2.1
Сопутствующие стандарты	ИСО/МЭК 17021, перечисления a)-d) пункта 9.2.1 ИСО/МЭК 27005, подразделы 3.1-3.9 (ИСО/МЭК Руководство 73) ИСО/МЭК 27005, подразделы 7.1, 7.2, 7.3 и 7.4 ИСО/МЭК 27006 подразделы 3.1, 3.5, пункт 9.1.2 и перечисления b)-d) подпункта 9.1.4.2
Свидетельства аудита	Свидетельства аудита включают: - область действия СМИБ (перечисление b) пункта 4.3.1); - схему организационной структуры; - стратегию организации; - формулировку политики бизнеса, бизнес-процессы и виды деятельности; - документацию, касающуюся ролей и обязанностей; - конфигурацию сети; - информацию об объектах, включая список отделений, фирм, офисов и помещений и их схемы размещения; - взаимодействия и зависимости, которые деятельность бизнеса, осуществляемая в рамках области действия СМИБ, имеет вне ее области действия; - соответствующие законы, предписания и договоры; - основную информацию об активах; - документированную политику СМИБ.
Практическое руководство по аудиту	**Система менеджмента информационной безопасности (раздел 4)**
	Общие требования (подраздел 4.1)
	Общий контекст СМИБ определяется в соответствии с подразделом «4.1 Общие требования» ИСО/МЭК 27001, охватывая все требования, изложенные в последующих по отношению к 4.1 разделах. В течение выполнения аудита следует подтвердить, что СМИБ: - сформирована и осуществлена в контексте общей деятельности бизнеса организации и рисков, с которыми она сталкивается; - документально оформлена, удовлетворяя требованиям документирования (изложенным в подразделе 4.3). Кроме того, должно быть продемонстрировано, что СМИБ установлена, реализована, приведена в действие, подвергается мониторингу и проверкам, поддерживается и совершенствуется. Например, организация демонстрирует свою способность выполнения этих процессов.
	Разработка и управление СМИБ (подраздел 4.2)
	Разработка СМИБ ()
	Область действия СМИБ (перечисление a) пункта 4.2.1)

[1)] Ссылки без указанной даты относятся к версии стандарта, приведенной в «Нормативных ссылках» или «Библиографии».

Продолжение таблицы А.1

	Аудитор должен проверить и подтвердить, что организация определила сферу действия и границы СМИБ. Область действия СМИБ должна быть идентифицирована, чтобы обеспечить уверенность в том, что в СМИБ учтены все важные активы и осуществляется менеджмент риска. Кроме того, нужно идентифицировать границы, взаимодействия и зависимости для рассмотрения вопроса рисков, которые могут возникать через них. Нужно подтвердить, что информация об организации была собрана с целью определения контекста, в котором действует организация, и отношения организации к СМИБ и процессам менеджмента риска информационной безопасности для определения области действия и границ. Аудитор должен подтвердить, что организация принимала во внимание следующую информацию, чтобы определить область действия и границы: - стратегии, цели бизнеса и политики организации; - бизнес-процессы; - функции и структуру организации; - правовые, нормативные и договорные требования, имеющие отношение к организации; - основные информационные активы; - месторасположение организации и ее географические характеристики; - ограничения, влияющие на организацию; - ожидания заинтересованных сторон; - социально-культурную среду; - интерфейсы (например, информационный обмен со средой). Следует проверить и подтвердить предоставление организацией обоснования для любого исключения из области действия. Следует подтвердить наличие у организации собственных служб и администрации, способных обеспечить уверенность в постоянном действии СМИБ в течение всего жизненного цикла (подраздел 4.1 ИСО/МЭК 27001 и подраздел 3.5 ИСО/МЭК 27006). Дальнейшее руководство по аудиту области СМИБ приведено в пункте 6.2.3 настоящего стандарта.
	Политика СМИБ (перечисление b) пункта 4.2.1)
	Аудитор должен подтвердить, что политика СМИБ организации конкретным образом описана с точки зрения характеристик бизнеса, организации, ее месторасположения, активов и технологий. Аудитор должен также подтвердить, что политика СМИБ четко идентифицирует: - структуру для установления целей СМИБ (исходную информацию и логическое обоснование для установления целей, а в случае описания политики СМИБ и политик информационной безопасности в одном документе – цели), а также направление и принципы действий с точки зрения руководства; - необходимые требования бизнеса, правовые и договорные требования, а также иные требования, важные для проверяемой организации; - положение менеджмента риска информационной безопасности по отношению к общему менеджменту риска организации и их взаимодействие, включая CSR, внутреннее управление, финансовый контроль и безопасность и т. д.; - логическое обоснование для менеджмента рисков, например, какие основные активы должны рассматриваться как важные с точки зрения защиты и какие аспекты информационной безопасности, т. е. конфиденциальность, целостность или доступность, должны оцениваться наиболее серьезно при проведении оценки риска СМИБ; - одобрение и ответственность высшего руководства. Аудит политики СМИБ может проводиться путем: - подтверждения того, что политика СМИБ создана как документ, который включает подписи или печати, указывающие, что политика утверждена высшим руководством; - подтверждения посредством соответствующих документов, что процедуры создания политики (например, способы санкционирования или проверки политики в организации) и правила для этих процедур определены, правила документально оформлены и методы контроля документации специфицированы; - бесед с руководством, чтобы понять его подход и ответственность в организации СМИБ; - оценивания, посредством изучения протоколов и записей по результатам проводимых руководством проверок, участия и заинтересованности руководства в реализации, поддержке и совершенствовании политики СМИБ; - оценки эффективности доведения руководством политики СМИБ, например, сосредотачивая ее на конкретной аудитории, на всех уровнях организации;

Продолжение таблицы А.1

	- проведение бесед с персоналом, находящимся в области действия СМИБ, чтобы проверить осознание им важности выполнения целей информационной безопасности, соблюдения политики информационной безопасности и своих обязанностей, связанных с информационной безопасностью; - рассмотрение политики информационной безопасности (если это возможно) и ее связи с политикой СМИБ. Аудит целей СМИБ может проводиться путем подтверждения того, что: - цели СМИБ организации определены, отражены в политике СМИБ и согласованы с общими целями бизнеса; - меры и средства контроля и управления и процессы СМИБ идентифицированы и документально оформлены в соответствии с целями СМИБ; - цели документированы в достаточной мере; - цели СМИБ соответствующим образом доведены до всех уровней организации; - в организации определены лица, ответственные за ресурсы, необходимые для достижения целей. Рекомендуется, чтобы аудитор изучал документально оформленную политику и цели СМИБ на этапе аудита, посвященном проверке документации. Политика и цели СМИБ должны пересматриваться и обновляться в соответствии с изменениями контекста менеджмента риска. Аудитор должен подтвердить проведение постоянного совершенствования по отношению к контексту среды бизнеса. Аудитор должен иметь в виду, что соответствие политике СМИБ и выполнение целей может измеряться количественным или качественным образом.
	Подход к оценке риска (перечисление c) пункта 4.2.1)
	ИСО/МЭК 27001 требует от организаций определения подхода к оценке риска, в перечислениях d)–f) пункта 4.2.1 определены элементы этого подхода. В ИСО/МЭК 27001 не указан какой-то определенный подход к оценке риска, в нем просто отмечается, что любой подход является приемлемым, пока он отвечает его требованиям. Аудитор должен проверить, что подход к оценке риска соответствует требованиям к оценке риска, приведенным в ИСО/МЭК 27001, подходит для организации и соответствует существующему общему подходу к менеджменту риска. Необходимо подтвердить, что подход к оценке риска реализован с целью идентификации рисков бизнес-процессов и деятельности и принятия соответствующих мер в отношении рисков. ИСО/МЭК 27005 предоставляет руководство по оценке риска и менеджменту риска. Аудитор должен сознавать, что для оценки риска существуют количественные и качественные методы или любые их комбинации и решение о том, какой подход использовать, зависит от организации. Процессы и процедуры, приведенные в перечислениях c)–j) пункта 4.2.1 ИСО/МЭК 27001:2005, должны быть определены, реализованы и документально оформлены как подход к оценке риска в соответствии с заявлением руководства, описанным в политике СМИБ организации (см. перечисление b) 4) пункта 4.2.1 ИСО/МЭК 27001:2005 – критерии оценки рисков). В определение подхода включается рассмотрение соответствия правовым и договорным требованиям, а также иным требованиям, важным в отношении рисков и активов, которыми организация должна стратегически управлять, в контексте бизнеса и оценивания риска. Во время аудита должно быть подтверждено, что подход реализован и выполняется, как требуют перечисления b)–j) пункта 4.2.1 ИСО/МЭК 27001:2005. Аудитор должен подтвердить, что результаты оценок риска, полученные в соответствии с подходом к оценке риска, сопоставимы и воспроизводимы. Иными словами, аудитор должен подтвердить, что подход позволяет любым сотрудникам, отвечающим за оценку риска, придти к одинаковым результатам независимо от того, кто и когда проводит оценку риска, при условии, что они обладают определенным уровнем компетентности в сфере оценки риска и проводят оценки одних и тех же активов в соответствии с процессами и процедурами, определенными в подходе. Если получается иной результат, должна быть возможность идентифицировать, где и когда возникло различие в оценке риска. Также для организации необходимо, чтобы существовал подход, способный приводить к одинаковому выбору мер и средств контроля и управления для обработки риска, если оцененные риски одинаковы, т. е. с одним и тем же уровнем риска и свойствами (активы и требования безопасности). Такое подтверждение должно проводиться путём отбора записей из отчетов об оценке риска, для прослеживания в прямом и обратном направлении последовательности процесса оценки риска, вместе с аудитами активов на месте.

Продолжение таблицы А.1

	На критерии принятия риска часто влияют политики менеджмента риска организации, цели, технология, денежные средства, соответствующие законы и предписания и заинтересованные стороны, и в итоге они определяются организацией. Поэтому аудиторам необходимо с должным вниманием проверять эффективность критериев с точки зрения вышеуказанных объектов, подтверждая также, что они определены и существуют. За более детальной интерпретацией критериев принятия риска аудиторы могут обращаться к подразделу 7.2 ИСО/МЭК 27005:2008[1)].
А.2 Идентификация, анализ и оценивание риска, идентификация и оценивание вариантов обработки риска (ИСО/МЭК 27001 перечисления d)–f) пункта 4.2.1)	
Критерии аудита	ИСО/МЭК 27001, перечисления d), e), f) пункта 4.2.1
Сопутствующие стандарты	ИСО/МЭК 27005, подразделы 8.2, 8.3, разделы 9, 10
Свидетельства аудита	Свидетельства аудита включают: - инвентарную опись активов; - документированную методику оценки риска; - отчеты об оценке риска.
Практическое руководство по аудиту	**Идентификация риска (перечисление d) пункта 4.2.1)**
	Аудитор должен проверить инвентарную опись активов, чтобы подтвердить, что все соответствующие значимые активы, входящие в область действия СМИБ, включены в инвентарную опись и для всех активов определены ответственные владельцы. Он должен проверять идентификацию связанных с активами угроз, используемых угрозами уязвимостей и вызываемых ими сбоев обеспечения безопасности, т. е. сценарии инцидентов, указанные в ИСО/МЭК 27005.
	Анализ и оценивание риска (перечисление e) пункта 4.2.1)
	Важно удостовериться, что при оценке риска рассматриваются все важные активы, входящие в область действия СМИБ, и что оценка угроз/уязвимостей в отношении активов адаптирована под организацию, а не просто использует стандартные списки угроз и уязвимостей. Также важно отслеживать риски, которые по своей сути неправильно установлены или значимость которых преуменьшена, например, если соответствующие меры и средства контроля и управления являются дорогостоящими или трудно реализуемыми или если риски были неправильно поняты. Аудитор должен на выборке подтвердить, что все значимые активы, перечисленные в инвентарной описи активов, включены в оценку риска и проверить выборку сценариев инцидентов с оцененным риском, чтобы дать оценку, отражают ли они соответствующим образом потребности и влияния бизнеса. Наличие компетентного персонала важно для хорошего функционирования СМИБ. Аудитор должен оценить свидетельства того, что среднесрочные и долгосрочные риски, связанные с утратой работоспособного персонала, адекватным образом оценены организацией и пересмотрены с учетом последних корректировок и что реализованы соответствующие меры и средства контроля и управления информационной безопасностью для повышения устойчивости организации в отношении таких потерь.
	Варианты обработки риска (перечисление f) пункта 4.2.1)
	Аудитор должен проверить выбранные организацией варианты обработки риска. Следует проверить, специфицирована ли для всех идентифицированных рисков соответствующая «обработка» (т. е. снижение риска посредством применения соответствующих мер и средств контроля и управления, предотвращение риска, перенос риска на третьи стороны или сознательное принятие рисков, если они подпадают под аппетит к риску руководства). Аудитор должен искать расхождения и другие аномалии и проверять, были ли недавние изменения (например, новые системы ИТ или бизнес-процессы) соответствующим образом включены в оценку риска и решения по обработке риска.
А.3 Выбор целей контроля и мер и средств контроля и управления, утверждение предлагаемых остаточных рисков, получение разрешения руководства и «Положение о применимости» (ИСО/МЭК 27001, перечисления g)–j) пункта 4.2.1)	
Критерии аудита	ИСО/МЭК 27001, перечисления g)–j) пункта 4.2.1, Приложение А

[1)] Отменен. Действует ИСО/МЭК 27005:2011. Для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только указанный ссылочный стандарт.

Продолжение таблицы А.1

Сопутствующие стандарты	ИСО/МЭК 27005, подразделы 9.1, 9.2, раздел10 ИСО/МЭК 27006, пункт 9.1.2
Свидетельства аудита	Свидетельства аудита включают: - документированную методику оценки риска; - отчеты об оценке риска; - документы, описывающие степень снижения рисков принятыми мерами и средствами контроля и управления (результаты оценки риска); - записи, указывающие на утверждение остаточных рисков руководством (в частности, в случаях, когда остаточные риски выше уровня, определенного в критериях для принятия рисков, в записи должно быть включено их обоснование); - записи, демонстрирующие санкционирование руководством реализации и введения в действия СМИБ; - положение о применимости.
Практическое руководство по аудиту	**Выбор целей контроля и мер и средств контроля и управления (перечисление g) пункта 4.2.1)**
	Для соблюдения требований информационной безопасности, выведенных из оценки риска, и применения вариантов обработки риска, выбранных для этих требований, аудитор должен проверить на соответствующей выборке, что меры и средства контроля и управления выбраны и запланированные цели контроля достигнуты. Аудитор должен проверить, что выбранные меры и средства контроля и управления и цели контроля соответствуют требованиям информационной безопасности с учётом требований контроля, определенных в приложении А ИСО/МЭК 27001 (что касается интерпретации требований контроля в приложении А, то хорошим справочным материалом могут быть лучшие практические приемы, описанные в ИСО/МЭК 27002 как руководства по реализации). Любые существенные отличия от требований приложения А в выборе мер и средств контроля и управления (например, есть ли не принятые организацией цели контроля и меры и средства контроля и управления из приложения А, или есть ли дополнительные цели контроля и меры и средства контроля и управления, выбранные за рамками приложения А) должны быть идентифицированы и проверены на наличие логического обоснования. Кроме того, аудитор должен проверить, учитывались ли в процессе выбора мер и средств контроля и управления общепринятые лучшие практические приемы для соответствующей сферы бизнеса. Следует проверить, что любые требования информационной безопасности, четко предписанные политиками организации, отраслевыми предписаниями, законами или договорами и т. д., надлежащим образом отражены в документально оформленных целях контроля и мерах и средствах контроля и управления и что риски снижены до четких критериев принятия рисков. Следует подтвердить, что обработка рисков применяется повторно, если остаточные риски не удовлетворяют критерию принятия рисков даже после принятия мер и средств контроля и управления.
	Утверждение предлолагаемых остаточных рисков (перечисление h) пункта 4.2.1) **Получение разрешения руководства (перечисление i) пункта 4.2.1)**
	Аудитор должен вкратце оценить остаточные риски информационной безопасности и подтвердить, что организация получила одобрение руководства в отношении остаточных рисков, которые остаются после выбора мер и средств контроля и управления для обработки рисков. Следует проверить, что руководство провело формальное рассмотрение и принятие остаточных рисков, что риски находятся в рамках определенного аппетита организации к риску, что решения о принятии риска принимаются руководством в форме распоряжения на достаточно авторитетном уровне и что в случаях, когда уровни остаточных рисков не могут быть снижены ниже критериев принятия, руководство принимает решение об официальном принятии рисков и причины такого решения фиксируются. Кроме того, аудитор должен подтвердить, что руководство санкционировало реализацию и введение в действие СМИБ, например, посредством официального приказа, утверждения проекта, письма с выражением поддержки от исполнительного директора и т. д. Следует проверить, что это не простая формальность, а существуют свидетельства того, что руководство действительно понимает и поддерживает СМИБ.
	Положение о применимости (перечисление j) пункта 4.2.1)
	Аудитор должен проверить «Положение о применимости» организации, в котором документированы и обоснованы цели контроля и меры и средства контроля и управления, как применяемые, так и неприменяемые. Важно, чтобы «Положение о применимости» демонстрировало связь между идентифицированными рисками и выбранными для их снижения мерами и средствами контроля и управления. Также важно, чтобы были приведены обоснования для мер и средств контроля и управления, идентифицированных как неприменяемые. Аудитор должен подтвердить, что для всех перечисленных в приложении А ИСО/МЭК 27001 целей контроля и мер и средств контроля и управления существуют соответствующие записи.

Продолжение таблицы А.1

	«Положение о применимости» также должно включать существующие меры и средства контроля и управления. Необходимо, чтобы «Положение о применимости» проверялось и утверждалось/санкционировалось руководителями соответствующего уровня с записями об истории создания, утверждения, пересмотра, обновления и т. д. в качестве свидетельств.
А.4 Реализация и функционирование СМИБ (ИСО/МЭК 27001, пункт 4.2.2)	
Критерии аудита	ИСО/МЭК 27001, пункт 4.2.2
Сопутствующие стандарты	ИСО/МЭК 27001, приложение А ИСО/МЭК 27002 ИСО/МЭК 27005, подпункт 8.2.1.4, подраздел 9.1
Свидетельства аудита	Свидетельства аудита включают: - план обработки риска и записи о продвижении проектов плана; - документально оформленные процедуры и записи для измерения эффективности контроля.
Практическое руководство по аудиту	Аудитор должен подтвердить, что организация сформулировала и реализовала план обработки риска с идентифицированными вариантами обработки риска. Важно подтвердить, что: - план обработки риска реализован с учетом приоритетов и обязанностей, как было определено; - для поддержки функционирования СМИБ выделены адекватные ресурсы (см. также А.9); - приоритеты и сроки реализации соответствующей обработки риска четко определены; - определены фонды, роли и обязанности для обработки риска; - план обработки риска используется и упреждающим образом обновляется как инструментальное средство менеджмента информационной безопасности. Аудитор должен проверить реализацию и функционирование СМИБ относительно документально оформленных требований СМИБ, производя выборку мер и средств контроля и управления (см. перечисление g) пункта 4.2.1 и приложение А ИСО/МЭК 27001) на предмет их реализации и функционирования. Необходимо искать свидетельства, подтверждающие или опровергающие взаимосвязь между документированными рисками и планируемыми и реализованными мерами и средствами контроля и управления. Аудитор должен подтвердить, что цель и способ измерения эффективности выбранных мер и средств контроля и управления четко определены. В методе измерения эффективности мер и средств контроля и управления важна возможность проверки, действительно ли меры и средства контроля и управления снижают риски или влияния инцидентов (ИСО/МЭК 27005, подпункт 8.2.1.4). При проверке измерений, относящихся к СМИБ, следует обратить внимание на то, что измерения могут выполняться рядом способов, некоторые из которых более сложные, чем другие. Аудитору нужно сознавать, что несмотря на доступность руководства по измерениям, относящимся к СМИБ, требования ИСО/МЭК 27001 будут удовлетворяться, пока критерии получения сопоставимых и воспроизводимых результатов оценки эффективности контроля определены и одобрены руководством. Также важно обеспечить уверенность в том, что измерения, относящиеся к СМИБ, соответствуют требованиям бизнеса организации с учетом результатов процессов оценки и обработки риска. Эффективные измерения убеждают, что контроль фактически снижает соответственные риски. При проверке функционирования СМИБ аудитор должен оценивать, как организация обеспечивает уверенность в эффективности мер и средств контроля и управления. С этой целью аудитор должен оценить степень и достаточность относящихся к СМИБ измерений.
А.5 Мониторинг и пересмотр СМИБ (ИСО/МЭК 27001, пункт 4.2.3)	
Критерии аудита	ИСО/МЭК 27001, пункт 4.2.3
Сопутствующие стандарты	ИСО/МЭК 27005, подразделы 12.1, 12.2
Свидетельства аудита	Свидетельства аудита включают: - отчеты о связанных с безопасностью событиях/инцидентах безопасности; - документацию проводимых руководством проверок (входная и выходная); - описание (процедуры) измерения эффективности мер и средств контроля и управления и записи об измерении и оценке мер и средств контроля и управления; - записи об использовании измерений (включая меры по усилению мер и средств контроля и управления, записи о корректирующих и превентивных мерах, а также план обработки риска); - документы, содержащие информацию об информационных активах, анализе и оценке риска, план обработки риска и положение о применимости; - ежегодный план по обеспечению информационной безопасности.

Продолжение таблицы А.1

Практическое руководство по аудиту	Аудитор должен проверить процессы мониторинга и проверки СМИБ, используя такие свидетельства, как планы, протоколы совещаний по проверкам, отчеты о результатах проводимых руководством проверок/внутренних аудитов СМИБ, отчеты о нарушениях/инцидентах и т. д. Аудитор должен оценить, в какой степени обеспечено обнаружение, оповещение и рассмотрение ошибок обработки, нарушений безопасности или других инцидентов. Важно определить, осуществляет ли (и каким образом) организация эффективную и активную проверку реализации СМИБ, чтобы обеспечить уверенность в том, что меры и средства контроля и управления безопасности, которые определены в плане обработки риска, политиках и т. д., действительно реализованы и действуют. Аудитор должен также проверить относящиеся к СМИБ измерения и их использование для стимулирования постоянного совершенствования СМИБ. Следует также подтвердить, что подлежащие рассмотрению изменения (перечисления d) 1)–6) пункта 4.2.3 в ИСО/МЭК 27001) отражены в процессах идентификации, анализа, оценивания и обработки рисков. Кроме того, следует подтвердить, что документы и записи СМИБ, связанные с оценкой риска, обновляются. Аудитор должен проявить особое внимание к аудиту процессов мониторинга и проверки СМИБ. Они будут сильно различаться в зависимости от вида и размеров организации, мероприятия, которые должны быть продемонстрированы организацией, четко изложены в ИСО/МЭК 27001. Особый интерес для аудиторов представляет результат изменений, т. е. принимала ли организация внутренние и (или) внешние изменения своих операций и оказывали ли эти изменения влияние на СМИБ.
А.6 Поддержка и совершенствование СМИБ (ИСО/МЭК 27001, пункт 4.2.4 и раздел 8)	
Критерии аудита	ИСО/МЭК 27001, подраздел 4.1, пункт 4.2.4, раздел 8
Сопутствующие стандарты	ИСО/МЭК 27001, пункт 4.2.4 и раздел 8
Свидетельства аудита	Свидетельства аудита включают: - отчеты об идентифицированных усовершенствованиях, исходя из мероприятий, определенных в ИСО/МЭК 27001, пункт 4.2.3; - отчеты о несоответствиях; - отчеты о корректирующих/превентивных мерах; - отчеты о связанных с безопасностью событиях/инцидентах безопасности; - документально оформленные процедуры и меры и средства контроля и управления в подтверждение СМИБ; - записи о функционировании СМИБ; - отчеты об оценке риска; - процедуры для корректирующих и превентивных мер; - Положение о применимости
Практическое руководство по аудиту	**Поддержка и совершенствование СМИБ (ИСО/МЭК 27001, пункт 4.2.4)**
	Идентифицированные улучшения, определенные в перечислении a) пункта 4.2.4 ИСО/МЭК 27001, указывают на улучшения, которые были определены в ходе мониторинга и анализа согласно пункту 4.2.3 ИСО/МЭК 27001. Аудитор должен проверить средства и записи, посредством которых определяется потребность в совершенствовании СМИБ, а также способ реализации улучшений. Аудитор должен также искать свидетельства в форме приказов руководства, протоколов совещаний, отчетов, электронных почтовых сообщений и т. д., документирующие потребность в улучшениях, разрешающие их и приводящие к их реализации. Аудиторы СМИБ должны искать документально подтверждённые свидетельства совершенствований политик, процедур, методов, мер и средств контроля и управления, новых оценок риска, проверок и изменений политики информационной безопасности, новых видов деятельности бизнеса, включая новые заинтересованные стороны поддержки (не только ИТ, но также возможностей и предполагаемого срока службы оборудования), мероприятий по информированию и менеджменту инцидентов, изменений процедур обработки и транспортировки информации, а также изменений соответствия правовым, техническим и связанным с безопасностью требованиям, касающимся внешних сторон. Таким образом, при аудите следует также подтвердить, что процедуры и процессы для реализации улучшений соответствуют требованиям, определенным в перечислениях b)–d) пункта 4.2.4 ИСО/МЭК 27001.
	Совершенствование СМИБ (раздел 8)
	Постоянное совершенствование (подраздел 8.1)

Продолжение таблицы А.1

	Аудитор должен проверить, каким образом организация определяет, возможно ли совершенствование СМИБ, как она оценивает взаимосвязанные риски, и как это связано с идентифицированными требованиями безопасности и мониторингом функционирования СМИБ. Аудитор должен проверить, как общие цели организации переводятся через соответствующие процессы во внутренние требования информационной безопасности, и каким образом эти требования сообщаются и подвергаются мониторингу. Таким образом, аудитор должен искать свидетельства того, что организация анализирует данные мониторинга СМИБ и затем использует результаты для оценивания эффективности СМИБ и совершенствования СМИБ в случае необходимости. Аудитор должен подтвердить, что цели и приоритеты совершенствования согласуются с целями СМИБ. Однако в случае, если организация не имеет политики и целей, связанных с постоянным совершенствованием, должен быть сделан вывод, что организация явно не соблюдает стандарт. Если руководство установило (реальную) цель совершенствования, а свидетельства совершенствования отсутствуют, эта информация должна быть возвращена для проводимой руководством проверки, чтобы руководство могло принять решение, какое действие является соответствующим – например, корректирование цели или предоставление других средств для воздействия на процесс. Если организация использует статистику качества функционирования (например, снижение числа определенных инцидентов безопасности) для измерения совершенствования, аудитор должен тщательно оценить, действительно ли эта статистика связана с идентифицированными рисками или не был ли выбор основан только на простоте вычисления.
	Корректирующие действия (подраздел 8.2)
	Аудитор должен получить и проверить информацию о корректирующих действиях, связанных со СМИБ, такую как отчеты и планы действий, являющиеся результатом проводимой руководством проверки(ок) СМИБ или аудитов (см. ИСО/МЭК 27001, подраздел 7.3), запросы об изменениях СМИБ, бюджетные/инвестиционные предложения и технико-экономические обоснования и т. д. Аудитор должен искать свидетельства того, что СМИБ на самом деле существенно улучшилась, как результат обратной связи – проверить документацию, связанную с результатами реализации пунктов плана действий, чтобы подтвердить, действительно ли вопрос несоответствий и их основных причин эффективно разрешается руководством в разумные временные сроки. Часто бывает так, что несоответствия исправляются, однако меры по предупреждению их повторного возникновения не принимаются, потому что анализ основных причин не имел успеха. Вместе с составлением отчетов о корректирующих мерах аудитор должен проверить записи о корректирующих мерах и посредством проведения наблюдения на месте, исходя из реальных случаев, подтвердить, являются ли зафиксированные меры эффективными. С точки зрения менеджмента риска СМИБ анализ основных причин должен быть выполнен: - для установления, не обусловлено ли это фактом, что риски не идентифицированы; - если риски идентифицированы, то для проверки применения к рискам мер и средств контроля и управления; - если риски идентифицированы и к ним применены меры и средства контроля и управления, то для проверки, являются ли примененные меры и средства контроля и управления соответствующими для рисков; - если риски идентифицированы и к ним применены соответствующие меры и средства контроля и управления, то для проверки, эффективно ли реализованы примененные меры и средства контроля и управления и выполнены ли они так, как ожидалось. Любой из вышеприведенных случаев или их комбинация будет причиной несоответствий. В контексте менеджмента риска возникновение несоответствия может рассматриваться как подверженность риску, а потенциальные несоответствия могут рассматриваться как прогнозируемые риски. Аудитор должен проверить и подтвердить с помощью описанного выше детального анализа, установлены ли основные причины несоответствий и принимаются ли соответствующие меры в отношении несоответствий с помощью записей и наблюдаемых фактов на местах, насколько это возможно.
	Превентивные меры (подраздел 8.3)
	В дополнение к проверке осуществления улучшений СМИБ, вытекающих из ранее идентифицированных фактических несоответствий, аудитор должен определить, занимает ли организация более активную позицию в отношении реагирования на потенциальные улучшения, возникающие или проектируемые новые требования и т. д. Аудитор должен искать свидетельства изменений СМИБ (таких как добавление, изменение или устранение мер и средств контроля и управления информационной безопасностью) в ответ на идентификацию существенно изменившихся рисков.

Продолжение таблицы А.1

	При аудите превентивных мер могут учитываться следующие моменты: 1) каким образом организация определяет потенциальные несоответствия и их причины. Типичные примеры включают: - идентификацию новых или изменившихся рисков посредством обновления оценки риска (перечисление d) пункта 4.2.3 и подраздел 8.3 ИСО/МЭК 27001); - анализ тенденций для характеристик СМИБ. Ухудшающаяся тенденция может указывать на то, что в случае непринятия мер может возникнуть несоответствие; - сигналы оповещения для обеспечения раннего предупреждения о приближающихся «неконтролируемых» операционных условиях; - мониторинг инцидентов и анализ тенденций инцидентов; - оценивание несоответствий, произошедших в сходных обстоятельствах, но в отношении других частей СМИБ или других частей организации, или даже других организаций; - процесс планирования, как для предсказуемых ситуаций (например, из-за расширения, технического обслуживания или смены персонала), так и для непредсказуемых ситуаций (например, изменения законодательства, природные проблемы, такие как ураганы, землетрясения, наводнения и т. д.); 2) каким образом организация определяет, какая мера требуется и как эта мера реализуется. Аудитор должен искать свидетельства того, что: - организация проанализировала причины потенциальных несоответствий (для этого может быть уместным использование диаграмм причин и следствий и других инструментальных средств информационной безопасности); - требуемые меры применены во всех соответствующих частях организации и своевременны; - существует четкое определение обязанностей по определению, оцениванию, реализации и проверке превентивных мер; - в случае новых или изменившихся мер и средств контроля и управления осуществляется адекватное обучение; 3) аудитор должен подтвердить, что: - ведутся соответствующие записи; - записи являются истинным отражением результатов; - контроль записей осуществляется в соответствии с пунктом 4.3.3 ИСО/МЭК 27001:2005; 4) для проверки принятых превентивных мер аудитор должен рассмотреть: - являлись ли меры эффективными (т. е. было ли предотвращено возникновение несоответствия и были ли какие-либо дополнительные выгоды); - существует ли потребность продолжать превентивные меры без их изменений; - следует ли изменить превентивные меры или есть ли необходимость планирования новых мер.
А.7 Документация СМИБ (ИСО/МЭК 27001, подраздел 4.3)	
Критерии аудита	ИСО/МЭК 27001, пункты 4.3.1–4.3.3
Сопутствующие стандарты	–
Свидетельства аудита	Свидетельства аудита включают: - документацию СМИБ, указанную в ИСО/МЭК 27001, перечисления a)–i) пункта 4.3.1
Практическое руководство по аудиту	**Требования к документации (подраздел 4.3)**
	Документация СМИБ (пункт 4.3.1)
	Важно идентифицировать требования документирования, специфицированные в СМИБ. Аудитор должен рассмотреть требования пункта 4.3.1 ИСО/МЭК 27001 и несколько положений, указанных в его разделах 5–8 в дополнение к приложению А по мерам и средствам контроля и управления, а также требования, указанные в документации СМИБ организацией. Аудитор должен запросить и получить информацию о функциональных процессах проверяемой организации, провести опрос персонала всех уровней (включая административный персонал, владельцев процессов и операторов) и проследить за их деятельностью и поведением, а также за выполнением процессов, чтобы подтвердить, что реализация и функционирование СМИБ на месте соответствуют документально оформленным и специфицированным требованиям. Необходимость любой документации должна оцениваться в свете наблюдаемой потребности в согласованности, важности содержащейся в ней информации и роли, которую может играть любая документация в предотвращении любых значимых идентифицированных рисков.
	Контроль? документации СМИБ (пункт 4.3.2)

Продолжение таблицы А.1

	Аудитор должен проверить наличие и соблюдение документально оформленной процедуры управления обновлениями документации, политик, процедур, записей СМИБ и т. д. Аудитор должен также определить, осуществляется ли формальное управление изменениями документации СМИБ. Например, изменения просматриваются и заранее утверждаются руководством, а также распространяются среди всех пользователей документации СМИБ, например, путем обновления определенной справочной совокупности материалов, поддерживаемых во внутрикорпоративной сети, и (или) явного уведомления всех соответствующих пользователей.
	Записи СМИБ (пункт 4.3.3)
	Аудитор должен оценить меры и средства контроля и управления, защищающие значимые записи СМИБ, такие как различные отчеты о проверках обеспечения информационной безопасности и отчеты о результатах аудита, планы действий, формальные документы СМИБ (включая их изменения), книги регистрации посетителей, формы предоставления/изменения прав доступа и т. д. Необходимо проверить адекватность мер и средств контроля и управления для идентификации, хранения, защиты, восстановления, времени хранения и уничтожения таких записей, особенно в ситуациях наличия правовых, договорных и иных требований, важных для реализации СМИБ в соответствии с требованиями ИСО/МЭК 27001 (например, защиты персональных данных).
А.8 Ответственность руководства (ИСО/МЭК 27001, раздел 5)	
Критерии аудита	ИСО/МЭК 27001, подраздел 5.1, пункты 5.2.1 и 5.2.2
Сопутствующие стандарты	ИСО/МЭК 27006, перечисление i) подпункта 9.2.3.2.2 ИСО/МЭК 27001, перечисление b) 5) пункта 4.2.1, Приложение А.5.1.1, А.6.1.1 ИСО/МЭК 17021, перечисление f) подпункта 9.2.3.2 ИСО/МЭК 27006, перечисление f) подпункта 9.2.3.2.2 ИСО/МЭК 27005, подраздел 9.2
Свидетельства аудита	Свидетельства аудита включают: - политику СМИБ с датой утверждения, подписями и т. д.; - записи о проверках политики СМИБ; - относящиеся к безопасности планы/графики для мероприятий СМИБ, например, план обработки риска, программа/план обучения и подготовки, программа/план внутреннего аудита и т. д.; - протоколы проверок, проводимых руководством, с входной/выходной документацией, протоколы совещаний комиссии по информационной безопасности организации и т. д.; - документацию ролей и обязанностей; - отчет о результатах внутреннего аудита; - отчет об оценке рисков; - опросы руководства; - записи об утверждении остаточных рисков, утверждении плана обработки риска, записи проводимых руководством проверок, бюджетные решения по бизнес-плану и результаты утверждения запросов о решениях; - записи о проверках мероприятий цикла Планирование-Осуществление-Проверка-Действие и мер и средств контроля и управления; - критерии компетентности; - кадровую документацию и записи о компетентности; - программы/планы подготовки; - отчет и записи о подготовке.
Практическое руководство по аудиту	**Обязательства руководства (подраздел 5.1)**
	Аудитор должен проверить степень ответственности руководства по обеспечению информационной безопасности, используя такие свидетельства, как: - официальное утверждение руководством политики СМИБ; - утверждение руководством целей и планов реализации СМИБ вместе с выделением достаточных ресурсов и установлением соответствующих приоритетов для связанной с ней деятельности (см. также пункт 5.2.1); - четкие роли и обязанности по обеспечению информационной безопасности, включая процесс назначения и принятия ответственности за надлежащую защиту ценных информационных активов; - приказы руководства, электронные почтовые сообщения, протоколы собраний, презентации, информационные совещания, перечни служебных обязанностей и т. д., выражающие поддержку СМИБ и ответственность за неё; - относящиеся к рискам информационной безопасности критерии принятия риска и их официальное принятие, аппетит к риску и т. д.;

Продолжение таблицы А.1

	- определение области, обеспечение ресурсами и инициирование внутренних аудитов и проводимых руководством проверок СМИБ.
	Распределение ресурсов для СМИБ (пункт 5.2.1)
	Аудитор должен проверить, что осуществляется адекватный менеджмент ресурсов, необходимых для реализации, поддержки и совершенствования СМИБ. Это означает, что организация должна идентифицировать, планировать, предоставлять, использовать, контролировать и изменять соответствующие ресурсы, если это требуется. Рекомендуется не проверять менеджмент ресурсов автономно. Независимо от способа структурирования организации и идентификации ею своих процессов аудиторы должны быть способны проверить адекватность и эффективность менеджмента ресурсов для достижения запланированных результатов. Аудиторам важно проверить, оценивала ли организация свое прошлое и текущее функционирование (например, используя анализ затрат и выгод, оценку риска) при решении вопроса о том, какие ресурсы должны выделяться. Менеджмент ресурсов может оцениваться путем опроса руководства и другого ответственного персонала, чтобы проверить наличие соответствующих процессов. Однако это должно подкрепляться собранными во время аудита объективными свидетельствами. Свидетельства могут быть получены на различных этапах аудита – анализ затрат, процесс функционирования и результаты. Это следует выполнять при аудите всех процессов, связанных с ними систем и документации процессов, а именно: - ответственности и обязанностей руководства; - процесса проводимой руководством проверки; - процессов СМИБ, включая менеджмент риска, корректирующие и превентивные меры и постоянное совершенствование; - перечней служебных обязанностей; - бюджетных записей и записей о времени для конкретных мероприятий СМИБ. Аудиторы должны избегать вынесения субъективных решений о достаточности выделенных организацией ресурсов и ограничивать свою роль оценкой эффективности процесса менеджмента ресурсов.
	Информирование и обучение, относящиеся к СМИБ (пункт 5.2.2)
	Аудитор должен проверить подготовку лиц, фактически участвующих в работе СМИБ, и общие мероприятия информирования об информационной безопасности, предназначенные для всех сотрудников. Следует проверить, установлена ли явным образом необходимая компетентность и требования обучения/информированности для специалистов в сфере информационной безопасности и других лиц с конкретными ролями и обязанностями и поддерживаются ли потребности информирования и обучения, относящиеся к информационной безопасности, достаточными средствами из бюджета. Аудитор должен проверить отчеты об оценке обучения и прочее и найти свидетельства, подтверждающие, что любые необходимые меры совершенствования принимаются фактически. Необходимо выборочно проверить, отмечено ли в кадровых записях сотрудников связанное со СМИБ обучение и т. д. (где это возможно). Аудитор должен оценить общий уровень информированности об информационной безопасности посредством опросов/выборки или проверки результатов опросов/выборки, производимых в рамках СМИБ. Для удовлетворения требованиям компетентности/эффективности ИСО/МЭК 27001 организации обычно нужно выполнить следующее: - определить уровень компетентности, которым должен обладать персонал, выполняющий работу, которая влияет на информационную безопасность; - определить, какой персонал, уже выполняющий работу, обладает требуемой компетентностью; - решить, какая дополнительная компетентность требуется; - решить, как эта дополнительная компетентность должна достигаться – обучение персонала (внутреннее или внешнее), теоретическая или практическая подготовка, наем нового компетентного персонала, поручение существующему компетентному персоналу другой работы; - проверить эффективность действий, предпринимаемых для удовлетворения потребностей компетентности; - периодически проверять компетентность персонала. На протяжении процесса аудита организация обязана поддерживать соответствующие записи об образовании, обучении, навыках и опыте. Однако ИСО/МЭК 27001 не определяет, как будет устанавливаться этот процесс или точный характер поддерживаемых записей. 1) При аудите соответствия организации требованиям оценивания компетентности и обучения аудитор, как правило, должен искать свидетельства рассмотрения следующих вопросов.

Продолжение таблицы А.1

	Организации нужно идентифицировать, какой компетентностью должен обладать персонал, выполняющий работу, которая влияет на информационную безопасность. Целью аудитора должно быть определение, существует ли систематический подход для идентификации такой компетентности и проверка эффективности этого подхода. Выходом процесса может быть перечень, реестр, база данных, кадровый план, план повышения компетентности, договор, план проекта или продукции и т. д. Сначала должны быть проведены беседы с руководством, чтобы удостовериться, что оно понимает важность определения требуемой компетентности. Беседы с руководством также могут служить потенциальным источником информации о новых или меняющихся видах деятельности или процессах, которые могут приводить к иным требованиям компетентности в организации. Проверка компетентности может быть также необходима при рассмотрении нового тендера или договора. Свидетельства этого могут быть найдены в соответствующих записях. Требования компетентности могут быть включены в документацию договоров, в которых действия субподрядчиков могут оказывать влияние на процессы и/или информационную безопасность. Аудиторам нужно установить, определила ли организация новые или изменившиеся потребности в компетентности, например, во время надзорного аудита. 2) Аудитор должен проверить квалификацию персонала, реализующего на рабочих местах меры и средства контроля и управления информационной безопасностью. Аудитор должен проверить наличие некоторой формы процесса оценки, чтобы удостовериться, что компетентность соответствует деятельности организации и что персонал, выбранный как компетентный, демонстрирует соответствующую компетентность. Процесс должен также подтверждать, что в отношении любых недостатков принимаются меры и что эффективность персонала оценивается. Необходимо убедиться, что мероприятия, влияющие на информационную безопасность, осуществляются компетентными лицами. Свидетельства могут быть получены во время аудита, уделяющего особое внимание процессам, мероприятиям, задачам и продуктам, где вмешательство человека может оказывать наибольшее влияние. Аудитор может проверять перечни служебных обязанностей, мероприятия тестирования или инспектирования, процессы мониторинга, записи проводимых руководством проверок, определение обязанностей и полномочий, записи о несоответствиях, отчеты о результатах аудита, жалобы клиентов, записи об аттестации процессов и т. д. 3) Организации нужно оценивать эффективность действий, предпринимаемых для удовлетворения потребностей компетентности. Организация может использовать ряд методов, включая ролевые игры, оценивание коллегами, наблюдение, проверки записей об обучении и записей в трудовой книжке и/или опросы (дополнительные примеры см. в таблице 2 ИСО 19011:2011). Правомерность конкретного метода оценивания будет зависеть от многих факторов. Например, записи об обучении могут проверяться с целью подтверждения, что курс обучения был успешно завершен (но необходимо обратить внимание на то, что это, в частности, не предоставляет свидетельства компетентности лица, проходящего обучение). Однако тот же метод будет неприемлемым для оценивания удовлетворительности действий аудитора во время аудита. Вместо этого могут потребоваться наблюдения, оценивания коллегами, опросов и т. д. Организации может требоваться демонстрация достижения компетентности персоналом посредством комбинации образования, обучения и/или рабочего опыта. 4) Поддержание компетентности Аудитору нужно проверить наличие некоторой формы эффективного процесса мониторинга и принятия по его результатам мер. Способы осуществления этого включают постоянный процесс повышения квалификации (такой, как описан в подразделе 7.4 ИСО 19011), регулярные оценки персонала и результатов его труда или регулярное инспектирование, тестирование или аудит продукта или системы, за которую отвечают данные лица или группы. Постоянные изменения требований компетентности могут указывать на то, что организация активно поддерживает уровень качества функционирования персонала.
А.9 Внутренние аудиты СМИБ и проверка СМИБ со стороны руководства (ИСО/МЭК 27001, разделы 6 и 7) В этом разделе представлено руководство по внешнему аудиту или руководство по самооценке, что равноценно внутреннему аудиту	
Критерии аудита	ИСО/МЭК 27001, разделы 6, 7
Сопутствующие стандарты	ИСО/МЭК 27005, подраздел 7.9 ИСО/МЭК 27006, пункты 9.1.2, 9.1.4, подпункт 9.2.3.2.2 ИСО/МЭК 17021, подпункты 9.2.3.2, 9.3.2.1
Свидетельства аудита	Свидетельства аудита включают: - программу, планы, отчеты и записи внутренних аудитов; - протоколы проводимых руководством проверок с входными и выходными документами; - отчеты об оценке риска.

Продолжение таблицы А.1

Практическое руководство по аудиту	**Внутренние аудиты СМИБ (раздел 6)**
	Аудитор должен проверить внутренние аудиты СМИБ организации, используя программы и планы аудитов СМИБ, отчеты о результатах аудита, планы действий и т. д. Следует подтвердить, что обязанности по проведению внутренних аудитов СМИБ официально поручены компетентным и надлежащим образом обученным аудиторам. Аудиторы должны определить, до какой степени внутренние аудиты СМИБ подтверждают соответствие СМИБ требованиям, определенным в ИСО/МЭК 27001, правовым и договорным требованиям, а также иным требованиям и требованиям СМИБ организации, установленным в результате процесса оценки риска. Перечисления a)–d) раздела 6 ИСО/МЭК 27001 могут быть распространены на перечни контрольных вопросов для поддержки аудита. Аудитор должен также проверить рассмотрение и контроль согласованных планов действий, корректирующих мер и т. д. в согласованные временны́е сроки, уделяя особое внимание любым просроченным мерам для текущих примеров. Организация должна быть способна извлекать максимальную пользу из использования доступных ресурсов во время проведения внутренних аудитов СМИБ. Должны существовать свидетельства того, что организация: - определила требования компетентности для своих внутренних аудиторов СМИБ; - предоставила соответствующее обучение; - установила процесс мониторинга деятельности своих внутренних аудиторов СМИБ и аудиторских групп; - включила в свои аудиторские группы персонал, обладающий соответствующими характерными для данной области деятельности знаниями (чтобы они могли идентифицировать, где изменения конкретного процесса или деятельности могут приводить к существенным последствиям для информационной безопасности). Следует удостовериться, что организация спланировала внутренние аудиты СМИБ и определила методы аудита, чтобы обеспечить эффективное и результативное использование ресурсов. Это также поможет удостовериться в том, что риски, связанные с ошибками аудита в аудиторском процессе и результатами аудита, сведены к минимуму. У организации должен быть установлен процесс использования результатов прошлых аудитов при планировании будущих внутренних аудитов СМИБ. Аудитор должен проверить, что организация использует подобные данные при установлении частоты аудитов таких процессов и деятельности. Принимая в расчет вышеупомянутые факторы и изучив вопрос, ведет ли процесс внутреннего аудита СМИБ к каким-либо «осязаемым» усовершенствованиям СМИБ, аудитор СМИБ должен быть способен сформировать заключение, реализовала ли организация эффективную программу внутреннего аудита СМИБ. Аудитор СМИБ должен быть также способен сформировать заключение, действительно ли результаты внутренних аудитов СМИБ обеспечивают адекватные свидетельства использования компонентов для усовершенствования процессов СМИБ.
	Проверка СМИБ со стороны руководства (раздел 7)
	Аудит проверки СМИБ со стороны руководства (подраздел 7.1)
	ИСО/МЭК 27001 требует от руководства проведения проверки СМИБ организации через запланированные интервалы времени (по крайней мере, раз в год) для обеспечения уверенности в ее постоянной пригодности, адекватности и эффективности. Нужно определить, когда руководство осуществляло предыдущую проверку СМИБ и когда оно планирует сделать это в следующий раз. Частота проверок должна быть определена, например, в политике СМИБ или в политике менеджмента информационной безопасности. Проверка может проводиться на отдельном совещании, но это не является требованием стандарта. Существует много способов, посредством которых руководство может проводить проверку СМИБ, например, получение и проверка отчетов, электронное взаимодействие или проведение проверки как части регулярных совещаний руководства, где также обсуждаются такие вопросы, как бюджет и плановые цели. Процесс проводимой руководством проверки не должен быть мероприятием, осуществляемым исключительно для удовлетворения требований стандарта и аудиторов; он должен быть интегральной частью процесса управления бизнесом организации. Общая проводимая руководством проверка представляет собой сложный процесс, осуществляемый на различных уровнях организации. Проверка всегда должна быть двусторонним процессом, производимым высшим руководством с участием всех уровней организации. Это участие может быть разнообразным от ежедневных, еженедельных, ежемесячных совещаний подразделений организации до простых обсуждений и отчетов.

Окончание таблицы А.1

	Аудиторы должны искать свидетельства того, что входы и выходы процесса проводимой руководством проверки соответствуют размерам и сложности организации и что они используются для совершенствования СМИБ. Аудиторы должны также рассмотреть, как структурировано руководство организации и как в этой структуре используется процесс проводимой руководством проверки. Записи проводимой руководством проверки необходимы, но их формат не специфицирован. Наиболее распространенным видом записей являются протоколы совещаний, но приемлемыми видами записей могут быть также электронные записи, статистические диаграммы, презентации и т. д. Важно обеспечить наличие свидетельств для демонстрации того, что были учтены все вопросы, перечисленные в разделе 7 ИСО/МЭК 27001:2005, даже если было принято решение, что никакие действия не нужны. Процесс проводимой руководством проверки может также включать элементы планирования СМИБ, где рассматриваются изменения процессов и систем. В этом случае аудиторы должны проверить, учитываются ли следующие моменты: - оцениваются ли предложенные изменения до реализации? - рассматриваются ли вопросы, связанные со СМИБ, при подготовке стратегических планов? - идентифицируются ли необходимые меры и средства контроля и управления до реализации изменений, например, до начала аутсорсинга процесса?
	Входные данные для проверки со стороны руководства (подраздел 7.2)
	Подраздел 7.2 ИСО/МЭК 27001 специфицирует информацию, требуемую для проводимой руководством проверки, и пункты данного подраздела необходимо учесть. Однако это не все вопросы, которые могут быть включены в проверку. Они не могут быть рассмотрены по отдельности или одновременно, а только как часть общей проверки бизнеса. Аудиторы должны сознавать, что исходная информация может быть представлена в различных формах, таких как отчеты, графики тенденций и т. д. Проверяя отчеты, предоставляемые руководству, протоколы и другие записи и/или опрашивая вовлеченных лиц, следует проверить, что входило в предыдущую проводимую руководством проверку(и) (ИСО/МЭК 27001 определяет девять пунктов, указывающих на результаты других аудитов/проверок, отзывы и предложения по усовершенствованию, информацию об уязвимостях и угрозах и т. д.). Необходимо оценить, в какой степени руководство играло активную роль и было полностью вовлечено в проверку(и).
	Результаты проводимой руководством проверки (подраздел 7.3)
	Подраздел 7.3 ИСО/МЭК 27001 специфицирует результаты проводимого руководством процесса проверки и любые требующие включения решения и действия, связанные с перечислениями а)–е) подраздела 7.3. Аудитор должен проверить результаты любой предыдущей проводимой руководством проверки(ок), включая основные решения руководства, планы действий и записи, связанные с подтверждением того, что согласованные действия надлежащим образом выполнены. В качестве результатов проводимого руководством процесса проверки должны существовать свидетельства решений относительно перечислений а)–е), такие как: - изменение политики и целей СМИБ; - планы и возможные меры для совершенствования; - изменение ресурсов; - обновленные планы бизнеса; - бюджет; - обновленное положение о применимости; - обновленное контрольное измерение. Результат связан не только с усовершенствованиями или изменениями, но может включать и решения по другим важным вопросам, таким как планы введения новых технологий, систем или продуктов. При необходимости, нужно подтвердить, что заключительные действия действительно были завершены надлежащим образом, уделяя особое внимание любым действиям, которые не были завершены или были завершены несвоевременно.

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
ИСО/МЭК 27000:2009	IDT	ГОСТ Р ИСО/МЭК 27000–2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ИСО/МЭК 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002–2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
ИСО/МЭК 27004:2009	IDT	ГОСТ Р ИСО/МЭК 27004–2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
ИСО/МЭК 27005:2008	IDT	ГОСТ Р ИСО/МЭК 27005–2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
ИСО/МЭК 27006:2007	IDT	ГОСТ Р ИСО/МЭК 27006–2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности
ИСО/МЭК 19011:2011	IDT	ГОСТ Р ИСО 19011–2012 Руководящие указания по аудиту систем менеджмента
ИСО/МЭК 17021:2011	IDT	ГОСТ Р ИСО/МЭК 17021–2012 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента

Примечание – В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:
– IDT — идентичные стандарты.

Библиография

[1] ISO/IEC 17021:2011, *Conformity assessment – Requirements for bodies providing audit and certification of management systems*

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

[3] ISO/IEC 27003:2010, *Information technology – Security techniques – Information security management system implementation guidance*

[4] ISO/IEC 27004:2009, *Information technology – Security techniques – Information security management – Measurement* (ИСО/МЭК 27004:2009, *Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения*) *

[5] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*

[6] ISO/IEC 27006:2007, *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems* (ИСО/МЭК 27006:2007, *Информационные технологии. Методы и средства обеспечения безопасности. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности*) *

[7] IAF MD 1:2007, *IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling, International Accreditation Forum*

* Официальный перевод этого стандарта находится в Федеральном информационном фонде.

УДК 006.035:004.056.5:004.057.2 ОКС 35.040

Ключевые слова: информационная технология, информационная безопасность, мера и средство контроля и управления, система менеджмента информационной безопасности, аудит, программа аудита, компетентность аудитора

Подписано в печать 20.03.2015. Формат 60x84 1/8.
Усл. печ. л. 3,26. Тираж 31 экз. Зак. 44

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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