ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27006-1—
(проект, первая редакция)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ

Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

Часть 1

Общие положения

(ISO/IEC 27006-1:2024, IDT)

Настоящий проект не подлежит применению до его утверждения

Москва
Российский институт стандартизации
2026

Предисловие

1 ПОДГОТОВЛЕН Федеральным автономным учреждением «Национальный институт аккредитации» (ФАУ НИА) на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 079 «Оценка соответствия»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от «__» _____ 20__ г. № ___

4 Настоящий стандарт идентичен международному документу ISO/IEC 27006-1:2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 1. Общие положения» (ISO/IEC 27006-1:2024 «Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 1: General», IDT).

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 27006—2020

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». 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 ежемесячно издаваемом 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.rst.gov.ru)

Содержание

Введение

ИСО/МЭК 17021-1 устанавливает требования и руководящие указания для органов, проводящих аудит и сертификацию систем менеджмента. Если такие органы намерены соответствовать ИСО/МЭК 17021-1 в части проведения аудита и сертификации систем менеджмента информационной безопасности (СМИБ) согласно ИСО/МЭК 27001, некоторые дополнительные требования и руководящие указания к ИСО/МЭК 17021-1 имеют решающее значение. Они предоставлены в настоящем стандарте.

В настоящем стандарте указаны требования к органам, осуществляющим аудит и сертификацию СМИБ. Он содержит общие требования для таких органов, которые называются органами по сертификации. Соблюдение этих требований призвано гарантировать, что органы по сертификации проводят сертификацию СМИБ компетентным, последовательным и беспристрастным образом, тем самым облегчая признание таких органов и принятие их сертификаций на национальной и международной основе.

Текст в настоящем стандарте соответствует структуре ИСО/МЭК 17021-1:2015.

В настоящем стандарте используются следующие глагольные формы:

– «должен» — указывает на требование;
– «следует» — указывает на рекомендацию;
– «может» — указывает на разрешение;
– «способен» — указывает на возможность или способность.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ

Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

Часть 1

Общие положения

Information security, cybersecurity and privacy protection. Requirements for bodies providing audit and certification of information security management systems. Part 1: General

Дата введения – _____

1 Область применения

Настоящий стандарт устанавливает требования и предоставляет руководящие указания для органов, осуществляющих аудит и сертификацию системы менеджмента информационной безопасности (СМИБ), в дополнение к требованиям, содержащимся в ИСО/МЭК 17021-1.

Требования, содержащиеся в настоящем стандарте, подтверждаются органами, осуществляющими сертификацию СМИБ с точки зрения компетентности и надежности. Руководящие указания, содержащиеся в настоящем стандарте, обеспечивают дополнительную интерпретацию этих требований к органу, осуществляющему сертификацию СМИБ.

Примечание – Настоящий стандарт может использоваться в качестве документа, содержащего критерии аккредитации, паритетной оценки или других процессов аудита.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных – последнее издание (включая все изменения)]:

ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirement (Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования)

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования)

3 Термины и определения

В настоящем стандарте используются термины и определения, приведенные в ИСО/МЭК 17021-1, а также следующие.

ИСО и МЭК ведут терминологические базы данных для использования в сфере стандартизации по следующим адресам:

- платформа онлайн-просмотра ИСО: доступна по адресу https://www.iso.org/obp;

- Электропедия МЭК: доступна по адресу http://www.electropedia.org/

3.1 **документ о сертификации** (certification document): Документ, указывающие на то, что система менеджмента информационной безопасности (СМИБ) заказчика соответствует конкретным стандартам СМИБ и любой дополнительной документации, требуемой в рамках системы менеджмента.

Примечание 1 – Данное определение не ограничивает количество документов, совместно именуемых документами о сертификации.

3.2 **управление (риском)** (control): Мера, которая поддерживает и/или изменяет риск (3.10).

Примечание 1 – Управление включает, но не ограничивает любой процесс, политику, устройство, практику или другие условия и/или действия, которые поддерживают и/или изменяют риск (3.10).

Примечание 2 – Управление не всегда может оказывать желаемый или предполагаемый изменяющий эффект.

[ИСО/МЭК 27002:2022, 3.1.8]

3.3 **внешний контекст** (external context): Внешняя среда, в которой организация (3.9) стремится к достижению своих целей.

Примечание 1 – Внешний контекст может включать следующее:

– культурная, социальная, политическая, правовая, нормативная, финансовая, технологическая, экономическая, природная и конкурентная среда на международном, национальном, региональном или локальном уровне;

– ключевые факторы и тенденции, влияющие на цели организации (3.9);

– взаимоотношения с внешними заинтересованными сторонами, их восприятие и ценности.

[ИСО/МЭК 27000:2018, 3.22]

3.4 **информационная безопасность** (information security): Сохранение конфиденциальности, целостности и доступности информации.

Примечание 1 – Кроме того, могут быть задействованы и другие свойства, такие как подлинность, подотчетность, невозможность отказа и надежность.

[ИСО/МЭК 27000:2018, 3.28]

3.5 **инцидент информационной безопасности** (information security incident): Одно или несколько нежелательных или неожиданных событий информационной безопасности, которые с высокой степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности (3.4).

[ИСО/МЭК 27000:2018, 3.31]

3.6 **информационная система** (information system): Набор приложений, услуг, информационно-технических активов или других компонентов для обработки информации.

[ИСО/МЭК 27000:2018, 3.35]

3.7 **внутренний контекст** (internal context): Внутренняя среда, в которой организация (3.9) стремится к достижению своих целей.

Примечание 1 – Внутренний контекст может включать:

– управление, организационную структуру, обязанности и подотчетности;

– политику, цели и стратегии, направленные на их достижение;

– возможности, понимаемые с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);

– информационные системы (3.6), информационные потоки и процессы принятия решений (формальные и неформальные);

– взаимоотношения с внутренними заинтересованными сторонами, их восприятие и ценности;

– культуру организации (3.9);

– стандарты, руководящие указания и модели, принятые организацией (3.9);

– форму и объем контрактных отношений.

[ИСО/МЭК 27000:2018, 3.38]

3.8 **система менеджмента** (management system): Совокупность взаимосвязанных или взаимодействующих элементов организации (3.9) для разработки политик, целей и процессов для достижения этих целей.

Примечание 1 – Система менеджмента может относиться к одному или нескольким аспектам деятельности, например, менеджмент качества, финансовый менеджмент или экологический менеджмент.

Примечание 2 – Элементы системы менеджмента определяют структуру организации (3.9), роли и ответственность, планирование, функционирование, политики, практики, правила, убеждения, цели и процессы для достижения этих целей.

Примечание 3 – Область применения системы менеджмента может охватывать всю организацию (3.9), конкретные и определенные функции

организации (3.9), конкретные и определенные части организации (3.9) или одну или более функций в группе организаций (3.9).

Примечание 4 – Это один из общих терминов и основных определений для стандартов систем менеджмента ИСО, приведенных в Приложении SL Сводного дополнения ИСО к Директивам ИСО/МЭК, Часть 1. Первоначальное определение было изменено путем изменения примечаний 1–3.

[ИСО/МЭК:2015, 3.5.3]

3.9 **организация** (organization): Лицо или группа лиц, которые имеют свои собственные функции с обязанностями, полномочиями и взаимоотношениями для достижения своих целей.

Примечание 1 – Понятие организации включает, но не ограничивает индивидуального предпринимателя, компанию, корпорацию, фирму, предприятие, орган власти, партнерство, благотворительную организацию или учреждение, или их часть или комбинацию, будь то корпоративные организации или нет, а также государственные или частные.

[ИСО/МЭК 27000:2018, 3.50]

3.10 **риск** (risk): Влияние неопределенности на цели.

Примечание 1 – Влияние выражается в отклонении от ожидаемого – положительном или отрицательном.

Примечание 2 – Неопределенность – это состояние, даже частичное, недостатка информации, связанной с пониманием или знанием события, его последствия или вероятности.

Примечание 3 – Риск часто характеризуется ссылкой на потенциальные «события» (как определено в Руководстве ИСО 73:2009, 3.5.1.3) и «последствия» (как определено в Руководстве ИСО 73:2009, 3.6.1.3) или их комбинацию.

Примечание 4 – Риск часто выражается в терминах комбинации последствий события (включая изменения обстоятельств) и связанной с ним «вероятности» (как определено в Руководстве ИСО 73:2009, 3.6.1.1) возникновения.

Примечание 5 – В контексте систем менеджмента информационной безопасности риски информационной безопасности могут быть выражены как влияние неопределенности на цели информационной безопасности.

Примечание 6 – Риск информационной безопасности связан с вероятностью того, что угрозы будут использовать уязвимости информационного

актива или группы информационных активов и тем самым причинят вред организации (3.9).

[ИСО/МЭК 27000:2018, 3.61]

3.11 **анализ рисков** (risk analysis): Процесс понимания природы риска (3.10) и определения уровня риска.

Примечание 1 – Анализ риска обеспечивает основу для оценивания риска и принятия решений по обработке риска (3.14).

Примечание 2 – Анализ риска включает установление значения риска.

[ИСО/МЭК 27000:2018, 3.63]

3.12 **оценка риска** (risk assessment): Общий процесс идентификации риска, анализа риска (3.11) и оценивания риска.

[ИСО/МЭК 27000:2018, 3.64]

3.13 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией (3.9) в отношении риска (3.10).

[ИСО/МЭК 27000:2018, 3.69]

3.14 **обработка риска** (risk treatment): Процесс модификации риска (3.10).

Примечание 1 – Обработка риска может включать:

– избежание риска путем решения не начинать или не продолжать деятельность, которая приводит к риску;

– принятие или увеличение риска для реализации возможности;

– устранение источника риска;

– изменение вероятности;

– изменение последствий;

– разделение риска с другой стороной или сторонами (включая контракты и финансирование риска);

– сохранение риска путем осознанного выбора.

Примечание 2 – Обработка риска, которая имеет дело с негативными последствиями, иногда называется «снижением риска», «устранением риска», «предотвращением риска» и «сокращением риска».

Примечание 3 – Обработка риска может создавать новые риски

или модифицировать существующие риски (3.10).

[ИСО/МЭК 27000:2018, 3.72]

3.15 **правило** (rule): Принятый принцип или инструкция, в которой излагаются ожидания организации (3.9) относительно того, что требуется делать, что разрешено или не разрешено

[ИСО/МЭК 27002:2022, 3.1.32 — модифицировано, удалено примечание 1]

4 Принципы

Должны применяться принципы ИСО/МЭК 17021-1:2015, Раздел 4.

5 Общие требования

5.1 Правовые и контрактные вопросы

Должны применяться требования ИСО/МЭК 17021-1:2015, 5.1.

5.2 Управление беспристрастностью

5.2.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 5.2. Дополнительно, должны применяться требования и руководящие указания, изложенные в 5.2.2.

5.2.2 Конфликты интересов

Органы по сертификации могут повысить ценность в проведении сертификационных аудитов и инспекционного контроля (например, выявляя возможности для улучшения, которые становятся очевидными в ходе аудита, не рекомендуя конкретные решения), не считая это консультированием или потенциальным конфликтом интересов.

Орган по сертификации не должен проводить внутренние анализы информационной безопасности СМИБ заказчика, подлежащей сертификации. Кроме того, орган по сертификации должен быть

независим от органа или органов (включая любых лиц), которые проводят внутренний аудит СМИБ.

5.3 Обязательства и финансирование

Должны применяться требования ИСО/МЭК 17021-1:2015, 5.3.

6 Требования к структуре

Должны применяться принципы ИСО/МЭК 17021-1:2015, Раздел 6.

7 Требования к ресурсам

7.1 Компетентность персонала

7.1.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 7.1. Дополнительно, должны применяться требования и руководящие указания, изложенные в 7.1.2 и 7.1.3.

7.1.2 Общие требования к компетентности

Орган по сертификации должен определить требования к компетентности для каждой функции сертификации, как указано в ИСО/МЭК 17021-1:2015, Таблица А.1. Орган по сертификации должен учитывать все требования, указанные в ИСО/МЭК 17021-1, а также 7.1.3 и 7.2.2 настоящего стандарта, которые имеют отношение к техническим областям СМИБ, как определено органом по сертификации. Приложение В содержит дополнительные руководящие указания по компетентности.

Орган по сертификации должен определить знания и навыки, необходимые для определенных функций в соответствии с Приложением А.

Если в конкретном стандарте (например, ИСО/МЭК 27006-2) установлены дополнительные конкретные критерии, включая требования к компетентности, они должны применяться.

7.1.3 Установление критериев компетентности

7.1.3.1 Требования к компетентности для проведения аудита СМИБ

7.1.3.1.1 Общие требования

Орган по сертификации должен иметь критерии для проверки компетентности членов аудиторской группы, чтобы гарантировать, что они обладают по крайней мере навыками применения своих знаний по:

a) информационной безопасности;

b) техническим аспектам деятельности, подлежащей аудиту;

c) системам менеджмента;

d) принципам аудита;

Примечание – Дополнительную информацию о принципах аудита можно найти в ИСО 19011.

e) мониторингу, измерению, анализу и оценке СМИБ.

Вышеуказанные требования a) - e) применяются ко всем аудиторам в аудиторской группе. Однако, b) может быть общим для членов аудиторской группы.

Члены аудиторской группы должны в совокупности иметь навыки, соответствующие вышеуказанным требованиям, которые могут быть продемонстрированы посредством опыта их применения.

Члены аудиторской группы должны в совокупности быть компетентными в отслеживании признаков инцидентов информационной безопасности в СМИБ заказчика до соответствующих элементов СМИБ.

От отдельных аудиторов не требуется иметь полный спектр опыта во всех областях информационной безопасности, но аудиторская группа в целом должна обладать соответствующей компетенцией для охвата области СМИБ в ходе аудита.

7.1.3.1.2 Терминология, принципы, практические методики и средства менеджмента информационной безопасности

Каждый аудитор аудиторской группы СМИБ должен обладать знаниями о:

a) структурах, иерархии и взаимосвязях конкретной документации СМИБ;

b) оценке рисков информационной безопасности и менеджменте рисками;

c) процессах, применимых к СМИБ.

Члены аудиторской группы должны в совокупности обладать знаниями о:

d) инструментах, методах, средствах, связанных с менеджментом информационной безопасности, и их применении;

e) современных технологиях, где информационная безопасность может иметь особое значение или представлять проблему.

7.1.3.1.3 Стандарты и нормативные документы системы менеджмента информационной безопасности

Каждый аудитор аудиторской группы СМИБ должен знать все требования, содержащиеся в ИСО/МЭК 27001.

Члены аудиторской группы должны в совокупности знать все элементы управления, содержащиеся в ИСО/МЭК 27001:2022, Приложение А, и их реализацию.

7.1.3.1.4 Практики менеджмента бизнеса

Каждый аудитор аудиторской группы СМИБ должен обладать знаниями о:

a) передовых отраслевых практиках и процедурах по информационной безопасности;

b) политиках и бизнес-требованиях к информационной безопасности;

c) общих концепциях, практических методиках и взаимоотношениях менеджмента бизнеса между политикой, целями и результатами;

d) процессах менеджмента и соответствующей терминологии.

Примечание – К указанным процессам также относятся управление персоналом, внешний и внутренний обмен информацией и другие соответствующие вспомогательные процессы.

7.1.3.1.5 Сектор бизнеса заказчика

Каждый аудитор аудиторской группе СМИБ, должен обладать знаниями о:

a) законодательных и нормативных требованиях в конкретной области информационной безопасности, а также особенностях географического расположения и юрисдикции;

Примечание – Знание законодательных и нормативных требований не предполагает наличия углубленной правовой базы.

b) рисках информационной безопасности, относящихся к сектору бизнеса;

c) общих терминологии, процессах и технологиях, относящихся к сектору бизнеса заказчика;

d) соответствующих практиках сектора бизнеса.

Критерий a) аудиторская группа может распределить между собой.

7.1.3.1.6 Продукция, процессы и организация заказчика

В совокупности члены аудиторской группы должны обладать знаниями о:

a) влиянии типа организации, размера, системы управления, структуры, функций и их взаимоотношений на разработку и внедрение СМИБ, а также деятельность по сертификации, включая аутсорсинг;

b) совокупности видов деятельности в широкой перспективе;

c) законодательных и нормативных требованиях, применимые к продукции или услугам.

7.1.3.2 Требования к компетентности для проведения анализа заявки

7.1.3.2.1 Сектор бизнеса заказчика

Персонал, проводящий анализ заявки с целью: определения необходимой компетентности аудиторской группы, отбора членов аудиторской группы и определения продолжительности аудита, должен обладать знаниями общей терминологии, процессов, технологий и рисков, связанных с сектором бизнеса заказчика.

7.1.3.2.2 Продукция, процессы и организация заказчика

Персонал, проводящий анализ заявки с целью: определения необходимой компетентности аудиторской группы, выбора членов аудиторской группы и определения продолжительности аудита, должен обладать знаниями о влиянии продуктов, процессов, типов организаций, размера, управления, структуры, функций и взаимоотношений заказчика на разработку и внедрение СМИБ, а также деятельность по сертификации, включая функции, предоставляемые извне.

7.1.3.3 Требования к компетентности для анализа отчетов об аудитах и принятия решений о сертификации

7.1.3.3.1 Общие положения

Персонал, анализирующий отчеты об аудитах и принимающий решения о сертификации, должен обладать знаниями, которые позволяют ему проверять соответствие области сертификации, а также изменения в области и их влияние на результативность аудита, в частности, постоянную действительность идентификации интерфейсов и зависимостей и связанных с ними рисков.

Кроме того, персонал, анализирующий отчеты об аудитах и принимающий решения о сертификации, должен обладать знаниями:

a) систем менеджмента в целом;

b) процессов и процедур аудита.

7.1.3.3.2 Терминология, принципы, практические методики и средства менеджмента информационной безопасности

Персонал, анализирующий отчеты об аудитах и принимающий решения о сертификации, должен обладать знаниями о:

a) пунктах, перечисленных в 7.1.3.1.2 a), b) и c);

b) законодательных и нормативных требованиях, относящихся к информационной безопасности.

7.1.3.3.3 Сектор бизнеса заказчика

Персонал, анализирующий отчеты об аудитах и принимающий решения о сертификации, должен обладать знаниями общей терминологии и рисков, связанных с соответствующими практиками сектора бизнеса.

7.1.3.3.4 Продукция, процессы и организация заказчика

Персонал, анализирующий отчеты об аудитах и принимающий решения о сертификации, должен обладать знаниями о продукции, процессах, типах организаций, размере, управлении, структуре, функциях и взаимоотношений заказчика.

7.2 Персонал, участвующий в деятельности по сертификации

7.2.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 7.2. Дополнительно, должны применяться требования и руководящие указания, изложенные в 7.2.2.

7.2.2 Демонстрация знаний и опыта аудитора

7.2.2.1 Общие аспекты

Орган по сертификации должен продемонстрировать, что каждый аудитор обладает знаниями и опытом посредством каждого из следующих действий:

a) признанные квалификации, относящиеся к СМИБ;

b) регистрация в качестве аудитора, где это применимо;

c) участие в курсах повышения квалификации СМИБ и получение соответствующих личных квалификаций;

d) актуальные записи о профессиональном развитии;

e) аудиты СМИБ, засвидетельствованные другим аудитором СМИБ.

7.2.2.2 Отбор аудиторов

В дополнение к 7.1.3.1 процесс отбора аудиторов должен гарантировать, что каждый аудитор:

a) имеет профессиональное образование или подготовку, эквивалентную высшему образованию;

b) имеет практический опыт работы на рабочем месте в области информационных технологий и информационной безопасности, достаточный для работы в качестве аудитора СМИБ;

c) получил достаточную подготовку по аудиту СМИБ и продемонстрировал навыки аудита СМИБ в соответствии с ИСО/МЭК 27001. Этот опыт должен быть получен путем выполнения роли аудитора-стажера под наблюдением аудитора СМИБ (см. ИСО/МЭК 17021-1:2015, 9.2.2.1.4) по крайней мере в одном первоначальном сертификационном аудите СМИБ (этап 1 и этап 2) или ресертификации и по крайней мере в одном инспекционном аудите. Этот опыт должен быть получен в ходе не менее 10 аудито-дней на месте СМИБ и проведенных в течение последних пяти лет. Участие должно включать анализ документов; анализ оценки рисков и ее внедрения, а также отчетность по аудиту;

d) поддерживает соответствующие и актуальные знания и навыки в области информационной безопасности и аудита.

Примечание 1 – Поддержание навыков может быть продемонстрировано посредством постоянного профессионального развития.

Примечание 2 – Орган по сертификации требует наличие каталога критериев компетентности для соответствия вышеуказанным требованиям и доказательствам (см. ИСО/МЭК 17021-1:2015, 7.1.2.).

7.2.2.3 Отбор технических экспертов

Процесс отбора технических экспертов должен гарантировать, что каждый технический эксперт:

a) имеет профессиональное образование или подготовку, эквивалентную высшему образованию;

b) имеет практический опыт на рабочем месте в области информационных технологий и информационной безопасности, достаточный для работы в качестве технического эксперта;

c) поддерживает соответствующие и актуальные знания и навыки в области информационной безопасности.

Примечание – Поддержание навыков может быть продемонстрировано посредством постоянного профессионального развития.

7.2.2.4 Отбор аудиторов на роль руководителя группы

В дополнение к 7.2.2.2 критерии отбора аудитора на роль руководителя группы должны гарантировать, что аудитор активно участвовал во всех этапах не менее трех аудитов СМИБ. Участие должно включать первоначальное определение области действия и планирование, анализ документов, анализ оценки рисков и ее внедрения, а также формальную отчетность по аудиту.

7.3 Привлечение индивидуальных внешних аудиторов и внешних технических экспертов

Должны применяться требования ИСО/МЭК 17021-1:2015, 7.3.

7.4 Записи о персонале

Должны применяться требования ИСО/МЭК 17021-1:2015, 7.4.

7.5 Аутсорсинг

Должны применяться требования ИСО/МЭК 17021-1:2015, 7.5.

8 Требования к информации

8.1 Общедоступная информация

Должны применяться требования ИСО/МЭК 17021-1:2015, 8.1.

8.2 Документы о сертификации

8.2.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 8.2. Дополнительно, должны применяться требования и руководящие указания, изложенные в 8.2.2 и 8.2.3.

8.2.2 Документы о сертификации СМИБ

Документы о сертификации должны быть подписаны должностным лицом, которому предоставлены соответствующие обязанности. Версия Заявления о применимости должна входить в документы о сертификации.

Примечание – Изменение Заявления о применимости, которое не изменяет меры обеспечения в области сертификации, не требует внесения изменений в документы о сертификации.

Если деятельность организации в области сертификации не осуществляется ни в каком-либо определенном физическом месте, в документе(ах) о сертификации должно быть указано, что вся деятельность организации осуществляется удаленно.

8.2.3 Ссылка на другие стандарты в документах о сертификации СМИБ

Документы о сертификации могут ссылаться на национальные и международные стандарты только в том случае, если:

а) организация сравнила все свои необходимые средства управления с теми, которые содержатся в ссылочном(ых) источнике(ах) средств управления, чтобы определить, что она не упустила случайно

ни одного такого ссылочного средства управления в соответствии с ИСО/МЭК 27001:2022, 6.1.3 c);

b) обоснование исключенных ссылочных средств управления указано в Заявлении о применимости (SoA) в соответствии с ИСО/МЭК 27001:2022, 6.1.3 d).

Стандарты на ссылочные средства управления могут быть основаны на ИСО/МЭК 27001:2022, Приложение А, или быть стандартами, которые включают средства управления информационной безопасности.

В документах о сертификации должно быть указано, что набор(ы) средств управления, применяемые в SoA, используются только для ссылки на актуальность включения или исключения средств управления в СМИБ и не используются для оценки соответствия.

8.3 Ссылка на сертификацию и использование сертификационных знаков

Должны применяться требования ИСО/МЭК 17021-1:2015, 8.3.

8.4 Конфиденциальность

8.4.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 8.4. Дополнительно, должны применяться требования и руководящие указания, изложенные в 8.4.2.

8.4.2 Доступ к записям организации

Перед проведением сертификационного аудита орган по сертификации должен попросить заказчика сообщить, если какая-либо связанная с СМИБ информация (такая как записи СМИБ или информация относительно разработки и результативности средств управления) не может быть представлена для анализа аудиторской группой, поскольку она содержит конфиденциальную или секретную информацию. Орган по сертификации должен определить, можно ли провести аудит СМИБ

должным образом в отсутствие такой информации. Если орган по сертификации приходит к выводу, что невозможно провести аудит СМИБ должным образом без анализа выявленной конфиденциальной или секретной информации, он должен сообщить заказчику, что сертификационный аудит не может быть проведен до тех пор, пока не будут предоставлены соответствующие механизмы доступа.

8.5 Обмен информацией между органом по сертификации и его заказчиками

Должны применяться требования ИСО/МЭК 17021-1:2015, 8.5.

9 Требования к процессу

9.1 Деятельность, предшествующая сертификации

9.1.1 Заявка на сертификацию

9.1.1.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.1.1. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.1.1.2.

9.1.1.2 Аспекты процедур по сертификации

Процедуры органа по сертификации не должны предполагать определенный способ внедрения СМИБ или определенный формат для документации и записей. Процедуры по сертификации должны быть сосредоточены на подтверждении того, что СМИБ заказчика соответствует требованиям, указанным в ИСО/МЭК 27001, а также политикам и целям заказчика.

Примечание – Организация может разработать собственные необходимые средства управления или выбрать их из любого источника, поэтому возможно, что организация сертифицирована по ИСО/МЭК 27001, даже если ни одно из ее необходимых средств управления не указано в ИСО/МЭК 27001:2022, Приложение А.

9.1.2 Анализ заявки

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.1.2.

9.1.3 Программа аудита

9.1.3.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.1.3. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.1.3.2, 9.1.3.3, 9.1.3.4, 9.1.3.5 и 9.1.3.6.

9.1.3.2 Общие аспекты

Программа аудита для аудитов СМИБ должна учитывать средства управления информационной безопасности, определенные заказчиком.

Примечание 1 – Средства управления информационной безопасности могут быть из ИСО/МЭК 27001:2022, Приложение А, и/или других применимых стандартов и/или могут быть разработаны самостоятельно.

Примечание 2 – Дополнительные руководящие указания по аудиту приведены в ИСО/МЭК 27007.

9.1.3.3 Применение дистанционного аудита

Органы по сертификации, намеревающиеся проводить деятельность по дистанционному аудиту, должны определить процедуры для определения уровня дистанционной деятельности по аудиту («дистанционные аудиты»), которые могут применяться для аудита СМИБ заказчика. Процедуры должны включать анализ рисков, связанных с использованием дистанционного аудита для заказчика, который должен учитывать следующие факторы:

a) имеющаяся инфраструктура органа по сертификации и заказчика;

b) сектор, в котором работает заказчик;

c) тип(ы) аудита в течение цикла сертификации от первоначального аудита до ресертификационного аудита;

d) компетентность лиц органа по сертификации и заказчика, которые участвуют в дистанционном аудите;

e) ранее продемонстрированное результаты деятельности дистанционных аудитов для заказчика;

f) область сертификации.

Анализ должен быть выполнен до проведения любого дистанционного аудита. Анализ и обоснование использования дистанционного аудита в течение цикла сертификации должны быть задокументированы.

План аудита и отчет об аудите должны включать четкие указания, была ли проведена деятельность по дистанционному аудиту.

Дистанционные аудиты не должны использоваться, если оценка риска выявляет неприемлемые риски для результативности процесса аудита.

Оценка риска должна пересматриваться в течение цикла сертификации, чтобы гарантировать ее постоянную пригодность.

П р и м е ч а н и е – В случае, если заказчик использует виртуальные площадки (т. е. место, где организация выполняет работу или предоставляет услугу, используя онлайн-среду, позволяющую вовлеченным лицам выполнять процессы независимо от физического местоположения), методы удаленного аудита являются важной частью плана аудита.

9.1.3.4 Общая подготовка к первоначальному аудиту

Орган по сертификации должен потребовать от заказчика принятия всех необходимых мер для обеспечения доступа к отчетам по внутреннему аудиту и отчетам независимых анализов информационной безопасности.

9.1.3.5 Периодичность анализов

Орган по сертификации не должен сертифицировать СМИБ, если нет достаточных доказательств, демонстрирующих, что мероприятия по проведению анализа со стороны руководства и внутренних аудитов СМИБ были реализованы, результативны и будут поддерживаться в рамках области сертификации.

9.1.3.6 Область сертификации СМИБ

Аудиторская группа должна провести аудит СМИБ заказчика в объеме, охватываемом установленной областью сертификации, на соответствие всем применимым для сертификации требованиям. Орган по сертификации должен подтвердить, что область применения СМИБ заказчика соответствует требованиям, установленным в ИСО/МЭК 27001:2022, 4.3.

Органы по сертификации должны обеспечить, что оценка и обработка рисков информационной безопасности заказчика надлежащим образом отражают его деятельность и распространяются на границы своей деятельности согласно установленной области сертификации. Органы по сертификации должны подтвердить, что это отражено в области сертификации СМИБ заказчиков и SoA. Орган по сертификации должен проверить наличие SoA для области сертификации.

Органы по сертификации должны обеспечить, что взаимодействие с услугами или видами деятельности, которые не полностью включены в область применения СМИБ, рассматриваются в рамках СМИБ, подлежащей сертификации, и включены заказчиком в оценку рисков информационной безопасности. Примером такого положения может быть совместное использование технических средств (например, ИТ-системы, базы данных и телекоммуникационные системы или аутсортинг бизнес-функций) с другими организациями.

9.1.4 Определение продолжительности аудита

9.1.4.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.1.4. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.1.4.2.

9.1.4.2 Продолжительность аудита

Орган по сертификации должен использовать Приложение С для определения продолжительности аудита.

Примечание – Дополнительные руководящие указания и примеры расчета продолжительности аудита приведены в Приложении D.

9.1.5 Выборка при наличии нескольких мест осуществления деятельности

9.1.5.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.1.5. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.1.5.2.

9.1.5.2 Несколько площадок

9.1.5.2.1 Если заказчик имеет несколько площадок, отвечающих критериям перечислений a) – c), органы по сертификации могут использовать подход к сертификационному аудиту нескольких площадок, основанный на их выборочной проверке:

a) все площадки работают в рамках одной и той же СМИБ, которая централизованно администрируется и подвергается аудиту и подлежит анализу со стороны центрального руководства;

b) все площадки включены в программу внутреннего аудита СМИБ заказчика;

c) все площадки включены в программу анализа СМИБ со стороны руководства заказчика.

9.1.5.2.2 Орган по сертификации, предполагающий использовать подход, основанный на выборочной проверке, должен иметь процедуры, обеспечивающие следующее:

a) при первоначальном анализе договора выявляется, насколько это возможно, разница между площадками, чтобы можно было определить адекватный уровень выборки;

b) репрезентативное количество площадок отобрано органом по сертификации с учетом:

1) результатов внутренних аудитов центрального офиса и (если необходимо) на площадках;

2) результатов анализа со стороны руководства;

3) различий в размерах площадок;

4) различий бизнес-целей площадок;

5) сложности информационных систем на различных площадках;

6) различий в методах работы;

7) различий в видах деятельности;

8) различий в разработке и функционировании средств управления;

9) потенциального взаимодействия с критическими информационными системами или информационными системами, обрабатывающими секретную информацию;

10) любых отличающихся правовых требований;

11) географических и культурных аспектов;

12) рисковых ситуаций на площадках;

13) инцидентов информационной безопасности на конкретных площадках;

c) репрезентативная выборка осуществляется из всех площадок в рамках области применения СМИБ заказчика; этот выбор должен основываться на оценочном выборе с целью отражения факторов, представленных в перечислении b), а также с учетом элемента случайности;

d) каждая включенная в СМИБ площадка, которая подвержена значительным рискам, подвергается аудиту органом по сертификации до проведения сертификации;

e) программа аудита должна быть разработана с учетом вышеуказанных требований и охватывать репрезентативные выборки области сертификации СМИБ в течение трехлетнего периода;

f) в случае обнаружения несоответствия на одной площадке, процедура корректирующих действий применяется ко всем площадкам, на которые распространяется действие сертификата.

Аудит должен охватывать деятельность заказчика, чтобы гарантировать, что единая СМИБ применяется ко всем площадкам и обеспечивает централизованное управление на оперативном уровне. Аудит должен учитывать все вышеуказанные вопросы.

9.1.6 Несколько системы менеджмента

9.1.6.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.1.6. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.1.6.2 и 9.1.6.3.

9.1.6.2 Интеграция документаций СМИБ и других систем менеджмента

Орган по сертификации может принять объединенную документацию (например, в отношении информационной безопасности, качества, здоровья и безопасности и окружающей среды), при условии, что СМИБ четко идентифицирована совместно с соответствующим взаимодействием с другими системами менеджмента.

9.1.6.3 Комбинированные аудиты систем менеджмента

Аудит СМИБ может быть совмещен с аудитами других систем менеджмента при условии, что есть возможность продемонстрировать, что такой аудит отвечает всем требованиям сертификации СМИБ. Все элементы, имеющее значение для СМИБ, должны быть четко обозначены и легко идентифицироваться в отчетах об аудитах. На качество аудита не должно отрицательно влиять совмещение аудитов.

9.2 Планирование аудитов

9.2.1 Установление целей, области и критериев аудита

9.2.1.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.2.1. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.2.1.2 и 9.2.1.3.

9.2.1.2 Цели аудита

Цели аудита должны включать:

a) определение результативности системы менеджмента;

b) обеспечение того, чтобы заказчик на основе оценки рисков определил необходимые средства управления; и

c) определение того, что установленные цели информационной безопасности были достигнуты.

9.2.1.3 Критерии аудита

Критерии аудита СМИБ заказчика должны включать ИСО/МЭК 27001.

9.2.2 Подбор и назначение аудиторской группы

9.2.2.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.2.2.

9.2.3 План аудита

9.2.3.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.2.3. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.2.3.2 и 9.2.3.3.

9.2.3.2 Общие аспекты

План аудита для аудитов СМИБ должен учитывать определенные средства управления информационной безопасности.

П р и м е ч а н и е – Хорошей практикой для органа по сертификации является согласование сроков аудита с проверяемой организацией, чтобы наилучшим образом продемонстрировать всю область сертификации организации. Аспекты могут включать сезон, месяц, день/дату и смены, в зависимости от ситуации.

9.2.3.3 Способы дистанционного аудита

Целью способов дистанционного аудита следует повышение эффективности и результативности аудита, а также поддержка целостности процесса аудита.

План аудита должен ссылаться на инструменты, которые используются для поддержки дистанционному аудиту.

9.3 Первоначальная сертификация

9.3.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.3. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.3.2.

9.3.2 Первоначальный сертификационный аудит

9.3.2.1 Этап 1

На этом этапе аудита орган по сертификации должен получить документацию по проекту СМИБ, охватывающую документацию, предусмотренную в ИСО/МЭК 27001.

Как минимум, следующая информация должна быть предоставлена заказчиком на 1 этапе сертификационного аудита:

a) общая информация по СМИБ и виды деятельности, которые она охватывает;

b) копию требуемой документации СМИБ, указанной в ИСО/МЭК 27001, и, при необходимости, другую сопутствующую документацию.

Орган по сертификации должен получить достаточное понимание структуры СМИБ в контексте организации заказчика, оценки и обработки рисков (включая определенные средства управления), политики и целей

информационной безопасности и, в частности, готовности заказчика к аудиту. Это должно использоваться для планирования 2 этапа аудита.

Результаты 1 этапа должны быть задокументированы в письменном отчете. Орган по сертификации должен проанализировать отчет об аудите 1 этапа, прежде чем принять решение о переходе к 2 этапу. Орган по сертификации должен подтвердить, что члены аудиторской группы 2 этапа обладают необходимой компетентностью. Это может сделать аудитор, возглавляющий группу, которая проводила аудит 1 этапа, если он сочтет это компетентным и целесообразным.

Примечание – Наличие лица из органа по сертификации, которое не участвует в аудите, анализирующего отчет и которое принимает решение о продолжении и подтверждает компетентность членов аудиторской группы для 2 этапа, обеспечивает определенную степень снижения связанных с этих рисков. Однако, другие меры по снижению риска могут быть уже реализованы для достижения той же цели.

Орган по сертификации должен информировать заказчика о дополнительных типах информации и записей, которые могут потребоваться для детального изучения на 2 этапе.

9.3.2.2 Этап 2

На основании результатов, задокументированных в отчете об аудите 1 этапа, орган по сертификации должен разработать план аудита для проведения 2 этапа. Помимо оценки результативного внедрения СМИБ, целью 2 этапа является подтверждение того, что заказчик придерживается своих собственных политик, целей и процедур.

Для этого аудит должен быть сосредоточен на заказчике:

a) лидирующей роли высшего руководства и приверженности целям информационной безопасности;

b) оценке рисков, связанных с информационной безопасностью; аудит также должен гарантировать, что оценки дают последовательные, действительные и сопоставимые результаты в случае повторения;

c) определении элементов управления на основе оценки рисков информационной безопасности и процессов обработки рисков;

d) результатах деятельности информационной безопасности и результативности СМИБ, оценивая их по отношению к целям информационной безопасности;

e) соответствии между определенными элементами управления, Заявлением о применимости, результатами оценки рисков информационной безопасности, процессом обработки рисков, а также политикой и целями информационной безопасности;

f) внедрении средств управления (см. Приложение E для примеров средств управления аудитом) с учетом внешнего и внутреннего контекста и связанных рисков, а также мониторинга, измерения и анализа организацией процессов и средств управления информационной безопасности, чтобы определить, действительно ли средства управления, заявленные как реализуемые, реализованы и эффективны в целом;

g) программах, процессах, процедурах, записях, внутренних аудитах и анализах результативности СМИБ для обеспечения их прослеживаемости до решений высшего руководства, а также политики и целей информационной безопасности.

9.4 Проведение аудитов

9.4.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.4. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.4.2 и 9.4.3.

9.4.2 Конкретные элементы аудита СМИБ

Аудиторская группа органа по сертификации должна:

a) потребовать от заказчика продемонстрировать, что оценка рисков, связанных с информационной безопасностью, является

актуальной и адекватной для функционирования СМИБ в рамках ее области действия;

b) установить, соответствуют ли процедуры заказчика по выявлению, изучению и оценке рисков, связанных с информационной безопасностью и результатам их реализации с политикой, целями и задачами заказчика.

Орган по сертификации также должен установить, являются ли процедуры, используемые при оценке рисков, надежными и надлежащим образом реализованными.

9.4.3 Отчет об аудите

9.4.3.1 В отчете об аудите должна быть указана следующая информация или ссылки на нее:

a) отчет об аудите анализа рисков информационной безопасности заказчика;

b) любые наборы средств управления информационной безопасности, используемые организацией для целей сравнения, как того требует ИСО/МЭК 27001:2022, 6.1.3 c).

9.4.3.2 Отчет об аудите должен быть достаточно подробным, чтобы облегчить и поддержать решение о сертификации. Он должен содержать:

a) важные журналы по аудиту и применяемые методологии аудита (см. 9.1.1.2);

b) ссылку на версию Заявления о применимости и, где применимо, любое полезное сравнение с результатами предыдущих сертификационных аудитов заказчика.

Заполненные анкеты, контрольные списки, наблюдения, журналы или записи аудитора могут составлять неотъемлемую часть отчета об аудите. Если используются данные методы, то такие документы должны быть представлены в орган по сертификации в качестве доказательств для поддержки в решении о сертификации. Информация

о выборках, оцененных во время аудита, должна быть включена в отчет об аудите или в другую документацию по сертификации.

Если использовались методы дистанционного аудита, в отчете должна быть указана степень, в которой они использовались при проведении аудита, и их результативность в достижении целей аудита.

Если деятельность организации не осуществляется в определенном физическом месте и, следовательно, вся деятельность организации осуществляется удаленно, в отчете об аудите должно быть указано, что вся деятельность организации осуществляется удаленно.

В отчете должна быть рассмотрена адекватность внутренней организации и процедур, принятых заказчиком для обеспечения доверия к СМИБ.

В отчет должно быть включено краткое изложение наиболее важных наблюдений, как положительных, так и отрицательных, относительно внедрения и результативности требований СМИБ и средств управления информационной безопасности.

9.5 Решение о сертификации

9.5.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.5. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.5.2.

9.5.2 Решение о сертификации

Решение о сертификации должно быть основано на рекомендациях аудиторской группы по сертификации, изложенных в отчете по сертификационному аудиту.

Сертификат не должен выдаваться заказчику до тех пор, пока не будет предоставлено достаточно доказательств, подтверждающих,

что меры по проведению анализов со стороны руководства и внутренних аудитов СМИБ были реализованы, эффективны и будут подтверждаться.

9.6 Подтверждение сертификации

9.6.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.6.1.

9.6.2 Деятельность по инспекционному контролю

9.6.2.1 Должны применяться требования ИСО/МЭК 17021-1:2015, 9.6.2. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.6.2.2, 9.6.2.3 и 9.6.2.4.

9.6.2.2 Процедуры инспекционного аудита должны быть частью процедур сертификационного аудита СМИБ заказчика, как описано в настоящем документе.

Цель инспекционного контроля состоит в том, что утвержденная СМИБ продолжает внедряться, учитываются последствия изменения в СМИБ, организованные по результатам изменений в операционной практике заказчика, а также для постоянного подтверждения соответствия требованиям сертификации. Программы инспекционного аудита должны, как минимум, охватывать:

a) элементы обеспечения СМИБ, такие как оценка рисков информационной безопасности и управление обеспечением, внутренние аудиты СМИБ, анализ со стороны руководства и корректирующие действия;

b) информация, поступающая от сторонних организаций, согласно требованиям ИСО/МЭК 27001 и других документов, необходимых для сертификации;

9.6.2.3 При проведении каждого инспекционного аудита со стороны органа по сертификации должно быть проанализировано, как минимум, следующее:

a) результативность СМИБ в отношении достижения целей политики информационной безопасности заказчика;

b) функционирование процедур периодической оценки и анализа на соблюдение соответствующих законодательства и регламентов в области информационной безопасности;

c) определенные изменения в средствах управления и соответствующие изменения в SoA;

d) внедрение и результативность средств управления, указанных в программе аудита.

9.6.2.4 Орган по сертификации должен быть способен адаптировать свою программу деятельности по инспекционному контролю для соответствия с вопросами информационной безопасности, связанными с рисками и воздействиями на заказчика, и обосновать эту программу.

Инспекционный аудит может быть совмещен с аудитами других систем менеджмента. Отчеты об аудитах должны четко указывать аспекты, относящиеся к каждой системе менеджмента.

В ходе инспекционного аудита органы по сертификации должны проверять записи по апелляциям и жалобам, направленные в орган по сертификации. В случае выявления любого несоответствия или несоблюдения требованиям сертификации, органы по сертификации должны проверять, что заказчик расследовал свои СМИБ и процедуры и предпринял соответствующие корректирующие действия.

Отчет по инспекционной деятельности должен также содержать информацию об устранении выявленных ранее несоответствий, версию SoA, а также важные изменения, произошедшие после предыдущего аудита. Отчеты, полученные в результате инспекционной деятельности, должны быть составлены так, как минимум, чтобы охватить все требования, изложенные в 9.6.2.2 и 9.6.2.3.

9.6.3 Ресертификация

9.6.3.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.6.3. Дополнительно, должны применяться требования и руководящие указания, изложенные в 9.6.3.2.

9.6.3.2 Ресертификационный аудит

Процедуры ресертификационных аудитов должны соответствовать процедурам, касающимся первоначального сертификационного аудита СМИБ заказчика, как описано в настоящем документе.

Время, отведенное для выполнения корректирующих действий, должно соответствовать степени серьезности несоответствия и связанного с ним риска информационной безопасности.

9.6.4 Специальные аудиты

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.6.4.

9.6.5 Приостановка, отзыв или сокращение области сертификации

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.6.5.

9.7 Апелляции

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.7.

9.8 Жалобы

9.8.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.8.

9.8.2 Жалобы

Жалобы представляют собой потенциальный инцидент и указывают на возможное несоответствие.

9.9 Записи о заказчиках

Должны применяться требования ИСО/МЭК 17021-1:2015, 9.9.

10 Требования к системе менеджмента для органов по сертификации

10.1 Варианты

10.1.1 Общие положения

Должны применяться требования ИСО/МЭК 17021-1:2015, 10.1. Дополнительно, должны применяться требования и руководящие указания, изложенные в 10.1.2.

10.1.2 Внедрение СМИБ

Рекомендуется, чтобы органы по сертификации внедряли СМИБ в соответствии с ИСО/МЭК 27001.

10.2 Вариант А: Общие требования к системе менеджмента

Должны применяться требования ИСО/МЭК 17021-1:2015, 10.2.

10.3 Вариант В: Требования к системе менеджмента согласно ИСО 9001

Должны применяться требования ИСО/МЭК 17021-1:2015, 10.3.

Приложение А
(обязательное)
Знания и навыки, необходимые для аудита и сертификации СМИБ

А.1 Обзор

Таблица А.1 определяет знания и навыки, которые орган по сертификации должен определить для конкретных функций сертификации, в дополнение к требованиям ИСО/МЭК 17021-1. «X» указывает, что орган по сертификации должен определить критерии и глубину знаний и навыков. Требования к знаниям и навыкам, указанные в Таблице А.1, более подробно поясняются в Разделе 7 и дается перекрестная ссылка в скобках в Таблице А.1.

Таблица А.1 – Таблица знаний и навыков, необходимых для аудита и сертификации СМИБ

	Функции в области сертификации		
Знания и навыки	Проведение анализа заявки для определения требуемой компетентности аудиторской группы, отбора членов аудиторской группы и определение продолжительности аудита	Проведение анализа отчетов об аудите и принятие решений о сертификации	Проведение аудита и руководство аудиторской группой
Терминология, принципы, практические методики и средства менеджмента информационной безопасности		X (см. 7.1.3.3.2)	X (см. 7.1.3.1.2)
Стандарты и нормативные документы системы менеджмента информационной безопасности			X (см. 7.1.3.1.3)
Практики менеджмента бизнеса			X (см. 7.1.3.1.4)
Сектор бизнеса заказчика	X (см. 7.1.3.2.1)	X (см. 7.1.3.3.3)	X (см. 7.1.3.1.5)
Продукция, процессы и организация заказчика	X (см. 7.1.3.2.2)	X (см. 7.1.3.3.4)	X (см. 7.1.3.1.6)

Примечание – Дополнительные аспекты компетентности содержатся в Приложении В.

Приложение В
(справочное)
Дополнительные аспекты компетентности

В.1 Общие аспекты компетентности

Существует несколько способов, которыми аудитор может продемонстрировать свои знания и опыт. Знания и опыт могут быть оценены, например, при помощи использования общепризнанных квалификаций. Регистрационные записи в рамках схемы сертификации персонала могут также использоваться для оценки необходимых знаний и опыта. Требуемый уровень компетенций для аудиторской группы следует установить с учетом сложности структуры СМИБ, а также отраслевой и технологической сферы деятельности организации.

В.2 Конкретные аспекты знаний и опыта

В.2.1 Стандартные знания, связанные со СМИБ

В дополнение к требованиям, изложенным в 7.1.3, следует учитывать следующее. Аудиторам следует знать и понимать следующие процедуры аудита и объектов СМИБ:

– составление и планирование программы аудита;
– тип и методология аудита;
– риски, связанные с аудитом;
– анализ процессов информационной безопасности;
– непрерывное совершенствование;
– внутренний аудит информационной безопасности.

Аудиторам следует знать и понимать следующие нормативные требования:

– интеллектуальная собственность;
– содержание, защита и хранение записей организации;
– защита данных и конфиденциальность;
– регулирование средств криптографической защиты информации;
– электронная коммерция;
– электронные и цифровые подписи;
– надзор за рабочими местами;
– перехват в телекоммуникациях и мониторинг данных (например, электронная почта);

– использование компьютеров в преступных целях;

– сбор электронных доказательств;

– тестирование на проникновение;

– международные и национальные отраслевые требования (например, банковское дело).

Возможно, что для конкретной отрасли знания и понимание установлены в конкретном стандарте (например, ИСО/МЭК 27006-2).

Приложение С
(обязательное)
Продолжительность аудита

С.1 Общие положения

В этом приложении содержатся дополнительные требования, связанные с ИСО/МЭК 17021-1:2015, 9.1.4. В нем содержатся минимальные требования и руководящие указания для органа по сертификации по разработке собственных процедур для определения количества времени, необходимого для сертификации областей действия СМИБ различных размеров и сложности по широкому спектру видов деятельности.

Органы по сертификации должны предоставлять аудиторам достаточно времени для выполнения всех видов деятельности, связанных с первоначальным аудитом, инспекционным контролем или ресертификационным аудитом. Расчет общей продолжительности аудита должен включать достаточное время для составления отчетов об аудите.

Органы по сертификации должны определять продолжительность аудита, которое будет затрачено на первоначальную сертификацию, инспекционный контроль и ресертификацию для каждого заказчика и сертифицированной СМИБ. Использование этого приложения на этапе планирования аудита приводит к последовательному подходу к определению соответствующей продолжительности аудита. Кроме того, продолжительность аудита может быть скорректирована на основе того, что обнаружено в ходе аудита, особенно на 1 этапе (например, различная оценка сложности области действия СМИБ или дополнительные площадки в области действия).

В этом приложении представлены:

– концепции, используемые для расчета продолжительности аудита (С.2);

– требования к процедурам определения продолжительности аудита для различных этапов первоначального аудита (С.3);

– требования к продолжительности аудита для инспекционного (С.4) и ресертификационного аудита (С.5);

– требования, связанные с аудитами на нескольких местах осуществления деятельности (С.6);

– требования к продолжительности аудита при расширении области действия (С.7).

Примеры расчета продолжительности аудита для иллюстрации применения этого приложения можно найти в Приложении D.

Основное предположение подхода в этом приложении заключается в том, что в схеме расчета для определения продолжительности аудита следует:

a) учитывать только атрибуты, которые могут быть оценены объективно;

b) быть достаточно простой для применения органами по сертификации и достижения ими достоверных, сопоставимых и воспроизводимых результатов;

c) быть достаточно сложной, чтобы гарантировать, что изменения в значениях атрибутов приводят к сопоставимым изменениям в конечной продолжительности аудита.

Определение продолжительности аудита основано на числах, приведенных в Таблице С.1, и должно учитывать факторы, способствующие модификации.

Подход к определению продолжительности аудита, определенный органом по сертификации, должен регулярно пересматриваться на предмет его достаточности с учетом сложности СМИБ.

С.2 Концепции

С.2.1 Численность персонала, выполняющего работу под управлением организации

Общая численность лиц, выполняющих работу под управлением организации для всех смен в рамках области сертификации, является отправной точкой для определения продолжительности аудита.

Примечание – Лица, выполняющие работу под управлением организации, включают весь персонал (независимо от того, являются ли они членами организации или нет) в рамках области сертификации, который должен работать в соответствии с требованиями СМИБ.

Лица, работающие неполное рабочее время и работающие под управлением организации, вносят вклад в численность лиц, выполняющих работу под управлением организации, пропорционально количеству отработанных часов по сравнению с лицом, работающим полное рабочее время и работающим под управлением организации. Это определение должно зависеть от количества отработанных часов по сравнению с сотрудником, работающим полное рабочее время.

Когда высокий процент лиц, выполняющих работу под управлением организации в рамках области сертификации, выполняют определенные идентичные действия, допускается сокращение численности лиц до использования Таблицы С.1 для расчета продолжительности аудита. Органы по сертификации должны

использовать факторы, приведенные в С.3.4, и учитывать влияние деятельности на риск информационной безопасности, чтобы определить, как применяется сокращение численности лиц в рамках области сертификации. Должны быть задокументированы согласованные и последовательные процедуры, которые можно повторять и применять между компаниями.

С.2.2 Аудито-день

Общая продолжительность аудита, указанная в Таблице С.1, означает аудито-дни, затраченные на проведение аудита. Данное приложение основывается на расчете восьмичасового рабочего дня (сокращение “д”).

С.2.3 Временная площадка

Временная площадка, подпадающая под область сертификации – это место, не входящее в число площадок, указанных в документах о сертификации, где деятельность в рамках области сертификации, осуществляется в течение определенного периода времени. Такие площадки могут варьироваться от основных площадок проектного управления до малых обслуживающих/установочных площадок. Необходимость посещения таких площадок, а также объем выборки, следует определять на основании оценки рисков деятельности, проведенной на данной временной площадке для достижения целей информационной безопасности. Выборка таких отобранных площадок, следует представлять как диапазон потребности организации в компетентности и вариантах обслуживания, с учетом размера и видов деятельности, а также различных этапов реализации проектов. Общий данные по выборке см. в 9.1.5.2.

С.3 Процедура определения продолжительности аудита при первоначальном аудите

С.3.1 Общие положения

Орган по сертификации должен иметь и соблюдать документированную процедуру расчета продолжительности аудита.

С.3.2 Дистанционные методы проведения аудита

Если для взаимодействия с организацией используются методы дистанционного аудита, такие как интерактивное веб-сотрудничество, веб-конференции, телеконференции и/или электронная проверка процессов организации, эти действия следует определять в плане аудита (см. 9.2.3) и могут рассматриваться как частично вносящие вклад в общую «продолжительность аудита на месте».

Примечание – Продолжительность аудита на месте относится к продолжительности аудита на месте, выделенном для отдельных площадок. Электронные аудиты удаленных площадок считаются дистанционными аудитами, даже если электронные аудиты физически проводятся на территории организации.

С.3.3 Расчет продолжительности аудита

График продолжительности аудита, приведенный в Таблице С.1 устанавливает начальную точку для среднего количества дней первоначального аудита [в этом приложении и Приложении D это число охватывает дни для первоначального аудита (Этап 1 и Этап 2)], что, как показал опыт, является подходящим для области действия СМИБ с заданной численностью лиц, выполняющих работу под управлением организации. Опыт также показал, что для областей действия СМИБ схожего размера некоторым требуется больше времени, чем другим.

График продолжительности аудита ниже предоставляет основу, которая должна использоваться для планирования аудита. Начальная точка основана на общей численности лиц, выполняющих работу под управлением организации для всех смен. Количество аудито-дней корректируется на основе значимых факторов, применяемых к области действия СМИБ, подлежащей аудиту, с присвоением дополнительного или вычитающего веса для каждого фактора для изменения базовой цифры. График продолжительности аудита в Таблице С.1 должен использоваться с учетом способствующих факторов и ограничений допустимого отклонения (см. С.3.5 и С.3.6). Термины, используемые в Таблице С.1, поясняются в С.2. В Приложении D приведены примеры того, как может применяться метод расчета настоящего приложения.

С.3.4 Определение начальной численности персонала

Органы по сертификации должны запрашивать у заказчика информацию, касающуюся большой численности лиц, выполняющих определенные идентичные действия, включая:

– численность лиц, вовлеченных в действие;

– тип действия или процесса.

Примеры факторов, которые могут сократить численность лиц, используемых в качестве основы для расчета, которые выполняют определенные идентичные действия, включают:

– лица, имеющие доступ только для чтения к информации для выполнения своих обязанностей;

– лица, не имеющие доступа к средствам обработки информации организации в рамках СМИБ;

– лица, имеющие конкретный доказуемый ограниченный доступ к средствам обработки информации компании в рамках СМИБ;

– лица, которые выполняют действия, где реализованы строгие запреты для ограничения раскрытия информации, например, меры, запрещающие пронос личных вещей и устройств в рабочую зону.

Сокращение численности лиц, выполняющих идентичные действия, должно быть сделано на основе риска действий, связанных с задачами. Квадратный корень из общей численности людей, выполняющих каждое идентичное действие, может использоваться для определения эффективной численности лиц, которая используется для расчетов продолжительности аудита, округленного до следующего полного числа. Это число должно быть максимальным допустимым сокращением численности персонала.

Характер задач, требования законодательства и важность информации, к которой лица имеют доступ, могут ограничивать сокращение.

Численность лиц, определенных после этой процедуры, является начальной точкой в Таблице С.1.

Примечание – Таблица структурирована идентично IAF MD 5.[9]

Таблица С.1 – График продолжительности аудита

Численность персонала, выполняющих работу под управлением организации	Общая продолжительность аудита для первоначального аудита системы менеджмента качества (аудито-дни, д)	Общая продолжительность аудита для первоначального аудита системы экологического менеджмента (аудито-дни, д)	Общая продолжительность аудита для первоначального аудита СМИБ (аудито-дни, д)	Дополнительные или вычитающие факторы	Общая продолжительность аудита
1–10	1,5–2	2,5–3	5	См. С.3.5	
11–15	2,5	3,5	6	См. С.3.5	
16–25	3	4,5	7	См. С.3.5	
26–45	4	5,5	8,5	См. С.3.5	
46–65	5	6	10	См. С.3.5	
66–85	6	7	11	См. С.3.5	
86–125	7	8	12	См. С.3.5	
126–175	8	9	13	См. С.3.5	
176–275	9	10	14	См. С.3.5	
276–425	10	11	15	См. С.3.5	
426–625	11	12	16,5	См. С.3.5	
626–875	12	13	17,5	См. С.3.5	
876–1 175	13	15	18,5	См. С.3.5	
1 176–1 550	14	16	19,5	См. С.3.5	
1 551–2 025	15	17	21	См. С.3.5	
2 026–2 675	16	18	22	См. С.3.5	
2 676–3 450	17	19	23	См. С.3.5	
3 451–4 350	18	20	24	См. С.3.5	
4 351–5 450	19	21	25	См. С.3.5	

Продолжение таблицы С.1

5 451–6 800	20	23	26	См. С.3.5	
6 801–8 500	21	25	27	См. С.3.5	
8 501–10 700	22	27	28	См. С.3.5	
> 10 700	Следуйте вышеуказанной прогрессии	Следуйте вышеуказанной прогрессии	Следуйте вышеуказанной прогрессии	См. С.3.5	

С.3.5 Факторы для корректировки продолжительности аудита

Таблица С.1 не должна использоваться изолированно. При распределении времени необходимо учитывать следующие факторы, связанные со сложностью структуры СМИБ, и, соответственно, требующие усилий при проведении аудита СМИБ:

a) сложность структуры СМИБ (например, критичность информации, риски, связанные со СМИБ и др.);

b) вид(ы) деловой активности, осуществляемой в рамках СМИБ;

c) ранее продемонстрированная результативность СМИБ;

d) объем и разнообразие технологий, применяемых при реализации различных компонентов СМИБ (например, количество различных ИТ-платформ, количество раздельных сетей);

e) масштаб привлечения аутсорсинга и сторонних соглашений в рамках области действия СМИБ;

f) степень развития информационной системы;

g) количество площадок и количество узлов аварийного восстановления (DR);

h) после первого этапа орган по сертификации рассмотрит количество и сложность управления;

i) для инспекционного контроля и ресертификационного аудита: объем и степень изменений, касающиеся СМИБ в соответствии с ИСО/МЭК 17021-1:2015, 8.5.3.

В Приложении D приведены примеры того, как эти различные факторы могут быть учтены при расчете продолжительности аудита.

Примерами факторов, требующих увеличения продолжительности аудита, являются:

– сложные логистические процессы, включающее в себя более одного здания или помещения в области действия СМИБ;

– персонал, говорящий больше чем на одном языке (требующий переводчика(ов) и(или) не дающий отдельным аудиторам возможность работать самостоятельно) или документация, представленная более чем на одном языке;

– виды деятельности, требующие посещения временных площадок с целью подтвердить деятельность постоянной(ых) площадки(ок), система менеджмента которого(ых) подлежит сертификации (см. перечисления нижеследующего списка);

– большое количество стандартов и регламентов, применимых к СМИБ.

Примерами факторов, позволяющих уменьшить продолжительность аудита, являются:

– процессы без или с низкой степенью риска;

– процессы, включающие один общий вид деятельности (например, только оказание услуг);

– предварительное знание организации (например, если организация уже сертифицировалась по другому стандарту тем же органом по сертификации);

– высокая степень готовности заказчика к сертификации (например, уже проходила сертификацию или признана по схеме третьей стороны);

– высокая степень зрелости действующей системы менеджмента.

В ситуации, когда заказчик или сертифицированная организация предоставляют свою продукцию или услуги на временных площадках, важно, чтобы оценки таких площадок включались в сертификационный аудит и программы инспекционного контроля.

В перечисленные выше факторы могут быть внесены корректировки. Факторы, требующие дополнения или вычитания продолжительности аудита, могут компенсировать друг друга. Во всех случаях, когда осуществляется корректировка времени, предусмотренному аудитом в Таблице С.1, должны быть предоставлены достаточные доказательства и записи, подтверждающие изменение.

С.3.6 Ограничения по отклонениям от продолжительности аудита

В целях обеспечения эффективности проводимого аудита, а также надежности и сопоставимых результатов, продолжительность аудита, предусмотренная в графике продолжительности аудита, не должна быть сокращена более, чем на 30 %.

Соответствующие причины отклонения должны быть установлены и задокументированы.

С.3.7 Продолжительность аудита на месте

Ожидается, что время, рассчитанное на планирование и написание отчета, в совокупности не следует, как правило, сокращать общую продолжительность аудита на месте (физическую/дистанционную) до менее чем 70 % от времени, рассчитанного в соответствии с С.3.3, С.3.4 и С.3.5. Если для планирования и/или написания отчета

требуется дополнительное время, это не должно быть оправданием для сокращения продолжительности аудита на месте. Время на поездку аудитора не включено в этот расчет и является дополнительным к продолжительности аудита, указанному в графике.

Примечание 1 – 70 % — это коэффициент, основанный на опыте аудитов СМИБ.

Примечание 2 – Термин «(физический/дистанционный)» означает, что аудиты «на месте» (для физических местоположений или электронных сайтов заказчика) могут проводиться физически или дистанционно (см. 9.2.3 и С.3.2). Для аудитов «на месте» см. также ИСО/МЭК 17021-1:2015, 9.4.1.

С.4 Продолжительность аудита при инспекционном аудите

Для цикла первоначального сертификационного аудита продолжительность инспекционного контроля в отношении данной организации следует рассчитывать пропорционально времени, затраченному на проведение первоначального аудита, к общему количеству времени, затрачиваемому в год на инспекционный контроль, что составляет примерно 1/3 от времени, затрачиваемого на проведение первоначального аудита. Плановую продолжительность инспекционного контроля следует периодически пересматривать для учета изменений, которые могут повлиять на продолжительность аудита. Время, затраченное на инспекционный аудит, должен быть увеличен с целью разрешения проведения аудита изменений в СМИБ (такие как аудит новых или измененных средств управления, процессов и услуг информационной безопасности).

С.5 Продолжительность аудита при ресертификационном аудите

Общее количество времени, затраченное на проведение ресертификационного аудита, должно зависеть от результатов любого предыдущего аудита, как указано в 9.4.3 и ИСО/МЭК 17021-1:2015, 9.6.3. Продолжительность аудита для проведения ресертификационного аудита следует составлять пропорционально, но не менее чем на две трети продолжительности аудита, требуемой на проведение первоначального сертификационного аудита для похожей организации на момент проведения ресертификационного аудита.

С.6 Продолжительность аудита на нескольких местах осуществления деятельности

Как правило, общая продолжительность аудита для аудита на месте должна рассчитываться с учетом общей численности лиц, выполняющих работу под управлением организации, независимо от их местонахождения.

В качестве альтернативы, по обоснованным причинам, которые должны быть задокументированы, разрешается суммировать продолжительность аудита, которая рассчитывается индивидуально для каждой площадки, при условии, что это общая продолжительность аудита больше, чем это определено в соответствии с первым абзацем настоящего пункта. Сокращения могут применяться для рассмотрения частей аудита, которые не имеют отношения к центральному офису или местным площадкам (если применимо). Причины обоснования таких сокращений должны быть зарегистрированы органом по сертификации.

Количество общих аудито-дней на месте, рассчитанное для области в соответствии с процедурой, указанной в С.3.3 и С.3.4 и настоящем пункте, должно быть распределено по всем различным площадкам на основе значимости площадки для системы менеджмента, деятельности, проводимой на площадке, и выявленных рисков. Обоснование распределения должно быть зарегистрировано органом по сертификации.

Любые сокращения должны применяться до сравнения продолжительности аудита с общей продолжительностью аудита.

С.7 Продолжительность аудита при расширении области действия

Продолжительность аудита, требуемое для расширения области действия СМИБ, должно рассчитываться с учетом таких факторов, как:

a) тип расширения:

b) деятельность по текущей сертификации;

c) количество мест, где осуществляется деятельность;

d) связанные с деятельностью соответствующие риски информационной безопасности;

e) количество средств управления, относящихся к расширению;

f) численность лиц, выполняющих работу под управлением организации в новой области действия; и

g) время, требуемое для анализа внедрения расширенной области действия в СМИБ.

Органы по сертификации должны иметь процедуры, которые обеспечивают последовательный подход к расширению области действия.

Для первоначального аудита новой области действия время должно рассчитываться на основе численности лиц и площадок, добавляемых к уже существующей области действия с использованием С.3.3, С.3.4 и С.3.5.

Продолжительность аудита должна быть добавлена к расчетной продолжительности анализа СМИБ заказчика. Это дополнительное время должно быть не менее:

1) 0,5 д (аудито-дней), если аудит расширения области действия проводится совместно с инспекционным аудитом или ресертификационным аудитом.

2) 1,0 д (аудито-дней), если аудит при расширении области действия проводится как отдельный аудит.

Приложение D

(справочное)

Методы расчета продолжительности аудита

D.1 Общие положения

В этом приложении приводятся дополнительные руководящие указания по разработке формулы для расчета продолжительности аудита. D.2 приводит пример классификации факторов, которые могут быть использованы в качестве основы для расчета продолжительности аудита, а D.3 приводит пример расчета продолжительности аудита.

Примечание – Концепции в этом приложении начинаются после того, как были применены любые сокращения лиц, выполняющих определенные идентичные действия, как описано в С.3.4.

D.2 Классификация факторов для расчета продолжительности аудита

В Таблице D.1 приведены примеры классификации основных факторов расчета продолжительности аудита, перечисленных в С.3.5, a) - i). Данная классификация может использоваться органами по сертификации для выведения схемы расчета продолжительности аудита в соответствии с 9.1.4.2.

Таблица D.1 – Классификация факторов для расчета продолжительности аудита

	Влияние усилия		
	сокращение усилия	нормальное усилие	увеличение усилия
Факторы (см. С.3.5)			
a) сложность структуры СМИБ: – требования информационной безопасности [конфиденциальность, целостность и доступность (КЦД)]; – количество критических активов; – количество процессов и услуг	– Только незначительная секретная или конфиденциальная информация, низкие требования по доступности. – Мало критических активов. (с точки зрения КЦД) – Один ключевой бизнес-процесс с несколькими связями и несколькими участвующими структурными единицами	– Высокие требования по доступности или некоторая секретная/ конфиденциальная информация. – Несколько критических активов. – 2–3 простых бизнес-процесса с несколькими связями и несколькими участвующими структурными единицами	– Большое количество секретной или конфиденциальной информации (например, данные: медицинские, персональные, о страховании, банковские) или высокие требования по доступности. – Много критических активов – Более двух сложных процессов с большим количеством связей и участвующих структурных единиц
b) вид(ы) деловой активности, осуществляемой в рамках СМИБ	– Низкий риск бизнеса без нормативных требований	– Высокие нормативные требования	– Высокий риск бизнеса с (только) ограниченными нормативными требованиями

Продолжение таблицы D.1

	Влияние усилия		
	сокращение усилия	нормальное усилие	увеличение усилия
c) ранее продемонстрированная результативность СМИБ	— Недавно сертифицирован — Не сертифицирован, но СМИБ полностью реализована посредством нескольких циклов аудита и доработки, включая документированные внутренние аудиты, анализы со стороны руководства и эффективную систему постоянного улучшения	— Недавний инспекционный аудит. — Не сертифицирован, но СМИБ частично реализована: доступны и реализованы некоторые инструменты системы менеджмента; действуют некоторые процессы постоянного улучшения, но они документированы частично	— Не сертифицирован, недавних аудитов нет — СМИБ новая и не полностью внедрена (например, отсутствуют конкретные механизмы управления системой менеджмента, неразвиты процессы постоянного улучшения, ситуативное исполнение процессов)
d) объем и разнообразие технологий при реализации различных компонентов СМИБ (например, количество различных ИТ-платформ, количество раздельных сетей);	— Высокостандартизированная среда с незначительным разнообразием (несколько ИТ-платформ, серверов, операционных систем, баз данных, сетей и др.)	— Стандартизированные, но разнообразные ИТ-платформы, серверы, операционные системы, базы данных, сети	— Большое разнообразие или сложность ИТ (например, множество различных сетевых сегментов, типов серверов или баз данных, несколько основных приложений)
e) масштаб привлечения аутсорсинга и сторонних соглашений в рамках области действия СМИБ	— Без аутсорсинга и с малой зависимостью от поставщиков, или — Четко определенные, управляемые и контролируемые договоренности по аутсорсингу. — Компания на аутсорсинге имеет сертифицированную СМИБ. — Доступны соответствующие независимые страховые отчеты	— Несколько частично регулируемых соглашений по аутсорсингу	— Большая зависимость от аутсорсинга или поставщиков, с большим влиянием на важные деловые активности, или — Неизвестный объем или уровень аутсорсинга, или — Несколько неконтролируемых соглашений по аутсорсингу
f) степень развития информационной системы	— Внутриорганизационная разработка системы отсутствуют. — Использование стандартизированных платформ программного обеспечения	— Использование стандартизированных платформ программного обеспечения со сложной конфигурацией/ параметрированием. — (высоко) кастомизированное программное обеспечение. — Некоторая деятельность по разработке (Внутриорганизационная или по аутсорсингу)	— Обширная внутренняя деятельность по разработке программного обеспечения по нескольким текущим проектам для важных бизнес-целей
g) количество площадок и количество узлов аварийного восстановления (DR)	— Низкие требования по доступности, а также отсутствует или существует один сайт DR	— Средние или высокие требования по доступности, а также отсутствует или существует один сайт DR	— Высокие требования по доступности, например, услуги в режиме 24/7. — Несколько сайтов DR — Несколько центров обработки данных

Продолжение таблицы D.1

	Влияние усилия		
	сокращение усилия	нормальное усилие	увеличение усилия
h) количество и сложность средств управления	— Меньшее, чем обычно, количество средств управления, при этом некоторые общие области управления не включены – например, отсутствуют средства управления разработкой систем или физические средства управления	— Типичное количество и сложность средств управления	— Большее, чем обычно, количество подробных и сложных средств управления, например, много средств управления, связанных с сетевыми протоколами или криптографией
i) для инспекционного или ресертификационного аудита: объем и степень изменений, касающиеся СМИБ в соответствии с ИСО/МЭК 17021-1:2015, 8.5.3	— Нет изменений после последнего ресертификационного аудита	— Незначительные изменения в области или SoA СМИБ, например, в некоторых политиках, документах — Незначительные изменения в вышеуказанных факторах	— Значительные изменения в области или SoA СМИБ, например, новые процессы, структурные единицы, направления, методологии менеджмента оценки рисков, политики, документация, обработки рисков. — Значительные изменения в вышеуказанных факторах

D.3 Пример расчета продолжительности аудита

Следующий пример иллюстрирует, как орган по сертификации может использовать факторы, указанные в С.3, для расчета продолжительности аудита. Расчет продолжительности аудита в примере ниже работает следующим образом:

Шаг 1: Определение факторов, связанных с бизнесом и организацией (кроме ИТ): Определить подходящий балл для каждой из категорий, приведенных в Таблице D.2, и просуммировать результаты.

Шаг 2: Определение факторов, связанных с ИТ-средой: Определить подходящий балл для каждой из категорий, приведенных в Таблице D.3, и просуммировать результаты.

Шаг 3: Основываясь на результатах шагов 1 и 2 выше, определить влияние факторов на продолжительность аудита, выбрав соответствующую запись в Таблице D.4.

Шаг 4: Окончательный расчет: Количество дней, определенное путем применения графика продолжительности аудита (Таблица С.1), умножается на коэффициент, полученный в результате Шага 3. При использовании выборки при наличии нескольких мест осуществления деятельности, рассчитанные аудито-дни увеличиваются на основе усилий, необходимых для выполнения плана выборки при наличии нескольких мест осуществления деятельности.

Этот результат является окончательным количеством аудито-дней.

Т а б л и ц а D.2 – Факторы, связанные с бизнесом и организацией (кроме ИТ)

Категория	Балл
Тип(ы) бизнеса и нормативных требований	1. Организация работает в некритических секторах бизнеса и в секторах без нормативного регулирования[a] 2. Организация имеет заказчиков в критических секторах бизнеса[a] 3. Организация работает в критических секторах бизнеса[a]
Процесс и задачи	1. Стандартные процессы со стандартными задачами; небольшое количество продукции или услуг 2. Стандартные, но не повторяющиеся процессы, с большим количеством продукции или услуг 3. Сложные процессы, большое количество видов продукции или услуг, большое количество структурных единиц, включенных в область сертификации (СМИБ охватывает очень сложные процессы или относительно большое количество или уникальных видов деятельности)
Уровень внедрения системы менеджмента	1. СМИБ уже внедрена и функционирует, и(или) действуют другие системы менеджмента 2. Некоторые элементы других систем менеджмента реализованы, некоторые – нет 3. Не реализованы никакие другие системы менеджмента вообще, СМИБ новая и не внедрена
[a] Критические сектора бизнеса – это сектора, которые могут повлиять на критические социальные услуги, и вызвать риск здоровья людей, безопасности, экономики, имиджа государства и способности правительства продолжать функционировать, что в свою очередь может оказать значительное неблагоприятное воздействие на государства.	

Т а б л и ц а D.3 – Факторы, связанные с ИТ-средой

Категория	Балл
Сложность структуры ИТ	1. Немногочисленные или высокостандартизированные ИТ-платформ, серверов, операционных систем, баз данных, сетей и др. 2. Несколько различных ИТ-платформ, серверов, операционных систем, баз данных, сетей 3. Много разных ИТ-платформ, серверов, операционных систем, баз данных, сетей
Зависимость от аутсорсинга и поставщиков, включая облачные сервисы	1. Незначительное или полное отсутствие зависимости от аутсорсинга или поставщиков 2. Некоторая зависимость от аутсорсинга или поставщиков, связанная с некоторыми, но не всеми важными деловыми активностями 3. Высокая зависимость от аутсорсинга или поставщиков, большое влияние на важные деловые активности
Разработка информационных систем	1. Отсутствие или очень ограниченная внутриорганизационная разработка системы/приложения 2. Некоторая внутриорганизационная или переданная на аутсорсинг разработка системы/приложения для некоторых важных целей бизнеса 3. Масштабная внутриорганизационная или переданная на аутсорсинг разработка системы/приложения для важных целей бизнеса

Т а б л и ц а D.4 – Влияние факторов на продолжительность аудита

		Сложность ИТ		
		Низкая (от 3 до 4)	Средняя (от 5 до 6)	Высокая (от 7 до 9)
Сложность структуры бизнеса	Высокая (от 7 до 9)	+5 % – +20 %	+10 % – +50 %	+20 % – +100 %
	Средняя (от 5 до 6)	−5 % – −10 %	0 %	+10 % – +50 %
	Низкая (от 3 до 4)	−10 % – −30 %	−5 % – −10 %	+5 % – +20 %

П р и м е р 1 – Организация, подлежащая аудиту, имеет 700 сотрудников, таким образом, согласно Таблице С.1, для первоначального аудита требуется 17,5 дней. Организация не работает в критическом секторе бизнеса, имеет высокостандартизированные и повторяющиеся задачи и недавно внедрила СМИБ. Согласно Таблице D.2, это даст фактор, связанный с бизнесом и организацией, 1 + 1 + 3 = 5. У организации очень мало ИТ-платформ и баз данных, но она широко использует аутсорсинг. Разработка программного обеспечения не осуществляется внутри организации или не передается на аутсорсинг. Согласно Таблице D.3, это даст фактор, связанный с ИТ-средой, 1 + 3 + 1 = 5. Используя Таблицу D.4, это не приведет ни к какой корректировке продолжительности аудита.

П р и м е р 2 – Используя ту же организацию, что и в Примере 1, за исключением того, что несколько систем менеджмента уже действуют и СМИБ уже хорошо внедрена, можно изменить расчет согласно Таблице D.2 на 1 + 1 + 1 = 3. Согласно Таблице D.4, это приведет к сокращению продолжительности аудита от 5 % до 10 %, т. е. продолжительность аудита сократится от 1 дня до 1,5 дней, что в общей сложности составит от 16 дней до 16,5 дня.

Приложение Е
(справочное)
Руководящие указания по анализу средств управления, внедренных в соответствии с Приложением А ИСО/МЭК 27001:2022

Е.1 Цель

Согласно требованию из 9.3.2.2 f), реализация средств управления, которые были определены как необходимые заказчиком для СМИБ (согласно Заявлению о применимости), должна быть проанализирована на 2 этапе первоначального аудита и во время инспекционного контроля или действий по ресертификации. Анализы предназначены для определения того, реализованы ли средства управления и эффективны ли они, а также соответствуют ли они заявленным целям информационной безопасности.

Обычно только после того, как аудитор посещает организацию, орган по сертификации узнает, какие средства управления необходимы организации, или, например, что они уже описаны с использованием того же текста средств управления, что и в ИСО/МЭК 27001:2022, Приложение А. Орган по сертификации также не знает взаимосвязи между средствами управления информационной безопасности или взаимосвязи между средствами управления информационной безопасности и процессами организации. Таким образом, первоначальный аудит может быть ограничен аудитом отдельных средств управления, тогда как последующие аудиты могут использовать более эффективный подход аудита средств управления в контексте процессов организации и планов обработки рисков, в которых они развернуты.

Тем не менее, органы по сертификации знают, что организации обязаны сравнивать свои необходимые средства управления с предусмотренными в ИСО/МЭК 27001:2022, Приложение А, и, следовательно, существует взаимосвязь между необходимыми средствами управления организации и предусмотренными в ИСО/МЭК 27001:2022, Приложение А. Руководящие указания, приведенные в Таблице Е.1, призваны помочь органу по сертификации в разработке планов аудита для учета необходимых средств управления, определенных заказчиком, с учетом их взаимосвязи с средствами управления из ИСО/МЭК 27001:2022, Приложение А.

Е.2 Как пользоваться Таблицей Е.1

Е.2.1 Общие положения

Таблица Е.1 содержит пример руководящих указаний по анализу необходимых средств управления. Она использует средства управления, перечисленные в ИСО/МЭК 27001:2022, Приложение А, но аудиторам следует использовать взаимосвязь между этими средствами управления и необходимыми средствами управления организации для интерпретации руководящих указаний, приведенных в Таблице Е.1, для сбора свидетельств аудита с целью демонстрации результативности средств управления.

Примечание – Таблица Е.1 не предназначена для предоставления руководящих указаний по анализу средств управления, не связанных с теми, которые указаны в ИСО/МЭК 27001:2022, Приложение А.

Большинство средств управления содержат организационные аспекты, которые могут быть подтверждены, например, путем анализа документации заказчика по средствам управления, процессам или процедурам, собеседованиям или наблюдениям.

Многие средства управления основаны на правилах, установленных организацией заказчика. Такие правила могут быть в форме политик по конкретному направлению, требований к процессам или процедурам или другим типам правил, которые доводятся до сведения персонала. Таблица Е.1 использует общий термин «правила» для обозначения таких требований или ожиданий, установленных руководством организации заказчика.

Многие средства управления можно протестировать методом выборки, т. е. путем анализа выборки результатов управленческой деятельности.

Е.2.2 Графа «Испытание системы»

Многие средства управления в ИСО/МЭК 27001:2022, Приложение А, реализованы как технологические средств управления, например, через конкретные системные настройки, конфигурации или функциональность технологии. Доказательства результатов деятельности технологических средств управления часто можно собрать с помощью испытания системы или с помощью специализированных инструментов аудита или отчетности. Испытание системы означает прямой анализ информационных систем: аудитор может проанализировать системные настройки и конфигурации или оценивать результаты инструментов тестирования. Если у заказчика есть используемые инструменты, которые известны

аудитору, они также могут использоваться для поддержки аудита, или аудитор может анализировать результаты оценки, выполненной заказчиком.

Графа «испытание системы» в Таблице Е.1 содержит руководящие указания по анализу технологических средств управления:

– «пусто» означает, что испытание системы обычно неприменимо или не является необходимым при аудите СМИБ;

– «возможно» означает, что испытание системы обычно возможно для оценки реализации средств управления, но может не быть необходимым при аудите СМИБ;

– «рекомендовано» означает, что испытание системы обычно необходимо при аудите СМИБ.

Е.2.3 Графа «Визуальный осмотр»

Другие средства управления в ИСО/МЭК 27001:2022, Приложение А, могут быть проанализированы посредством «визуального осмотра» на площадке для оценки их реализации и результативности. Полагаться на анализ соответствующей документации на бумажном носителе или на собеседовании недостаточно, поэтому аудитору следует рассмотреть возможность проверки средств управления на месте, где она реализована.

Примечание – Визуальный осмотр на площадке также может быть достигнут с использованием методов удаленного осмотра, например, при наличии лица на площадке с видео в режиме реального времени для аудитора.

Графа «визуальный осмотр» в Таблице Е.1 содержит руководящие указания по анализу физических доказательств средств управления:

– «пусто» означает, что визуальный осмотр обычно неприменим или не является необходимым при аудите СМИБ;

– «возможно» означает, что визуальный осмотр обычно возможен для оценки реализации средств управления, но может не быть необходимым при аудите СМИБ;

– «рекомендовано» означает, что визуальный осмотр обычно необходим при аудите СМИБ.

Е.2.4 Возможные доказательства разработки и реализации средств управления

В графе «возможные доказательства разработки и реализации средств управления» приводятся руководящие указания по доказательствам, которые могут помочь аудитору провести оценку соответствия по ИСО/МЭК 27001:2022, 8.3 (требование реализации плана обработки рисков и, следовательно, необходимых средств управления). Различные пункты списка в данной графе не являются

требованиями и не представляют собой исчерпывающий список. Поскольку они вытекают из текста средств управления ИСО/МЭК 27001:2022, Приложение А, они не обязательно подходят для соответствующих необходимых средств управления организации. В этом случае следует использовать другие формы доказательств. Заявление о применимости организации и связанную с ним документацию по СМИБ следует использовать в качестве технических условий необходимых средств управления организации. Заявление о применимости организации содержит необходимые средства управления, обоснование их включения, независимо от того, реализованы они или нет, и обоснование любых средств управления, исключенных из ИСО/МЭК 27001:2022, приложение А.

Т а б л и ц а Е.1 – Оценка средств управления

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
5 Средства организационного управления			
5.1 Политики информационной безопасности			— Политика информационной безопасности — Политики по конкретному направлению информационной безопасности, которые организация считает необходимыми — Распространение политик среди соответствующего персонала и заинтересованных сторон
5.2 Роли и обязанности по обеспечению информационной безопасности			— Распределенные ролей и обязанностей по внедрению, функционированию и управлению информационной безопасностью
5.3 Разделение обязанностей			— Выявленные конфликтующие обязанности или области ответственности и соответствующие правила разделения
5.4 Обязанности руководства			— Заявления руководства и поддержка целей, политик, процедур информационной безопасности и т. д. — Упоминание личной ответственности за информационную безопасность персонала
5.5 Взаимодействие с органами власти			— Определенные контактные лица с соответствующими органами власти — Правила отчетности по инцидентам — Содержание информационного потока от и к соответствующим органам власти
5.6 Контакты с профессиональными сообществами			— Членство и определенные контактные лица с профессиональными сообществами или другими форумами и ассоциациями [например, группы реагирования на компьютерные чрезвычайные ситуации (CERT), агентства по кибербезопасности] — Правила того, что может обсуждаться в таких организациях — Содержание информационного потока от и к таким организациям

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
5.7 Информация об угрозах			— Подход к сбору соответствующей информации об угрозах — Анализ информации об угрозах в отношении организации и ее распространение соответствующим сторонам
5.8 Информационная безопасность в управлении проектами			— Установленная информационная безопасность в управлении проектами на протяжении всего жизненного цикла проекта, например, в определении требований, испытаний — Для выборки проектов выявлены риски информационной безопасности и соответствующая обработка рисков
5.9 Инвентаризация информации и других связанных активов	возможно		— Инвентаризации информации и других связанных активов, поддерживаемые СМИБ — Поддерживаемое право собственности на активы при инвентаризации активов — Правила по обязанностям владельца активов, например, классификация
5.10 Допустимое использование информации и других связанных активов			— Документированные правила для допустимого использования информации и других связанных активов — Процедуры обработки информации и других связанных активов
5.11 Возврат активов			— Правила возврата активов организации, например, контрольные списки для изменения или прекращения трудоустройства, контракта или соглашения — Образец документированных записей о возврате
5.12 Классификация информации			— Правила и схема классификации информации, например, в политике по конкретному направлению — Образец информации из различных источников, который следует классифицировать
5.13 Маркировка информации		возможно	— Правила маркировки информации и других связанных активов — Процедуры маркировки конкретных типов информации и других связанных активов
5.14 Передача информации	возможно		— Правила передачи информации, например, в политике по конкретному направлению — Определение случаев использования передачи информации, определенных в СМИБ, и соответствующих правил, процедур или соглашений, охватывающих, например, физическую, электронную или устную передачу — Образцы реализованных процедур или соглашений о передаче информации
5.15 Управление доступом	возможно		— Правила управления физическим и логическим доступом к информации и другим связанным активам, например, в политике по конкретному направлению по управлению доступом — Выдержки (образцы) прав доступа для высокорискованного физического или логического доступа к информации и другим активам, проверенные на соответствие вышеуказанным правилам

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
5.16 Управление идентификацией			— Процедуры управления идентификаторами, назначенными лицам или нечеловеческим сущностям в течение жизненного цикла
5.17 Информация об аутентификации	рекомен-довано		— Описание процесса распределения и управления информацией об аутентификации — Инструкции для пользователей по правильному обращению с информацией, используемой для аутентификации — Если используются пароли, настройки безопасности (например, длина, сложность, регулярная смена) систем управления паролями
5.18 Права доступа	рекомен-довано		— Правила управления доступом, например, политике по конкретному направлению по управлению доступом (физической и логической) — Описание процесса назначения, обновления или отзыва прав доступа — Правила и процесс регулярного пересмотра прав доступа — Права доступа, назначенные выборке идентификаторов — Результаты выполненных пересмотров прав доступа
5.19 Информационная безопасность в отношениях с поставщиками			— Правила управления рисками информационной безопасности в отношениях с поставщиками, например, в политике по конкретному направлению использования продуктов и услуг поставщика — Процессы или процедуры управления информационной безопасностью в отношениях с поставщиками на протяжении всего жизненного цикла отношений — Результаты оценок поставщиков [например, компоненты инфраструктуры информационно-коммуникационных технологий (ИКТ), услуги] — Результаты мониторинга соответствия установленным требованиям информационной безопасности (например, для выборки отношений с поставщиками)
5.20 Обеспечение информационной безопасности в соглашениях с поставщиками			— Реестр соглашений с внешними сторонами, связанных с типом отношений с поставщиками — Соглашения с поставщиками (выборка) с соответствующими требованиями информационной безопасности и Соглашениями об Уровне Обслуживания
5.21 Управление информационной безопасностью в цепочке поставок информационно-коммуникационных технологий (ИКТ)			— Правила обработки информационной безопасности при приобретении продуктов или услуг ИКТ — Практики управления рисками информационной безопасности цепочки поставок ИКТ — Результаты выполненного анализа рисков, т. е. уменьшение средств управления для выборки конкретных цепочек поставок ИКТ

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
5.22 Мониторинг, анализ и управление изменениями в услугах поставщиков			— Процессы управления изменениями в практиках и предоставлении услуг информационной безопасности поставщиков — Планы регулярного мониторинга, анализа, оценки практик информационной безопасности поставщиков (например, посредством отчетов об услугах, аудитов поставщиков) — Результаты мониторинга и анализ деятельности, включая планы действий
5.23 Информационная безопасность при использовании облачных сервисов			— Правила управления рисками информационной безопасности в облачных сервисах, например, в политике по конкретному направлению по использованию облачных сервисов — Список облачных сервисов, используемых организацией — Процессы управления рисками информационной безопасности, связанными с использованием облачных сервисов — Конкретные положения по защите данных организации и доступности сервисов, если соглашения об облачных сервисах не охватывают требования организации к конфиденциальности, целостности, доступности и обработке информации
5.24 Планирование и подготовка управления инцидентами информационной безопасности			— Процессы, план, роли и обязанности по обработке инцидентов информационной безопасности — Процедуры отчетности о событиях информационной безопасности и примеры таких отчетов
5.25 Оценка и принятие решений по событиям информационной безопасности			— Критерии оценки событий информационной безопасности — Схема категоризации и приоритизации инцидентов информационной безопасности
5.26 Реагирование на инциденты информационной безопасности			— Процедуры реагирования на инциденты информационной безопасности — Записи инцидентов и соответствующих мер реагирования на инциденты
5.27 Извлечение уроков из инцидентов информационной безопасности			— Записи произошедших инцидентов информационной безопасности, включая типы, масштабы и понесенные затраты — Уроки, извлеченные из анализа инцидентов информационной безопасности, например, усовершенствования плана управления инцидентами, улучшение средствами управления и действий по повышению осведомленности
5.28 Сбор доказательств			— Процедуры работы с доказательствами, связанными с инцидентами информационной безопасности, например, для идентификации, сбора, приобретения и сохранения

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
5.29 Информационная безопасность во время сбоев			— Планы по поддержанию надлежащих уровней информационной безопасности во время сбоев — Включение требований информационной безопасности в планирование и процесс управления непрерывностью бизнеса
5.30 Готовность ИКТ к обеспечению непрерывности бизнеса			— Требования к непрерывности ИКТ, полученные из анализа влияния на бизнес — Планы обеспечения непрерывности ИКТ — Результаты регулярных тестов непрерывности ИКТ
5.31 Юридические, законодательные, нормативные и контрактные требования			— Список соответствующих стран, в которых организация ведет бизнес или использует продукты и услуги, которые могут повлиять на информационную безопасность организации — Выявленные внешние требования, включая правовые, нормативные или контрактные требования, относящиеся к информационной безопасности, в частности, в отношении использования криптографии в любой форме
5.32 Права интеллектуальной собственности			— Правила управления правами интеллектуальной собственности, например, в политике по конкретному направлению — Процедуры обработки авторских прав на документы, прав на дизайн, товарных знаков, патентов и лицензий на исходный код и соответствующие материальные средства
5.33 Защита записей	рекомен-довано		— Правила управления записями, связанные с применимыми законами, регламентами и контрактными требованиями, например, в политике по конкретному направлению — Процедуры хранения, обработки цепочки поставок, сохранения и утилизации записей — Конфигурация систем хранения данных для обеспечения требований к управлению записями (например, сохранение, запоминание)
5.34 Конфиденциальность и защита персональной идентифицируемой информации (PII)			— Правила обработки персональной идентифицируемой информации (PII), например, в политике по конкретному направлению — Список соответствующих стран, в которых организация ведет бизнес или использует продукты и услуги, которые могут повлиять на конфиденциальность и защиту PII — Выявленные внешние требования, включая правовые, нормативные или контрактные требования по сохранению конфиденциальности и защите PII — Анализы, выполненные сторонами, ответственными за обработку PII, которые показывают, что требования выполняются с помощью соответствующих технических и организационных мер

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
5.35 Независимый анализ информационной безопасности			— Планы проведения независимых анализов информационной безопасности — Отчетность о результатах независимых анализов (выборка) перед высшим руководством — Корректирующие действия, предпринятые в случаях, когда подход организации к управлению информационной безопасностью был признан неадекватным
5.36 Соблюдение политик, правил и стандартов информационной безопасности			— Планы анализа соблюдения организацией политики информационной безопасности, политик по конкретным направлениям, правил и стандартов — Результаты таких анализов (выборка) и предпринятые корректирующие действия
5.37 Документированные рабочие процедуры			— Операционные процедуры для объектов обработки информации, соответствующие информационной безопасности
6 Средства управления персоналом			
6.1 Отбор			— Правила и процесс проверки биографических данных с учетом применимых законов, регламентов и этики — Проверка биографических данных, выполненная для выборки новых сотрудников и текущего персонала, если применимо (например, продвижения по службе, секретные профили работы)
6.2 Сроки и условия найма			— Общие правила или общие сроки и условия, связанные с обязанностями по обеспечению информационной безопасности, например, кодекс поведения — Принятие персоналом сроков и условий, касающихся информационной безопасности — Образец конкретных обязанностей по обеспечению информационной безопасности, согласованных персоналом с критически важными ролями (например, имеющим доступ к секретной информации или привилегированный доступ к системам)
6.3 Осведомленность, образование и обучение в области информационной безопасности			— Программа по осведомленности, образованию и обучению в области информационной безопасности, включая конкретное содержание для важных целевых групп — Список участников проведенных обучений по информационной безопасности — Меры реагирования на ожидаемое поведение относительно собеседований с выборкой участников
6.4 Дисциплинарный процесс			— Формальный дисциплинарный процесс, доведенный до сведения персонала и других соответствующих заинтересованных сторон

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
6.5 Обязанности после увольнения или смены работы			— Подписанное принятие персоналом конкретных обязанностей и ответственности, действительных после ухода из компании или после смены работы
6.6 Соглашения о конфиденциальности или неразглашении			— Подписанные персоналом соглашения о конфиденциальности и другими соответствующими заинтересованными сторонами
6.7 Дистанционная работа	возможно		— Правила дистанционной работы, например, в политике по конкретному направлению — Примеры мер физической и коммуникационной безопасности — Проектирование защищенных устройств обработки информации, разрешенных для дистанционного использования [например, «Принеси свое собственное устройство» (BYOD), ноутбуки]
6.8 Отчетность о событиях информационной безопасности			— Механизм предоставления отчетстности о событиях информационной безопасности, которые могут быть идентифицированы персоналом — Инструкции или сообщения для повышения осведомленности об отчетности о событиях информационной безопасности
7 Физические средства управления			
7.1 Физические периметры безопасности		возможно	— Правила построения безопасных зон и прочности физических барьеров — Физический периметр безопасности и проектирование безопасной зоны для каждого соответствующего местоположения
7.2 Физический вход	возможно	рекомен-довано	— Система авторизации доступа (физическая или электронная) для точек входа в безопасные зоны — Журналы доступа для отслеживания входа персонала и посетителей — Физическое проектирование зон доставки и погрузки с соответствующими описаниями процессов
7.3 Обеспечение безопасности офисов, помещений и объектов		возможно	— Проектирование и реализация физической безопасности офисов и объектов для защиты обрабатываемой секретной информации.
7.4 Мониторинг физической безопасности	возможно	возможно	— Проектирование систем физического наблюдения для обнаружения несанкционированного физического доступа — Защита систем мониторинга — Журналы, создаваемые при функционировании систем физического наблюдения
7.5 Защита от физических и экологических угроз		рекомен-довано	— Результаты оценки рисков физических и экологических угроз — Разработка соответствующих мер защиты от физических и экологических угроз

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
7.6 Работа в безопасных зонах		возможно	— Правила работы в безопасных зонах (указание конкретных мер безопасности) — Реализованные меры безопасности для безопасных зон
7.7 Чистые стол и экран		рекомен-довано	— Правила чистых стола и экрана, например, в политике по конкретному направлению — Выборочные проверки поведения чистого стола и экрана (например, рабочие зоны и принтеры)
7.8 Размещение и защита оборудования		возможно	— Правила размещения и защиты оборудования — Выборочные проверки размещения и защиты оборудования
7.9 Безопасность активов за пределами помещения			— Правила использования активов за пределами помещений организации (например, руководящие указания BYOD) — Результаты собеседований или опросов, проведенных среди персонала, использующего активы за пределами помещений организации
7.10 Носители данных	возможно		— Правила использования съемных носителей данных, например, в политике по конкретному направлению — Конфигурации устройств для ограничения или защиты передачи информации со съемных носителей и на съемные носители данных (включая, например, шифрование) — Процессы для безопасной утилизации и записи на основе таких процессов
7.11 Поддержка коммунальных служб		рекомен-довано	— Установленные меры защиты коммунальных служб, особенно в центрах обработки данных (например, температура, электроснабжение, вода) — Аварийные положения об отключении электроэнергии, воды, газа или других коммунальных служб
7.12 Безопасность кабельной проводки		возможно	— Физическая маршрутизация и защита кабельной проводки
7.13 Обслуживание оборудования			— Процедуры обслуживания различных типов оборудования — Записи об обслуживании оборудования
7.14 Безопасная утилизация или повторное использование оборудования	возможно	возможно	— Правила утилизации или повторного использования оборудования, содержащего носители данных — Записи о физическом или логическом уничтожении информации или оборудования
8 Технологические средства управления			

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.1 Пользовательские конечные устройства	возможно		— Правила безопасной конфигурации и обработки пользовательских конечных устройств, например, в политике по конкретному направлению — Мероприятия по повышению осведомленности конечного пользователя, охватывающие требования безопасности и процедуры защиты пользовательских конечных устройств — Правила разделения и защиты деловой информации на личных устройствах (BYOD), если применимо — Проектирование безопасных устройств обработки информации, разрешенных для удаленного использования (например, BYOD, ноутбуки)
8.2 Привилегированные права доступа	возможно		— Правила ограниченного распределения, использования и мониторинга привилегированных прав доступа, например, в политике по конкретному направлению — Процессы авторизации и анализа для управления привилегированными правами доступа
8.3 Ограничение доступа к информации	рекомен-довано		— Правила ограничений доступа к информации и другим связанным активам, например, в политике по конкретному направлению — Методы и процессы управления доступом для защиты доступа к секретной информации на протяжении всего ее жизненного цикла (т. е. создание, обработка, хранение, передача, утилизация)
8.4 Доступ к исходному коду	рекомен-довано		— Процедуры управления доступом на чтение и запись к исходному коду, инструментам разработки и библиотекам программного обеспечения
8.5 Безопасная аутентификация	рекомен-довано		— Правила технологий аутентификации и процедуры для управления доступом, например, в политике по конкретному направлению — Решения на основе риска и соответствующие реализации процедур входа в системы или приложения — Использование надежной или многофакторной аутентификации для критически важных информационных систем
8.6 Управление производительностью	возможно		— Текущие и ожидаемые требования к производительности — Измерения использования ресурсов, например, средств обработки информации, человеческих ресурсов, офисов и других объектов — Процедуры либо для обеспечения достаточной производительности, либо для снижения требований к производительности

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.7 Защита от вредоносных программ	рекомен-довано		— Правила защиты от вредоносных программ — Покрытие активов и соответствующей конфигурации программного обеспечения для обнаружения вредоносных программ, основанных на риске — Другие процедуры и меры по защите информации и других ресурсов от вредоносных программ — Мероприятия по повышению осведомленности конечного пользователя в отношении вредоносных программ
8.8 Управление техническими уязвимостями	рекомен-довано		— Сбор и управление информацией о технических уязвимостях используемых информационных систем — Результаты сканирования уязвимостей (регулярно выполняемого) или тестов на проникновение — Выполненные оценки подверженности организации техническим уязвимостям и запланированные меры по смягчению — Процесс обновления программного обеспечения для обеспечения установки самых последних подтвержденных исправлений и обновлений приложений
8.9 Управление конфигурацией	рекомен-довано		— Правила конфигураций, включая конфигурации безопасности, оборудования, программного обеспечения, служб и сетей — Процессы управления, внедрения или применения, мониторинга и анализа конфигураций — Стандартные шаблоны для безопасной конфигурации оборудования, программного обеспечения, служб и сетей (т. е. усиление безопасности)
8.10 Удаление информации			— Правила для своевременного удаления информации, хранящейся в информационных системах, устройствах или на любых других носителях данных, например, в соответствии с политикой по конкретному направлению по хранению данных — Процедуры для безопасного удаления секретной информации в системах, приложениях и службах — Соглашения с третьими лицами с положениями об удалении информации, в которых третьи стороны хранят информацию организации
8.11 Маскирование данных			— Правила маскировки данных, например, в соответствии с политикой организации по конкретному направлению по управлению доступом — Результаты анализов, проведенных для определения того, где защита секретной информации (например, PII) требует таких методов, как маскировка данных, псевдонимизация или анонимизация — Методы, используемые для маскировки данных, псевдонимизации или анонимизации

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.12 Предотвращение утечки данных	возможно		— Правила мер по предотвращению утечки данных, которые должны применяться к системам, сетям и любым другим устройствам, которые обрабатывают, хранят или передают конфиденциальную информацию — Выявленная информация, требующая защиты от утечки — Выявленные соответствующие каналы утечки с мерами по предотвращению утечки, включая мониторинг — Конфигурация системы предотвращения потери данных
8.13 Резервное копирование информации	рекомен-довано		— Правила резервного копирования информации, программного обеспечения и систем, например, в политике по конкретному направлению резервного копирования — Планы резервного копирования, основанные на установленных бизнес-требованиях организации — Оперативные процедуры для мониторинга своевременного и правильного выполнения резервного копирования и устранения сбоев — Тесты восстановления резервных копий, выполняемые через регулярные промежутки времени
8.14 Резервирование средств обработки информации			— Определенные требования к доступности бизнес-сервисов и информационных систем — Архитектура систем с высокими требованиями, обеспечивающая соответствующую избыточность — Результаты выполненных тестов отказоустойчивости
8.15 Ведение журнала	рекомен-довано		— Правила относительно цели, для которой создаются журналы, какие данные собираются, и любые конкретные требования к журналу по обработке данных журнала, например, в политике по конкретному направлению по ведению журналов — Список журналов, относящихся к безопасности, и меры по обеспечению их защиты от несанкционированных манипуляций — Процедуры для выполнения регулярного анализа и интерпретации событий журнала, например, для выявления необычных действий или аномального поведения — Конфигурация систем журналов
8.16 Мониторинг действий	возможно		— Правила мониторинга сетей, систем и приложений на предмет аномального поведения — Установленные базовые показатели нормального поведения и полученные критерии для срабатывания оповещений — Журналы мониторинга, поддерживаемые в течение определенных периодов хранения — Результаты анализа, выполненного для выявления аномального поведения

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.17 Синхронизация часов	возможно		— Список источников эталонного времени, используемых организацией — Методы синхронизации часов, и обработка разницы во времени
8.18 Использование привилегированных служебных программ	возможно		— Список используемых служебных программ, которые могут переопределять элементы управления системы и приложений — Процессы, процедуры и другие методы, используемые для ограничения и строгого управления таких служебных программ
8.19 Установка программного обеспечения в операционные системы	возможно		— Процедуры и меры, используемые для управления установкой программного обеспечения в операционных системах, включая инвентаризацию установленного программного обеспечения с версиями — Правила относительно типов программного обеспечения, которые могут устанавливать пользователи — Ограничения на установку программного обеспечения лицами, не являющимися обученными администраторами
8.20 Безопасность сетей	рекомен-довано		— Правила обеспечения безопасности информации в сетях и защиты подключенных сервисов от несанкционированного доступа — Меры и функции безопасности, реализованные для защиты информации в сетях и поддерживающих их средствах обработки информации, например, шаблоны конфигурации, конфигурация криптографических элементов управления, наборы правил шлюзов, пример конфигурации сетевых устройств — Документация по сетевой архитектуре (схемы, файлы конфигурации, разделение) — Правила аутентификации подключений систем к сети
8.21 Безопасность сетевых сервисов			— Правила безопасного использования сетей и сетевых сервисов — Список сетей и сетевых сервисов, используемых с механизмами безопасности и уровнями обслуживания — Гарантии, полученные от провайдеров сетевых сервисов
8.22 Разделение сетей			— Правила разделения сетевых доменов на основе, например, уровней доверия, критичности и секретности и в соответствии с политикой по конкретному направлению по управлению доступом — Топология сети (включая беспроводную) и разделение зон с описанием цели и правил — Определения периметров безопасности сетевых доменов — Процессы управления периметрами безопасности сетевых доменов, а также правила межсетевого экрана

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.23 Веб-фильтрация	возможно		— Правила безопасного и надлежащего использования онлайн-ресурсов, включая любые ограничения для нежелательных или ненадлежащих веб-сайтов — Меры, принятые для снижения воздействия вредоносного контента внешних веб-сайтов, например, правила фильтрации — Мероприятия по повышению осведомленности и обучению, проводимые для всего персонала по безопасному и надлежащему использованию онлайн-ресурсов
8.24 Использование криптографии	рекомен-довано		— Правила эффективного использования криптографии, включая приемлемые шифры и управление ключами, например, в политике по конкретному направлению по криптографии — Список криптографических методов, используемых организацией — Стандарты, процедуры и методы управления ключами, включая генерацию, хранение, архивирование, извлечение, распространение, изъятие и уничтожение криптографических ключей
8.25 Безопасный жизненный цикл разработки	возможно		— Правила безопасной разработки программного обеспечения, чтобы информационная безопасность была спроектирована и реализована в течение безопасного жизненного цикла разработки — Разделение между средами разработки, тестирования и эксплуатации — Процессы безопасности и контрольные точки, обеспечивающие адекватное соблюдение требований информационной безопасности в течение всей разработки программного обеспечения — Полученные гарантии надлежащего соблюдения требований информационной безопасности, когда разработка программного обеспечения передается на аутсорсинг
8.26 Требования к безопасности приложений			— Процесс определения требований безопасности приложений на основе оценки конкретных рисков — Выполненные оценки рисков приложений с указанием конкретных требований информационной безопасности — Требования, определенные для выборки недавних разработок/реализаций приложений, в частности для транзакционных услуг, приложений электронного заказа и оплаты

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.27 Безопасная архитектура системы и принципы проектирования			— Установленные архитектура и принципы проектирования безопасности для обеспечения того, чтобы информационные системы безопасно проектировались, реализовывались и эксплуатировались в течение жизненного цикла разработки — Интеграция принципов проектирования безопасности в разработку программного обеспечения — Пример безопасной реализации для конкретного приложения, подтверждающий использование вышеуказанных принципов проектирования — Встроенные принципы проектирования безопасности в контракты на аутсорсинговую разработку, если применимо
8.28 Безопасное кодирование	возможно		— Правила принципов безопасного кодирования, используемые как для новых разработок, так и в сценариях повторного использования — Процессы для обеспечения применения принципов безопасного кодирования во время планирования и перед кодированием, во время кодирования и во время проверки и обслуживания — Применение конкретных принципов безопасного кодирования для образцов недавних действий по разработке, включая методы сканирования кода — Механизмы защиты для кода, включая ограничения доступа
8.29 Тестирование безопасности при разработке и приемке	рекомен-довано		— Правила тестирования безопасности для проверки соблюдения требований информационной безопасности при развертывании приложений или кода в эксплуатационной среде — Образцы наборов требований, фактически используемых для тестирования безопасности, и соответствующие результаты тестирования — Вывод и последующие действия автоматизированных инструментов тестирования (например, инструментов анализа кода, сканеров уязвимостей, функциональных тестов)
8.30 Аутсорсинг разработки			— Правила, определяющие, как меры информационной безопасности, требуемые организацией, должны быть реализованы при разработке аутсорсинговых систем — Процедуры, реализованные для управления, мониторинга и анализа деятельности, связанной с разработкой аутсорсинговых систем — Результаты мониторинга или анализа поставщиков для обеспечения соответствия ожиданиям

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Продолжение таблицы Е.1

Средства управления в ИСО/МЭК 27001:2022, Приложение А[a]	Испытание системы	Визуальный осмотр	Возможные доказательства разработки и внедрения средств управления
8.31 Разделение сред разработки, тестирования и эксплуатации	возможно		— Правила для уровня разделения между средами эксплуатации, тестирования и разработки, включая конкретные требования к различным средам разработки — Разделение между средами разработки, тестирования и эксплуатации — Защита сред тестирования и эксплуатации (например, ограничения доступа, сетевое разделение, обеспечение того, чтобы не использовалась секретная эксплуатационная информация)
8.32 Управление изменениями	рекомен-довано		— Правила управления изменениями для сохранения информационной безопасности — Процедуры управления изменениями, например, документация, спецификация, тестирование, контроль качества и управление внедрением — Пример выполненных изменений, показывающий, как изменения были протестированы, одобрены и развернуты
8.33 Тестовая информация	возможно		— Правила надлежащего выбора, использования, защиты и управления тестовой информацией — Процедуры защиты эксплуатационной информации во время ее использования в целях тестирования (например, маскировка) — Примеры удаления информации из тестовых сред
8.34 Защита информационных систем во время тестирования аудита	возможно		— Список запросов на тесты аудита или другая гарантирующая деятельность, включающая оценку операционных систем — Пример выполненных тестов аудита и как они были согласованы и проведены

[a] Числа, указанные в этом столбце, соответствуют контрольным числам в ИСО/МЭК 27001:2022, Приложение А.

Приложение ДА

(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Т а б л и ц а ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 17021-1:2015	IDT	ГОСТ Р ИСО/МЭК 17021-1-2025. «Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования»
ISO/IEC 27001:2022	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

П р и м е ч а н и е – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT – идентичные стандарты.

Библиография

[1] ISO 19011 Guidelines for auditing management systems (Руководящие указания по проведению аудита систем менеджмента)

[2] ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

[3] ISO/IEC 27002 Information security, cybersecurity and privacy protection — Information security controls (Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью)

[4] ISO/IEC 27006-2 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems (Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 2. Системы менеджмента конфиденциальной информации)

[5] ISO/IEC 27007 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing (Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководящие указания по аудиту систем менеджмента информационной безопасности)

[6] ISO 9000 Quality management systems — Fundamentals and vocabulary (Системы менеджмента качества. Основные положения и словарь)

[7] ISO 9001 Quality management systems — Requirements (Системы менеджмента качества. Требования)

[8] ISO Guide 73[1)] Risk management — Vocabulary (Менеджмент риска. Словарь)

[9] IAF MD5 Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems, https://iaf.nu/en/iaf-documents/?cat_id=7, Last viewed: 2023-07-31 (Определение продолжительности аудита системы менеджмента качества, системы экологического менеджмента и системы менеджмента охраны здоровья и безопасности труда, https://iaf.nu/en/iaf-documents/?cat_id=7, последний просмотр: 2023-07-31.

[1)] Отменен

УДК 658.562:004:006.354 ОКС 03.120.20

Ключевые слова: информационная безопасность, кибербезопасность, защита конфиденциальности, сертификация, аудит, орган по сертификации, система менеджмента информационной безопасности