Проект

Изображение государственного Герба Республики Казахстан

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Информационная безопасность, кибербезопасность и защита конфиденциальности**

**ТРЕБОВАНИЯ К ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ АУДИТ И СЕРТИФИКАЦИЮ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**ЧАСТЬ 1**

**Общие требования**

**СТ РК ISO/IEC 27006-1-**

*(*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)*

*Настоящий проект стандарта*

*не подлежит применению до его утверждения*

**Комитет технического регулирования и метрологии**

**Министерства торговли и интеграции Республики Казахстан**

**(Госстандарт)**

**Астана**

**Предисловие**

1. **ПОДГОТОВЛЕН И ВНЕСЕН** Республиканским государственным предприятием на праве хозяйственного ведения «Казахстанский институт стандартизации и метрологии» Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан
2. **УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ** Приказом Председателя Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан от «\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ года № \_\_\_\_

**3** Настоящий стандарт идентичен международному стандарту 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 (Информационная безопасность, кибербезопасность и защита конфиденциальности. требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 1. Общие положения).

Международный стандарт разработан Объединенным техническим комитетом ISO/IEC JTC 1, Информационные технологии, Подкомитетом SC 27, Информационная безопасность, кибербезопасность и защита конфиденциальности, в сотрудничестве с Техническим комитетом Европейского комитета по стандартизации (CEN) CEN/CLC/JTC 13 Кибербезопасность и защита данных в соответствии с Соглашением о техническом сотрудничестве между ISO и CEN (Венское соглашение).

Перевод с английского языка (en)

Официальный экземпляр международного стандарта, на основе которого подготовлен настоящий национальный стандарт и на которые даны ссылки, имеется в Едином государственном фонде нормативных технических документов

Степень соответствия – идентичная (IDT)

**4 ВВЕДЕН ВЗАМЕН** СТ РК ISO/IEC 27006-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».

*Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом каталоге документов по стандартизации, а текст изменений и поправок – в периодически издаваемых информационных указателях стандартов. В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в периодически издаваемых информационных указателях стандартов.*

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан

**Содержание**

|  |  |
| --- | --- |
| Введение |  |
| 1 Область применения | 1 |
| 2 Нормативные ссылки | 1 |
| 3 Термины и определения | 1 |
| 4 Принципы | 9 |
| 5 Общие требования | 9 |
| 6 Структурные требования | 9 |
| 7 Требования к ресурсам | 9 |
| 8 Требования к информации | 13 |
| 9 Требования к процессу | 15 |
| 10 Требования к системе менеджмента для органов сертификации | 22 |
| Приложение A *(обязательное)* Знания и навыки для аудита и сертификации ISMS | 24 |
| Приложение B *(информационное)* Дополнительные соображения о компетентности | 25 |
| Приложение C *(обязательное)* Продолжительность аудита | 26 |
| Приложение D *(информационное)* Методы расчета продолжительности аудита | 33 |
| Приложение E *(информационное)* Руководство по обзору внедренных элементов управления ISO/IEC 27001:2022, Приложение A | 38 |
| Приложение В.А *(информационное)* Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств | 57 |
| Библиография | 58 |

**Введение**

Стандарт ISO/IEC 17021-1 устанавливает требования и рекомендации для органов, проводящих аудит и сертификацию систем менеджмента. Если такие органы намерены соответствовать ISO/IEC 17021-1 с целью аудита и сертификации систем менеджмента информационной безопасности (СМИБ) в соответствии с ISO/IEC 27001, некоторые дополнительные требования и рекомендации к ISO/IEC 17021-1 имеют решающее значение. Они предоставлены в этом стандарте.

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

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Информационная безопасность, кибербезопасность и защита конфиденциальности**

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

**Часть 1**

**Общие положения**

**Дата введения**

# Область применения

В настоящем стандарте установлены требования и даны рекомендации для органов, проводящих аудит и сертификацию системы менеджмента информационной безопасностью (СМИБ), в дополнение к требованиям, содержащимся в ISO/IEC 17021-1.

Требования, содержащиеся в настоящем стандарте, продемонстрированы с точки зрения компетентности и надежности органами, проводящими сертификацию СМИБ.

Руководство, содержащееся в настоящем стандарте, дает дополнительную интерпретацию данных требований для органов, проводящих сертификацию СМИБ.

Примечание - Настоящий стандарте может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки или других процессов аудита.

**2 Нормативные ссылки**

Для применения настоящего стандарта необходимы следующие ссылочные стандарты по стандартизации:

ISO/IEC 17021-1:2015, Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1: Требования

ISO/IEC 27001:2022, Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов по ежегодно издаваемому каталогу документов по стандартизации по состоянию на текущий год и соответствующим периодически издаваемым информационным указателям стандартов, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

1. **Термины и определения**

В настоящем стандарте применяются термины приведенные в ISO/IEC 17021-1, а также следующие термины с соответствующими определениями.

ISO и IEC ведут терминологические базы данных для использования в стандартизации по следующим адресам:

— Платформа для просмотра ISO Online: доступна по адресу https://www.iso.org/obp

— IEC Electropedia: доступна по адресу https://www.electropedia.org/

**3.1 Сертификационный документ (certification document):** Документ, указывающий на то, что СМИБ клиента соответствует указанным стандартам СМИБ и любой дополнительной документации, требуемой в рамках системы менеджмента.

Примечание 1 - Данное определение не ограничивает количество документов, совместно известных как сертификационные документы.

**3.2 Контроль (control):** мера, которая поддерживает и/или изменяет риск (3.10)

Примечание 1- Контроли включают, но не ограничиваются, любым процессом, политикой, устройством, практикой или другими условиями и/или действиями, которые поддерживают и/или изменяют риск (3.10).

Примечание 2 - Контроли не всегда могут оказывать предполагаемое изменяющее воздействие.

[ИСТОЧНИК: ISO/IEC 27002:2022, 3.1.8]

**3.3 Внешний контекст (external context):** внешняя среда, в которой организация (3.9) стремится достичь своих целей.

Примечание 1- Внешний контекст может включать:

- культурную, социальную, политическую, юридическую, нормативную, финансовую, технологическую, экономическую, природную и конкурентную среду, на международном, национальном, региональном или местном уровне;

- ключевые движущие факторы и тенденции, оказывающие влияние на цели организации (3.9);

- взаимоотношения с внешними заинтересованными сторонами (3.37), их мнения и ценности.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.22]

**3.4 Информационная безопасность** **(information security):** Сохранение конфиденциальности, целостности и возможности применения информации.

Примечание 1 - Кроме того, могут быть использованы другие свойства, такие как подлинность, контролируемость, неопровержимость авторства и надежность.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.28]

**3.5 Инцидент информационной безопасности (information security incident):** Отдельное или серия нежелательных или непредвиденных событий информационной безопасности, которые имеют значительную вероятность нарушить бизнес-процессы и поставить под угрозу информационную безопасность (3.4).

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.31]

**3.6 Информационная система (information system):** Совокупность приложений, служб, ИТ-активов или других компонентов обработки информации.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.35]

**3.7 Внутренний контекст (internal context):** Внутренняя среда, в которой организация (3.50) стремится достичь решения своих задач.

Примечание 1

Внутренний контекст может включать:

- органы управления, организационную структуру, роли и обязанности;

- политики, задачи и стратегии, которые применяются для их достижения;

- возможности, понимаемые в терминах ресурсов и накопленных знаний (например, капитал, время, персонал, процессы, системы и технологии);

- информационные системы (3.6), информационные потоки и процессы принятия решений (как формализованные, так и не формализованные);

- отношения с внутренними заинтересованными сторонами, их мнения и ценности;

- корпоративная культура организации (3.9);

- стандарты, руководства и модели, принятые организацией;

- форму и объем договорных отношений.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.38]

**3.8 Система менеджмента (management system):** Набор взаимосвязанных или взаимодействующих элементов организации (3.9) для установления политик и целей, а также процессов для достижения этих целей.

Примечание 1 - система менеджмента может охватывать одну дисциплину или несколько дисциплин, например, менеджмент качества, финансовый менеджмент или экологический менеджмент.

Примечание 2 - Элементы системы менеджмента устанавливают структуру организации (3.9), роли и обязанности, планирование, эксплуатацию, политику, практику, правила, убеждения, цели и процессы для достижения этих целей.

Примечание 3 - Область действия системы менеджмента может включать всю организацию (3.9), конкретные и определенные функции организации (3.9), конкретные и определенные разделы организации (3.9) или одну или несколько функций в группе организаций (3.9).

Примечание 4 - Это представляет собой один из общих терминов и основных определений для стандартов систем менеджмента ISO, приведенных в Приложении SL Сводного дополнения ISO к Директивам ISO/IEC, Часть 1. Первоначальное определение было изменено путем изменения Примечаний 1–3 к определению.

[ИСТОЧНИК: ISO 9000:2015, 3.5.3]

**3.9 Организация (organization):** Лицо или группа лиц, наделенные своими собственными функциями с обязанностями, полномочиями и взаимосвязями для решения своих задач.

Примечание 1 - Понятие организации включает, но не ограничено этим, индивидуального предпринимателя, компанию, корпорацию, фирму, предприятие, орган власти, партнерство, благотворительную организацию или учреждение, часть или комбинацию всего перечисленного, имеющих или не имеющих статус юридического лица, государственных или частных.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.50]

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

Примечание 1 - Влияние – это отклонение от ожидаемого – положительное или отрицательное.

Примечание 2 - Неопределенность – состояние хотя бы частичной нехватки информации, связанной с пониманием события или знанием о нем, его последствий или вероятности.

Примечание 3 - Риск часто характеризуется ссылкой на возможные «события» (как это определено в ISO Guide 73:2009, 3.5.1.3) и «последствия» (как это определено в ISO Guide 73:2009, 3.6.1.3), или их комбинации.

Примечание 4 - Риск часто выражается в форме комбинации последствий события (включая изменения в обстоятельствах) и связанной с ним «вероятности» (как это определено в ISO Guide 73:2009, 3.6.1.1) возникновения.

Примечание 5 - В контексте систем менеджмента информационной безопасности, риски могут быть выражены как влияние неопределенности на задачи в области информационной безопасности.

Примечание 6 - риск в сфере информационной безопасности связан с возможностью того, что угрозы будут реализовываться через использование уязвимостей информационного актива или группы информационных активов и, тем самым, наносить ущерб организации (3.9).

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.61]

**3.11 Анализ риска (risk analysis):** Процесс понимания характера риска (3.10) и определения уровня риска (3.39).

Примечание 1 - Анализ риска обеспечивает основу для определения степени риска и принятия решения об обработке риска (3.14).

Примечание 2 - Анализ рисков включает прогнозную оценку риска.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.63]

**3.12 Оценка риска (risk assessment):** Единый процесс идентификации риска, анализа риска (3.11) и определения степени риска.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.64]

**3.13 Управление рисками (risk management):** Скоординированные действия по руководству и управлению организацией (3.9) в отношении рисков (3.10).

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.69]

**3.14 Обработка риска (risk treatment):** Процесс, нацеленный на изменение риска (3.10).

Примечание 1 - Обработка риска может включать в себя:

- избегание риска путем принятия решения не начинать или не продолжать деятельность, которая приводит к возникновению риска;

- принятие или повышение степени риска с целью реализации возможностей;

- устранение источника риска;

- изменение вероятности;

- изменение последствий;

- разделение риска с другой стороной или сторонами (путем включения в контракты или финансового обеспечения риска);

- сохранение риска на основе обоснованного выбора.

Примечание 2 - Меры по обработке риска, которые принимаются в отношении негативных последствий, иногда называются «снижением риска», «устранением риска» и «предотвращением риска».

Примечание 3 - Обработка риска может создавать новые риски и изменять существующие.

[ИСТОЧНИК: ISO/IEC 27000:2018, 3.72]

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

[ИСТОЧНИК: ISO/IEC 27002:2022, 3.1.32 — изменено, примечание 1 к определению исключено.]

**4 Принципы**

Применяются требования ISO/IEC 17021-1:2015, 4.

**5 Общие требования**

**5.1 Правовые и договорные вопросы**

Применяются требования ISO/IEC 17021-1:2015, 5.1.

**5.2 Управление беспристрастностью**

**5.2.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 5.2. Кроме того, применяются требования и рекомендации в 5.2.2.

**5.2.2 Конфликты интересов**

Органы по сертификации могут вносить вклад в проведение сертификационных и надзорных аудитов (например, выявляя возможности для улучшения, которые становятся очевидными в ходе аудита, не рекомендуя конкретных решений), не считая это консультированием или потенциальным конфликтом интересов.

Орган по сертификации не должен проводить внутренние проверки информационной безопасности СМИБ клиента, подлежащего сертификации. Кроме того, орган по сертификации должен быть независим от органа или органов (включая любых лиц), которые проводят внутренний аудит СМИБ.

**5.3 Ответственность и финансирование**

Применяются требования ISO/IEC 17021-1:2015, 5.3.

**6 Требования к структуре**

Применяются требования ISO/IEC 17021-1:2015, Раздел 6.

**7 Требования к ресурсам**

**7.1 Компетентность персонала**

**7.1.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 7.1. Кроме того, применяются требования и рекомендации 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 ISO/IEC 17021-1:2015, Таблица A.1. Орган по сертификации должен учитывать все требования, указанные в ISO/IEC 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 B содержит дополнительные руководства по компетентности.

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

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

**7.1.3 Определение критериев компетентности**

**7.1.3.1 Требования к компетентности для 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 ISO 19011.

e) мониторингу, измерению, анализу и оценке СМИБ.

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

Члены аудиторской группы должны в совокупности обладать навыками, соответствующими требованиям, указанным выше, которые могут быть продемонстрированы на опыте их применения.

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

От отдельных аудиторов не требуется иметь полный спектр опыта во всех областях информационной безопасности, но аудиторская группа в целом должна иметь соответствующую компетентность для охвата области проверяемой СМИБ.

**7.1.3.1.2 Терминология, принципы, практики и методы менеджмента информационной безопасности**

Каждый аудитор в аудиторской группе СМИБ должен обладать знаниями:

a) специфических структур документации СМИБ, иерархии и взаимосвязей;

b) оценки рисков информационной безопасности и управления рисками;

c) процессов, применимых к СМИБ.

Члены аудиторской группы должны в совокупности обладать знаниями:

d) инструментов, методов, методов, связанных с менеджментом информационной безопасности, и их применения;

e) современных технологий, в которых информационная безопасность может быть актуальной или представлять собой проблему.

**7.1.3.1.3 Стандарты и нормативные документы систем менеджмента информационной безопасности**

Каждый аудитор в группе аудита СМИБ должен знать все требования, содержащиеся в ISO/IEC 27001.

Члены группы аудита должны, в совокупности, знать все средства менеджмента, содержащиеся в ISO/IEC 27001:2022, Приложение A, и их реализацию.

**7.1.3.1.4 Практики управления бизнесом**

Каждый аудитор в группе аудита СМИБ должен знать:

a) передовые практики информационной безопасности отрасли и процедуры информационной безопасности;

b) политики и бизнес-требования к информационной безопасности;

c) общие концепции управления бизнесом, практики и взаимосвязь между политикой, целями и результатами;

d) процессы управления и связанную терминологию.

Примечание - Эти процессы также включают управление человеческими ресурсами, внутреннюю и внешнюю коммуникацию и другие соответствующие вспомогательные процессы.

**7.1.3.1.5 Клиентский сектор бизнеса**

Каждый аудитор в аудиторской группе СМИБ должен обладать знаниями о:

a) правовых и нормативных требованиях в конкретной области информационной безопасности, географии и юрисдикции(ях);

Примечание-Знание правовых и нормативных требований не подразумевает глубокого юридического образования.

b) рисках информационной безопасности, связанных с бизнес-сектором;

c) общей терминологии, процессах и технологиях, связанных с клиентским сектором бизнеса;

d) соответствующей практике бизнес-сектора.

Критерий a) может быть общим для аудиторской группы.

**7.1.3.1.6 Клиентские продукты, процессы и организация**

Члены аудиторской группы должны в совокупности обладать знаниями о:

a) влиянии типа организации, размера, управления, структуры, функций и отношений на разработку и внедрение СМИБ и сертификационных мероприятий, включая аутсорсинг;

b) сложных операциях в широкой перспективе;

c) правовых и нормативных требованиях, применимых к продукту или услуге.

**7.1.3.2 Требования к компетентности для проведения проверки заявки**

**7.1.3.2.1 Сектор бизнеса клиента**

Персонал, проводящий проверку заявки для: определения требуемой компетентности аудиторской группы, выбора членов аудиторской группы и определения времени аудита, должен обладать знаниями общей терминологии, процессов, технологий и рисков, связанных с сектором бизнеса клиента.

**7.1.3.2.2 Клиентские продукты, процессы и организация**

Персонал, проводящий проверку заявки для: определения требуемой компетентности аудиторской группы, выбора членов аудиторской группы и определения времени аудита, должен обладать знаниями о влиянии клиентских продуктов, процессов, типов организаций, размера, управления, структуры, функций и взаимоотношений на разработку и внедрение СМИБ и сертификационных мероприятий, включая внешние функции.

**7.1.3.3 Требования к компетентности для рассмотрения аудиторских отчетов и принятия решений о сертификации**

**7.1.3.3.1 Общие положения**

Сотрудники, рассматривающие аудиторские отчеты и принимающие решения о сертификации, должны обладать знаниями, которые позволяют им проверять соответствие области сертификации, а также изменения в области и их влияние на эффективность аудита, в частности, постоянную действительность идентификации интерфейсов и зависимостей и связанных с ними рисков.

Кроме того, сотрудники, рассматривающие аудиторские отчеты и принимающие решения о сертификации, должны обладать знаниями о:

a) системах менеджмента в целом;

b) процессах и процедурах аудита.

**7.1.3.3.2 Терминология, принципы, методы и методики менеджмента информационной безопасности**

Сотрудники, рассматривающие аудиторские отчеты и принимающие решения о сертификации, должны обладать знаниями о:

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

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

**7.1.3.3.3 Сектор бизнеса клиента**

Сотрудники, рассматривающие аудиторские отчеты и принимающие решения о сертификации, должны обладать знаниями об общей терминологии и рисках, связанных с практикой соответствующего сектора бизнеса.

**7.1.3.3.4 Клиентские продукты, процессы и организация**

Персонал, рассматривающий аудиторские отчеты и принимающий решения о сертификации, должен обладать знаниями о клиентских продуктах, процессах, типах организаций, размере, управлении, структуре, функциях и отношениях.

**7.2 Персонал, участвующий в сертификационных мероприятиях**

**7.2.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 7.2. Кроме того, должны применяться требования и рекомендации в 7.2.2.

**7.2.2 Демонстрация знаний и опыта аудитора**

**7.2.2.1 Общие положения**

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

a) признанные квалификации, специфичные для СМИБ;

b) регистрация в качестве аудитора, где это применимо;

c) участие в курсах обучения СМИБ и получение соответствующей личной квалификации;

d) актуальные записи о профессиональном развитии;

e) аудиты СМИБ, засвидетельствованные другим аудитором СМИБ.

**7.2.2.2 Выбор аудиторов**

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

a) имеет профессиональное образование или подготовку, эквивалентную университетскому уровню;

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 ISO/IEC 27001. Данный опыт должен быть получен путем выполнения роли аудитора-стажера под наблюдением оценщика СМИБ (см. ISO/IEC 17021-1:2015, 9.2.2.1.4) по крайней мере в одном первоначальном сертификационном аудите СМИБ (этап 1 и этап 2) или повторной сертификации и по крайней мере в одном надзорном аудите. Данный опыт должен быть получен в течение как минимум 10 дней выездных аудитов СМИБ и проведенных в течение последних пяти лет. Участие должно включать проверку документов; проверку 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 каталог критериев компетентности для соответствия вышеуказанным требованиям и доказательствам (см. ISO/IEC 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 университетскому уровню;

b) имеет практический опыт работы 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 для руководства группой**

В дополнение к 7.2.2.2 критерии отбора аудитора для руководства группой должны гарантировать, что аудитор активно участвовал во всех этапах как минимум трех аудитов СМИБ. Участие должно включать начальное определение области действия и планирование, рассмотрение документов, рассмотрение оценки риска и ее внедрения, а также формальную аудиторскую отчетность.

**7.3 Использование отдельных внешних аудиторов и внешних технических экспертов**

Применяются требования ISO/IEC 17021-1:2015, 7.3.

**7.4 Кадровые записи**

Применяются требования ISO/IEC 17021-1:2015, 7.4.

**7.5 Аутсорсинг**

Применяются требования ISO/IEC 17021-1:2015, 7.5.

**8 Требования к информации**

**8.1 Общественная информация**

Применяются требования ISO/IEC 17021-1:2015, 8.1.

**8.2 Документы по сертификации**

**8.2.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 8.2. Кроме того, применяются требования и указания, изложенные в пунктах 8.2.2 и 8.2.3.

**8.2.2 Документы по сертификации СМИБ**

Документы по сертификации должны быть подписаны должностным лицом, которому была назначена эта ответственность. Версия Заявления о применимости должна быть включена в документы по сертификации.

Примечание - Изменение Заявления о применимости, которое не меняет охват элементов управления в области сертификации, не требует обновления документов по сертификации.

Если никакая деятельность организации в области сертификации не осуществляется в определенном физическом месте, в документе(ах) по сертификации должно быть указано, что вся деятельность организации осуществляется удаленно.

**8.2.3 Ссылки на другие стандарты в документах по сертификации СМИБ**

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

a) организация сравнила все свои необходимые элементы управления с теми, которые находятся в источнике(ах) справочного контроля, чтобы определить, что она не упустила случайно ни один такой справочный элемент управления в соответствии с   
ISO/IEC 27001:2022, 6.1.3 c);

b) обоснование исключения эталонных элементов управления приведено в Заявлении о применимости (SoA) в соответствии с ISO/IEC 27001:2022, 6.1.3 d).

Стандарты контрольных элементов могут быть основаны на ISO/IEC 27001:2022, Приложение A, или быть стандартами, которые включают контрольные элементы информационной безопасности.

В документах по сертификации должно быть указано, что набор(ы) контрольных элементов, применяемых в SoA, используются только для ссылки на релевантность включения или исключения контрольных элементов в СМИБ и не используются для оценки соответствия.

**8.3 Ссылка на сертификацию и использование знаков**

Применяются требования ISO/IEC 17021-1:2015, 8.3.

**8.4 Конфиденциальность**

**8.4.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 8.4. Кроме того, применяются требования и рекомендации в 8.4.2.

**8.4.2 Доступ к организационным записям**

Перед сертификационным аудитом орган по сертификации должен попросить клиента сообщить, если какая-либо информация, связанная с СМИБ (например, записи СМИБ или информация о разработке и эффективности средств контроля), не может быть предоставлена для проверки аудиторской группой, поскольку она содержит конфиденциальную или чувствительную информацию. Орган по сертификации должен определить, может ли СМИБ быть адекватно проверена при отсутствии такой информации. Если орган по сертификации приходит к выводу, что невозможно адекватно проверить СМИБ без проверки выявленной конфиденциальной или чувствительной информации, он должен сообщить клиенту, что сертификационный аудит не может быть проведен до тех пор, пока не будут предоставлены соответствующие договоренности о доступе.

**8.5 Обмен информацией между органом по сертификации и его клиентами**

Применяются требования ISO/IEC 17021-1:2015, 8.5.

**9 Требования к процессу**

**9.1 Предсертификационные мероприятия**

**9.1.1 Применение**

**9.1.1.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 9.1.1. Кроме того, должны применяться требования и рекомендации в 9.1.1.2.

**9.1.1.2 Соображения по процедурам сертификации**

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

Примечание - Организация может разработать собственные необходимые элементы управления или выбрать их из любого источника, поэтому возможно, что организация сертифицирована по ISO/IEC 27001, даже если ни один из ее необходимых элементов управления не указан в ISO/IEC 27001:2022, Приложение A.

**9.1.2 Рассмотрение заявки**

Применяются требования ISO/IEC 17021-1:2015, 9.1.2.

**9.1.3 Программа аудита**

**9.1.3.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 9.1.3. Кроме того, Применяются требования и рекомендации 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 положения**

Программа аудита для аудитов СМИБ должна учитывать средства менеджмента информационной безопасности, определенные клиентом.

Примечание 1 - Средства менеджмента информационной безопасности могут быть из ISO/IEC 27001:2022, Приложение A, и/или других применимых стандартов и/или разработаны самостоятельно.

Примечание 2 - Дальнейшие рекомендации по аудиту приведены в ISO/IEC 27007.

**9.1.3.3 Развертывание удаленного аудита**

Органы по сертификации, намеревающиеся проводить удаленные аудиторские мероприятия, должны определить процедуры для определения уровня удаленных аудиторских мероприятий («удаленные аудиты»), которые могут применяться для аудита СМИБ клиента. Процедуры должны включать анализ рисков, связанных с использованием удаленного аудита для клиента, который должен учитывать следующие факторы:

a) доступная инфраструктура органа по сертификации и клиента;

b) сектор, в котором работает клиент;

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

d) компетентность лиц органа по сертификации и клиента, которые участвуют в удаленном аудите;

e) ранее продемонстрированное выполнение удаленных аудитов для клиента;

f) область сертификации.

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

План аудита и отчет по аудиту должны включать четкие указания, были ли выполнены мероприятия удаленного аудита.

Удаленные аудиты не должны использоваться, если оценка риска выявляет неприемлемые риски для эффективности процесса аудита.

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

Примечание В случае, если клиент 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 соответствующей частью плана аудита.

**9.1.3.4 Общая подготовка к первоначальному аудиту**

Орган по сертификации должен потребовать, чтобы клиент принял все необходимые меры для обеспечения доступа к отчетам внутреннего аудита и отчетам независимых проверок информационной безопасности.

**9.1.3.5 Периоды проверки**

Орган по сертификации не должен сертифицировать СМИБ, если нет достаточных доказательств того, что меры по управленческим проверкам и внутренним аудитам СМИБ были внедрены, эффективны и будут поддерживаться, охватывая область сертификации.

**9.1.3.6 Область сертификации СМИБ**

Аудиторская группа должна провести аудит СМИБ клиента, охватываемый определенной областью, на соответствие всем применимым требованиям сертификации. Орган по сертификации должен подтвердить в области СМИБ клиента, что клиент выполняет требования, указанные в ISO/IEC 27001:2022, 4.3.

Органы по сертификации должны гарантировать, что оценка и обработка рисков информационной безопасности клиента надлежащим образом отражают его деятельность и выходят за границы его деятельности, как определено в области сертификации. Органы по сертификации должны подтвердить, что это отражено в области действия СМИБ и SoA клиента. Орган по сертификации должен проверить, что для области сертификации существует SoA.

Органы по сертификации должны гарантировать, что интерфейсы с услугами или видами деятельности, которые не полностью входят в область действия СМИБ, рассматриваются в рамках СМИБ, подлежащей сертификации, и включены в оценку риска информационной безопасности клиента. Примером такой ситуации является совместное использование объектов (например, ИТ-систем, баз данных и телекоммуникационных систем или аутсорсинг бизнес-функции) с другими организациями.

**9.1.4 Определение времени аудита**

**9.1.4.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.1.4. Кроме того, должны применяться требования и рекомендации в 9.1.4.2.

**9.1.4.2 Время аудита**

Орган по сертификации должен использовать Приложение C для определения времени аудита.

Примечание - Дополнительные рекомендации и примеры расчета времени аудита приведены в Приложении D.

**9.1.5 Выборка на нескольких площадках**

**9.1.5.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.1.5. Кроме того, должны применяться требования и рекомендации в 9.1.5.2.

**9.1.5.2 Несколько площадок**

**9.1.5.2.1** Если у клиента есть несколько площадок, соответствующих критериям от a) до c) ниже, органы по сертификации могут рассмотреть возможность использования подхода на основе выборки для аудита сертификации на нескольких площадках:

a) все площадки работают в рамках одной и той же СУИБ, которая централизованно администрируется и проверяется, и подлежит проверке со стороны центрального руководства;

b) все площадки включены во внутреннюю программу аудита СУИБ клиента;

c) все площадки включены в программу проверки менеджмента СУИБ клиента.

**9.1.5.2.2** Орган по сертификации, желающий использовать подход на основе выборки, должен иметь процедуры, обеспечивающие:

a) Первоначальный обзор контракта выявляет, в максимально возможной степени, разницу между площадками, чтобы определить адекватный уровень выборки.

b) Орган по сертификации отобрал репрезентативное количество площадок, принимая во внимание:

1) результаты внутренних аудитов центрального офиса (если применимо) и площадок;

2) результаты управленческого анализа;

3) различия в размерах площадок;

4) различия в бизнес-целях площадок;

5) сложность информационных систем на разных площадках;

6) различия в рабочих практиках;

7) различия в осуществляемых мероприятиях;

8) различия в дизайне и работе средств контроля;

9) потенциальное взаимодействие с критически важными информационными системами или информационными системами, обрабатывающими конфиденциальную информацию;

10) любые отличающиеся правовые требования;

11) географические и культурные аспекты;

12) ситуацию риска на площадках;

13) инциденты информационной безопасности на определенных сайтах.

c) Из всех сайтов в области действия СМИБ клиента выбирается репрезентативная выборка; этот выбор должен быть основан на оценочном выборе, чтобы отразить факторы, представленные в пункте b) выше, а также случайный элемент.

d) Каждый сайт, включенный в СМИБ, который подвержен значительным рискам, проверяется органом по сертификации до сертификации.

e) Программа аудита была разработана с учетом вышеуказанных требований и охватывает репрезентативные выборки области действия сертификации СМИБ в течение трехлетнего периода.

f) В случае обнаружения несоответствия на одном сайте процедура корректирующих действий применяется ко всем сайтам, охватываемым сертификатом.

Аудит должен рассматривать деятельность клиента, чтобы гарантировать, что единая СМИБ применяется ко всем сайтам и обеспечивает централизованный менеджмент на операционном уровне. Аудит должен охватывать все вопросы, изложенные выше.

**9.1.6 Несколько систем менеджмента**

**9.1.6.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.1.6. Кроме того, должны применяться требования и рекомендации в 9.1.6.2 и 9.1.6.3.

**9.1.6.2 Интеграция СУИБ и другой документации системы менеджмента**

Орган по сертификации может принимать объединенную документацию (например, по информационной безопасности, качеству, охране труда и окружающей среды), если СУИБ может быть четко идентифицирована вместе с соответствующими интерфейсами с другими системами менеджмента.

**9.1.6.3 Объединение аудитов систем менеджмента**

Аудит СУИБ может быть объединен с аудитами других систем менеджмента, если можно продемонстрировать, что аудит удовлетворяет всем требованиям сертификации СУИБ. Все важные элементы СУИБ должны быть четко обозначены и легко идентифицируемы в отчетах по аудиту. Качество аудита не должно быть отрицательно затронуто объединением аудитов.

**9.2 Планирование аудитов**

**9.2.1 Определение целей, области и критериев аудита**

**9.2.1.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.2.1. Кроме того, должны применяться требования и рекомендации в 9.2.1.2 и 9.2.1.3.

**9.2.1.2 Цели аудита**

Цели аудита должны включать:

a) определение эффективности системы менеджмента;

b) обеспечение того, чтобы клиент на основе оценки рисков определил необходимые элементы управления; и

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

**9.2.1.3 Критерии аудита**

Критерии аудита СМИБ клиента должны включать ISO/IEC 27001.

**9.2.2 Выбор и назначение аудиторской группы**

**9.2.2.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.2.2.

**9.2.3 План аудита**

**9.2.3.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.2.3. Кроме того, должны применяться требования и рекомендации в 9.2.3.2 и 9.2.3.3.

**9.2.3.2 Общие положения**

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

Примечание. Хорошей практикой для органа по сертификации является согласование сроков аудита с проверяемой организацией, чтобы наилучшим образом продемонстрировать всю сферу деятельности организации. Соображения могут включать сезон, месяц, день/дату и смены, в зависимости от обстоятельств.

**9.2.3.3 Методы удаленного аудита**

Целью методов удаленного аудита должно быть повышение эффективности и результативности аудита, а также поддержка целостности процесса аудита.

План аудита должен ссылаться на инструменты, которые используются для содействия удаленному аудиту.

**9.3 Первоначальная сертификация**

**9.3.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.3. Кроме того, должны применяться требования и рекомендации 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, требуемую в ISO/IEC 27001.

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

a) общая информация, касающаяся СМИБ и охватываемых ею видов деятельности;

b) копия требуемой документации СМИБ, указанной в ISO/IEC 27001, и, при необходимости, другая сопутствующая документация.

Орган по сертификации должен получить достаточное понимание структуры СМИБ в контексте организации клиента, оценки и обработки рисков (включая определенные элементы управления), политики и целей информационной безопасности и, в частности, готовности клиента к аудиту. Это должно использоваться для планирования аудита этапа 2.

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

Примечание. Наличие человека из органа по сертификации, который не участвует в аудите и который решает продолжить и подтверждает компетентность членов аудиторской группы для этапа 2, обеспечивает определенную степень смягчения связанных рисков. Однако другие меры по смягчению рисков могут уже быть реализованы для достижения той же цели.

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

**9.3.2.2 Этап 2**

На основе результатов, задокументированных в отчете по аудиту этапа 1, орган по сертификации должен разработать план аудита для проведения этапа 2. Помимо оценки эффективного внедрения СМИБ, цель этапа 2 заключается в подтверждении того, что клиент придерживается своих собственных политик, целей и процедур.

Для этого аудит должен быть сосредоточен на:

a) руководстве 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 при повторении;

c) определении средств контроля на основе оценки рисков информационной безопасности и процессов обработки рисков;

d) эффективности информационной безопасности и их оценке в соответствии с целями информационной безопасности;

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

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

g) программы, процессы, процедуры, записи, внутренние аудиты и обзоры эффективности СМИБ для обеспечения их прослеживаемости до решений высшего руководства и политики и целей информационной безопасности.

**9.4 Проведение аудитов**

**9.4.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.4. Кроме того, должны применяться требования и рекомендации в 9.4.2 и 9.4.3.

**9.4.2 Конкретные элементы аудита СМИБ**

Аудиторская группа органа по сертификации должна:

a) потребовать от клиента продемонстрировать, что оценка рисков, связанных с информационной безопасностью, является актуальной и адекватной для работы СМИБ в рамках области действия СМИБ;

b) установить, соответствуют ли процедуры клиента по идентификации, проверке и оценке рисков, связанных с информационной безопасностью, и результаты их реализации политике, целям и задачам клиента.

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

**9.4.3 Отчет об аудите**

**9.4.3.1** Отчет об аудите должен содержать следующую информацию или ссылку на нее:

a) отчет об аудите анализа рисков информационной безопасности клиента;

b) любые наборы средств контроля информационной безопасности, используемые организацией для целей сравнения, как того требует ISO/IEC 27001:2022, 6.1.3 c).

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

a) существенные аудиторские следы и использованные аудиторские методологии (см. 9.1.1.2);

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

Заполненные анкеты, контрольные списки, наблюдения, журналы или аудиторские заметки могут составлять неотъемлемую часть аудиторского отчета. Если используются эти методы, эти документы должны быть представлены в орган по сертификации в качестве доказательств для поддержки решения о сертификации. Информация об образцах, оцененных во время аудита, должна быть включена в аудиторский отчет или в другую сертификационную документацию.

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

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

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

Отчёт должен включать сводку наиболее важных наблюдений, как положительных, так и отрицательных, относительно внедрения и эффективности требований СМИБ и средств контроля информационной безопасности.

**9.5 Решение о сертификации**

**9.5.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 9.5. Кроме того, применяются требования и рекомендации, изложенные в 9.5.2.

**9.5.2 Решение о сертификации**

Решение о сертификации должно основываться на рекомендациях по сертификации аудиторской группы, представленных в отчете о сертификационном аудите.

Сертификация не будет выдана клиенту, пока не будет достаточных доказательств, подтверждающих, что меры по управленческим проверкам и внутренним аудитам СУИБ были внедрены, эффективны и будут поддерживаться.

**9.6 Поддержание сертификации**

**9.6.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 9.6.1.

**9.6.2 Надзорные мероприятия**

**9.6.2.1** Применяются требования ISO/IEC 17021-1:2015, 9.6.2. Кроме того, применяются требования и рекомендации в 9.6.2.2, 9.6.2.3 и 9.6.2.4.

**9.6.2.2** Процедуры надзорного аудита должны быть подмножеством процедур сертификационного аудита СМИБ клиента, как описано в настоящем документе.

Цель надзора — проверить, что утвержденная СМИБ продолжает внедряться, рассмотреть последствия изменений в СМИБ, инициированных в результате изменений в операционных практиках клиента, и подтвердить постоянное соответствие требованиям сертификации. Программы надзорного аудита должны охватывать как минимум:

a) элементы обслуживания СМИБ, такие как оценка рисков информационной безопасности и обслуживание контроля, внутренний аудит СМИБ, обзор руководства и корректирующие действия;

b) сообщения от внешних сторон, как того требуют ISO/IEC 27001 и другие документы, необходимые для сертификации.

**9.6.2.3** Как минимум, каждый надзорный аудит, проводимый органом по сертификации, должен проверять следующее:

a) эффективность СМИБ в отношении достижения целей политики информационной безопасности клиента;

b) функционирование процедур периодической оценки и проверки соответствия соответствующим законам и правилам информационной безопасности;

c) изменения в определенных средствах контроля и вытекающие из этого изменения в SoA;

d) внедрение и эффективность средств контроля, указанных в программе аудита.

**9.6.2.4** Орган по сертификации должен иметь возможность адаптировать свою программу мероприятий по надзору для отражения вопросов информационной безопасности, связанных с рисками и воздействиями на клиента, и обосновать эту программу.

Надзорные аудиты могут быть объединены с аудитами других систем менеджмента. В аудиторских отчетах должны быть четко указаны аспекты, относящиеся к каждой системе менеджмента.

В ходе надзорных аудитов органы по сертификации должны проверять записи апелляций и жалоб, поданных в орган по сертификации. В случае выявления любого несоответствия или невыполнения требований сертификации органы по сертификации должны проверить, что клиент изучил собственную СМИБ и процедуры и предпринял соответствующие корректирующие действия.

Отчет о надзоре должен содержать, в частности, информацию об устранении несоответствий, выявленных ранее, версию SoA и важные изменения по сравнению с предыдущим аудитом. Как минимум, отчеты, вытекающие из надзора, должны быть составлены так, чтобы в совокупности охватывать требования 9.6.2.2 и 9.6.2.3.

**9.6.3 Повторная сертификация**

**9.6.3.1 Общие положения**

Должны применяться требования ISO/IEC 17021-1:2015, 9.6.3. Кроме того, должны применяться требования 9.6.3.2.

**9.6.3.2 Аудиты повторной сертификации**

Процедуры аудита повторной сертификации должны быть подмножеством процедур для первоначального сертификационного аудита СМИБ клиента, как описано в настоящем стандарте.

Время, отведенное на выполнение корректирующих действий, должно соответствовать серьезности несоответствия и связанному с ним риску информационной безопасности.

**9.6.4 Специальные аудиты**

Применяются требования ISO/IEC 17021-1:2015, 9.6.4.

**9.6.5 Приостановка, отзыв или сокращение области сертификации**

Применяются требования ISO/IEC 17021-1:2015, 9.6.5.

**9.7 Апелляции**

Применяются требования ISO/IEC 17021-1:2015, 9.7.

**9.8 Жалобы**

**9.8.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 9.8.

**9.8.2 Жалобы**

Жалобы представляют собой потенциальный инцидент и указание на возможное несоответствие.

**9.9 Клиентские записи**

Применяются требования ISO/IEC 17021-1:2015, 9.9.

**10 Требования к системе менеджмента для органов сертификации**

**10.1 Варианты**

**10.1.1 Общие положения**

Применяются требования ISO/IEC 17021-1:2015, 10.1. Кроме того, применяются требования и рекомендации в 10.1.2.

**10.1.2 Внедрение СМИБ**

Рекомендуется, чтобы органы по сертификации внедрили СМИБ в соответствии с ISO/IEC 27001.

**10.2 Вариант A: Общие требования к системе менеджмента**

Должны применяться требования ISO/IEC 17021-1:2015, 10.2.

**10.3 Вариант B: Требования к системе менеджмента в соответствии с ISO 9001**

Должны применяться требования ISO/IEC 17021-1:2015, 10.3.

**Приложение A**

*(обязательное)*

**Знания и навыки для аудита и сертификации СМИБ**

**A.1 Обзор**

В таблице A.1 указаны знания и навыки, которые орган по сертификации должен определить для конкретных функций сертификации, в дополнение к требованиям   
ISO/IEC 17021-1. «X» указывает, что орган по сертификации должен определить критерии и глубину знаний и навыков. Требования к знаниям и навыкам, указанные в Таблице A.1, более подробно поясняются в Разделе 7 и перекрестно ссылаются в скобках в Таблице A.1.

**Таблица A.1 — Таблица знаний и навыков для аудита и сертификации СМИБ**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Функция сертификации | | |
| Знания и навыки | Проведение обзора заявки для определения необходимой компетентности аудиторской группы, отбора членов аудиторской группы и определения времени аудита | Рассмотрение аудиторских отчетов и принятие решений о сертификации | Аудит и руководство аудиторской группой |
| Терминология, принципы, практики и методы менеджмента информационной безопасности |  | X (см. 7.1.3.3.2) | X (см. 7.1.3.1.2) |
| Стандарты/норматив-ные документы системы менеджмента информационной безопасности |  |  | X (см. 7.1.3.1.3) |
| Практики менеджмента бизнеса |  |  | X (см. 7.1.3.1.4) |
| Сектор бизнеса клиента | X (см. 7.1.3.2.1) | X (см. 7.1.3.3.3) | X (см. 7.1.3.1.5) |
| Продукты, процессы и организация клиента | X (см. 7.1.3.2.2) | X (см. 7.1.3.3.4) | X (см. 7.1.3.1.6) |

Примечание - Дополнительные соображения по компетентности содержатся в Приложении B.

**Приложение B**

*(информативное)*

**Дополнительные соображения о компетентности**

**B.1 Общие соображения о компетентности**

Существует несколько способов, с помощью которых аудиторы могут продемонстрировать свои знания и опыт. Знания и опыт можно оценить, например, с помощью признанных квалификаций. Регистрационные записи в рамках схемы сертификации персонала также могут использоваться для оценки требуемых знаний и опыта. Требуемый уровень компетентности для аудиторской группы должен быть установлен, отражая отраслевую/технологическую область организации и сложность СМИБ.

**B.2 Конкретные соображения о знаниях и опыте**

**B.2.1 Типичные знания, связанные с СМИБ**

В дополнение к требованиям в 7.1.3, следует учитывать следующее. Аудиторы должны обладать знаниями и пониманием следующих предметов аудита и СМИБ:

- программирование и планирование аудита;

- тип и методологии аудита;

- аудиторский риск;

- анализ процессов информационной безопасности;

- постоянное улучшение;

- внутренний аудит информационной безопасности.

Аудиторы должны обладать знаниями и пониманием нормативных требований по следующим вопросам:

- интеллектуальная собственность;

- содержание, защита и хранение организационных записей;

- защита данных и конфиденциальность;

- регулирование криптографического контроля;

- электронная коммерция;

- электронные и цифровые подписи;

- наблюдение на рабочем месте;

- перехват телекоммуникаций и мониторинг данных (например, электронной почты);

- компьютерное злоупотребление;

- сбор электронных доказательств;

- тестирование на проникновение;

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

Возможно, что для определенного сектора знания и понимание устанавливаются в определенном стандарте (например, ISO/IEC 27006-2).

**Приложение C**

*(обязательное)*

**Продолжительность аудита**

**C.1 Общие положения**

Данное приложение содержит дополнительные требования, связанные с ISO/IEC 17021-1:2015, 9.1.4. Данное приложение содержит минимальные требования и рекомендации для органа по сертификации по разработке собственных процедур для определения продолжительность, 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, надзорным аудитом или аудитом повторной сертификации. Расчет общего времени аудита должен включать достаточное время для аудиторской отчетности.

Органы по сертификации должны определять количество времени аудита, которое необходимо потратить на первоначальную сертификацию, надзор и повторную сертификацию для каждого клиента и сертифицированной СМИБ. Использование данного 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 этапе 1 (например, различная оценка сложности области действия СМИБ или дополнительные площадки в области действия).

В данном приложении представлены:

- концепции, которые используются для расчета продолжительности аудита (C.2);

- требования к процедурам определения продолжительности аудита для различных этапов первоначального аудита (C.3);

- требования к продолжительности аудита для надзора (C.4) и аудита повторной сертификации (C.5);

- требования, связанные с многосайтовыми аудитами (C.6);

- требования к продолжительности аудита для расширения области действия (C.7).

Примеры расчета продолжительности аудита, иллюстрирующие применение этого приложения, можно найти в Приложении D.

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

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

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

c) быть достаточно сложным, чтобы гарантировать, что изменения в значениях атрибутов приводят к сопоставимым изменениям в конечном времени аудита.

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

Подход к определению времени аудита, определенный органом по сертификации, должен регулярно пересматриваться, чтобы проверить, достаточно ли он для сложности СМИБ.

**C.2 Понятия**

**C.2.1 Количество лиц, выполняющих работу под контролем организации**

Общее количество лиц, выполняющих работу под контролем организации для всех смен в рамках области сертификации, является отправной точкой для определения времени аудита.

Примечание - Лица, выполняющие работу под контролем 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 неполный рабочий день, выполняющие работу под контролем организации, вносят вклад в количество лиц, выполняющих работу под контролем организации пропорционально количеству отработанных часов по сравнению с лицом, работающим полный рабочий день, выполняющим работу под контролем организации. Это определение должно зависеть от количества отработанных часов по сравнению с сотрудником, работающим полный рабочий день.

Когда высокий процент лиц, выполняющих работу под контролем организации в рамках области сертификации, выполняют определенные идентичные действия, допускается сокращение количества лиц до использования Таблицы C.1 для расчета времени аудита. Органы по сертификации должны использовать факторы, указанные в C.3.4, и учитывать влияние деятельности на риск информационной безопасности, чтобы определить, как применяется сокращение числа лиц в рамках сертификации. Последовательные и последовательные процедуры, которые можно повторять и применять на уровне компании, должны быть задокументированы.

**C.2.2 День аудитора**

Время аудита, указанное в Таблице C.1, указывается в терминах дней аудитора, потраченных на аудит. Это приложение основывает свои расчеты на восьмичасовом рабочем дне (сокращенно «d»).

**C.2.3 Временная площадка**

Временная площадка, которая попадает в сферу сертификации, — это место, отличное от площадок, указанных в документах по сертификации, где деятельность в рамках сертификации осуществляется в течение определенного периода времени. Эти площадки могут варьироваться от крупных площадок управления проектами до второстепенных площадок обслуживания/установки. Необходимость посещения таких площадок и объем выборки должны основываться на оценке рисков деятельности, выполняемой на этой временной площадке, для достижения целей информационной безопасности. Выборка таких выбранных площадок должна представлять диапазон потребностей организации в компетентности и вариаций услуг в свете размеров и типов деятельности, а также различных стадий проектов в процессе выполнения. Для общей выборки см. 9.1.5.2.

**C.3 Процедура определения времени аудита для первоначального аудита**

**C.3.1 Общие положения**

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

**C.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 виды деятельности должны быть определены в плане аудита (см. 9.2.3) и могут рассматриваться как частично вносящие вклад в общее «время аудита на месте».

Примечание. Время аудита на месте относится ко времени аудита на месте, выделенному для отдельных площадок. Электронные аудиты удаленных площадок считаются дистанционными аудитами, даже если электронные аудиты физически проводятся на территории организации.

**C.3.3 Расчет продолжительности аудита**

Диаграмма продолжительности аудита, представленная в Таблице C.1, устанавливает отправную 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 заданным количеством лиц, выполняющих работу под контролем организации. Опыт также показал, что для областей действия СМИБ схожего размера некоторым требуется больше времени, чем другим.

Диаграмма продолжительности аудита ниже представляет собой структуру, которая должна использоваться для планирования аудита. Отправная точка основана на общем количестве лиц, выполняющих работу под контролем организации для всех смен. Количество дней аудитора корректируется на основе значимых факторов, применяемых к области действия СМИБ, подлежащей аудиту, с присвоением добавочного или вычитательного веса для каждого фактора для изменения базовой цифры. Диаграмма продолжительности аудита в Таблице C.1 должна использоваться с учетом способствующих факторов и ограничений допустимого отклонения (см. C.3.5 и C.3.6). Термины, используемые в таблице C.1, поясняются в C.2. Приложение D содержит примеры того, как может применяться метод расчета настоящего приложения.

**C.3.4 Определение начального количества лиц**

Органы по сертификации должны запрашивать у клиента информацию, касающуюся большого количества лиц, выполняющих определенные идентичные действия, включая:

— количество лиц, вовлеченных в действие;

— тип действия или процесса.

Примеры факторов, которые могут уменьшить количество 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 продемонстрированный ограниченный доступ к средствам обработки информации компании в рамках СМИБ;

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

Сокращение числа лиц, выполняющих идентичные действия, должно быть сделано на основе риска действий, связанных с задачами. Квадратный корень из численности лиц, выполняющих каждое идентичное действие, может использоваться для определения эффективного числа лиц, которое используется для расчетов продолжительности аудита, округленного до следующего целого числа. Это число должно быть максимально допустимым сокращением численности лиц.

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

Число лиц, определенное после данной процедуры, является отправной точкой в Таблице C.1.

Примечание - Таблица структурирована идентично IAF MD5.[9]

**Таблица C.1 — График продолжительности аудита**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Количество лиц, выполняющих работу под контролем организации | Время аудита системы менеджмента качества для первоначального аудита (дни аудитора, d) | Время аудита системы экологического менеджмента для первичного аудита (дни аудитора, d) | Время аудита СМИБ для первичного аудита (дни аудитора, d) | Аддитивные и вычитательные факторы | Общая продолжительность аудита |
| 1-10 | 1,5-2 | 2,5-3 | 5 | См. C.3.5 |  |
| 11-15 | 2,5 | 3,5 | 6 | См. C.3.5 |  |
| 16-25 | 3 | 4,5 | 7 | См. C.3.5 |  |
| 26-45 | 4 | 5,5 | 8,5 | См. C.3.5 |  |
| 46-65 | 5 | 6 | 10 | См. C.3.5 |  |
| 66-85 | 6 | 7 | 11 | См. C.3.5 |  |
| 86-125 | 7 | 8 | 12 | См. C.3.5 |  |
| 126-175 | 8 | 9 | 13 | См. C.3.5 |  |
| 176-275 | 9 | 10 | 14 | См. C.3.5 |  |
| 276-425 | 10 | 11 | 15 | См. C.3.5 |  |
| 426-625 | 11 | 12 | 16,5 | См. C.3.5 |  |
| 626-875 | 12 | 13 | 17,5 | См. C.3.5 |  |
| 876-1175 | 13 | 15 | 18,5 | См. C.3.5 |  |
| 1176-1550 | 14 | 16 | 19,5 | См. C.3.5 |  |
| 1 551-2 025 | 15 | 17 | 21 | См. C.3.5 |  |
| 2 026-2 675 | 16 | 18 | 22 | См. C.3.5 |  |
| 2 676-3 450 | 17 | 19 | 23 | См. C.3.5 |  |
| 3 451-4350 | 18 | 20 | 24 | См. C.3.5 |  |
| 4351-5450 | 19 | 21 | 25 | См. C.3.5 |  |
| 5 451-6 800 | 20 | 23 | 26 | См. C.3.5 |  |
| 6 801-8 500 | 21 | 25 | 27 | См. C.3.5 |  |
| 8501-10700 | 22 | 27 | 28 | См. C.3.5 |  |
| >10700 | Следуйте прогрессу выше | Следуйте прогрессу выше | Следуйте прогрессу выше | См. C.3.5 |  |

**C.3.5 Факторы для корректировки продолжительности аудита**

Таблица C.1 не должна использоваться изолированно. Выделенное время должно также учитывать следующие факторы, которые относятся к сложности СМИБ и, следовательно, к усилиям, необходимым для аудита СМИБ:

a) сложность СМИБ (например, критичность информации, риск, связанный с СМИБ и т. д.);

b) тип(ы) бизнеса, выполняемого в рамках СМИБ;

c) ранее продемонстрированная производительность СМИБ;

d) объем и разнообразие технологий, используемых при внедрении различных компонентов СМИБ (например, количество различных ИТ-платформ, количество разделенных сетей);

e) объем аутсорсинга и сторонних соглашений, используемых в рамках СМИБ;

f) объем разработки информационной системы;

g) количество сайтов и количество сайтов аварийного восстановления (DR);

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

i) для надзорного или повторного сертификационного аудита: объем и степень изменений, относящихся к СМИБ в соответствии с ISO/IEC 17021-1:2015, 8.5.3.

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

Примеры факторов, требующих добавления продолжительности аудита:

- сложная логистика процесса, включающая более одного здания или местоположения в области действия СМИБ;

- персонал, говорящий на нескольких языках (требующий переводчика(ов) или не позволяющий отдельным аудиторам работать независимо) или документация, предоставляемая на нескольких языках;

- виды деятельности, требующие посещения временных объектов для подтверждения деятельности постоянных объектов, система менеджмента которых подлежит сертификации (см. параграф ниже следующего списка);

- большое количество стандартов и правил, которые применяются к СМИБ.

Примеры факторов, допускающих вычитание времени аудита:

- отсутствие или низкий уровень риска процессов;

- процессы, включающие одну общую деятельность (например, только обслуживание);

- предварительные знания об организации (например, если организация уже была сертифицирована по другому стандарту тем же органом по сертификации);

- высокая готовность клиента к сертификации (например, уже сертифицирована или признана другой сторонней схемой);

- высокая зрелость системы менеджмента на месте.

В ситуациях, когда клиент или сертифицированная организация предоставляет свою продукцию или услуги на временных площадках, важно, чтобы оценки таких площадок были включены в программы сертификационного аудита и надзора.

Корректировки могут быть сделаны для вышеуказанных факторов. Факторы, требующие добавления или вычитания времени аудита, могут компенсировать друг друга. Во всех случаях, когда вносятся корректировки во время, указанное в таблице аудита C.1, необходимо сохранять достаточные доказательства и записи для обоснования отклонения.

**C.3.6 Ограничение отклонения продолжительности аудита**

Для обеспечения эффективного проведения аудитов и получения надежных и сопоставимых результатов время аудита, указанное в таблице времени аудита, не должно быть сокращено более чем на 30 %.

Необходимо установить и задокументировать соответствующие причины отклонения.

**C.3.7 Продолжительность аудита на месте**

Ожидается, что продолжительность, рассчитанная на планирование и написание отчета, в совокупности не должно, как правило, сокращать общее «время аудита» на месте (физическое/дистанционное) до менее чем 70 % от времени, рассчитанного в соответствии с C.3.3, C.3.4 и C.3.5. Если для планирования и/или написания отчета требуется дополнительное время, это не должно быть оправданием для сокращения времени аудита на месте. Время на поездки аудитора не включено в этот расчет и является дополнительным к времени аудита, указанному в таблице.

Примечание 1 - 70 % это фактор, основанный на опыте аудитов СМИБ.

Примечание 2 - Термин «(физический/дистанционный)» означает, что аудиты «на месте» (физических местоположений или электронных сайтов клиента) могут проводиться физически или удаленно (см. 9.2.3 и C.3.2). Для аудитов «на месте» см. также ISO/IEC 17021-1:2015, 9.4.1.

**C.4 Продолжительность аудита для аудитов надзора**

Для цикла аудита первоначальной сертификации продолжительности аудита для данной организации должно быть пропорционально времени, затраченному на первоначальный аудит, при этом общее количество времени, затрачиваемого ежегодно на надзор, должно составлять около 1/3 времени, затраченного на первоначальный аудит. Планируемое время надзора должно периодически пересматриваться, чтобы учитывать изменения, которые могут повлиять на продолжительность аудита. Время, затрачиваемое на аудит надзора, должно быть увеличено, чтобы обеспечить аудит изменений в СМИБ (например, аудит новых или измененных средств менеджмента информационной безопасности, процессов и услуг).

**C.5 Продолжительность аудита для аудита повторной сертификации**

Общее количество времени, потраченного на проведение аудита повторной сертификации, должно зависеть от результатов любого предыдущего аудита, как определено в 9.4.3 и ISO/IEC 17021-1:2015, 9.6.3. Продолжительность для аудита повторной сертификации должно быть пропорционально, но не менее двух третей, времени аудита, необходимого для первоначального сертификационного аудита той же организации во время аудита повторной сертификации.

**C.6 Продолжительность аудита нескольких площадок**

Как правило, общее время аудита для аудита на площадке должно рассчитываться с учетом общего количества лиц, выполняющих работу под контролем организации, независимо от их местонахождения.

В качестве альтернативы, по обоснованным причинам, которые должны быть задокументированы, разрешается суммировать время аудита, которое рассчитывается индивидуально для каждой площадки, при условии, что это общее время аудита больше, чем определенное 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 зафиксированы органом по сертификации.

Общее количество дней аудиторов на месте — рассчитанное для области действия в соответствии с процедурой, указанной в C.3.3 и C.3.4 и в настоящем пункте — должно быть распределено по различным площадкам на основе релевантности площадки для системы менеджмента, видов деятельности, проводимых на площадке, и выявленных рисков. Обоснование распределения должно быть зафиксировано органом по сертификации.

Любые сокращения должны применяться до сравнения времени аудита с общим временем аудита.

**C.7 Продолжительность аудита для расширения области действия**

Продолжительность аудита, необходимая для расширения области действия СМИБ, должно быть рассчитано с учетом таких факторов, как:

a) тип расширения:

b) вид деятельности текущей сертификации;

c) количество мест, где происходит вид деятельности;

d) сопутствующие риски информационной безопасности, связанные с видом деятельности;

e) количество элементов управления, относящихся к расширению;

f) количество лиц, выполняющих работу под контролем организации в новой области; и

g) время, необходимое для проверки интеграции расширенной области в СМИБ.

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

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

Время аудита должно быть добавлено к расчетной продолжительности для проверки СМИБ клиента. Это дополнительное время должно быть не менее:

1) 0,5 дн. (аудиторских дней), если аудит расширения области проводится совместно с надзорным аудитом или аудитом повторной сертификации.

2) 1,0 дн. (аудиторских дней), если аудит расширения области проводится как отдельный аудит.

**Приложение D**

*(информативное)*

**Методы расчета продолжительности аудита**

**D.1 Общие положения**

В приложении приведены дополнительные рекомендации 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 - Понятия в этом приложении начинаются после того, как были применены любые сокращения лиц, выполняющих определенные идентичные виды деятельности, как описано в C.3.4.

**D.2 Классификация факторов для расчета продолжительности аудита**

Таблица D.1 приводит примеры классификации основных факторов для расчета продолжительности аудита, как указано в C.3.5, a) по i). Эта классификация может использоваться органами сертификации для получения схемы расчета продолжительности аудита в соответствии с 9.1.4.2.

**Таблица D.1 — Классификация факторов для расчета продолжительности аудита**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Влияние на усилия | | |
| Сниженные усилия | Нормальные усилия | Повышенные усилия |
| Факторы (см. C.3.5) |  |  |  |
| а) сложность СМИБ:  - требования к информационной безопасности [конфиденциальность, целостность и доступность, (CIA)]  - количество критических активов  - количество процессов и услуг | - Только немного чувствительной или конфиденциальной информации, низкие требования к доступности  - Мало критических активов (с точки зрения CIA)  - Только один ключевой бизнес-процесс с несколькими интерфейсами и несколькими вовлеченными бизнес-подразделениями | - Более высокие требования к доступности или некоторая конфиденциальная информация  - Некоторые критически важные активы  - 2-3 простых бизнес-процесса с несколькими интерфейсами и несколькими вовлеченными бизнес-подразделениями | - Более высокий объем конфиденциальной или конфиденциальной информации (например, здоровье, личная информация, страхование, банковское дело) или высокие требования к доступности  - Множество критических активов  - Более 2 сложных процессов с большим количеством интерфейсов и вовлеченных бизнес-подразделений |
| b) тип(ы) бизнеса, осуществляемого в рамках СМИБ | - бизнес с низкимуровнем рисков, без регулятивных требований | - Высокие нормативные требования | - Высокорисковый бизнес с (только) ограниченными нормативными требованиями |
| c) ранее продемонстрированная эффективность СМИБ | - Недавно сертифицированный  - Не сертифицирован, но СМИБ полностью внедрена в течение нескольких циклов аудита и улучшения, | - Недавний надзорный аудит  - Не сертифицирована, но частично внедрена СМИБ: Некоторые инструменты системы менеджмента доступны и внедрены; некоторые | - Нет сертификации и недавних аудитов  - СМИБ новая и не полностью внедрена (например, отсутствие механизмов контроля, специфичных для системы менеджмента, |

***Продолжение Таблица D.1***

|  |  |  |  |
| --- | --- | --- | --- |
|  | Влияние на усилия | | |
| Сниженное усилие | Сниженное усилие | Сниженное усилие |
|  | включая документированные внутренние аудиты, обзоры руководства и эффективную систему постоянного улучшения | процессы постоянного улучшения внедрены, но частично задокументированы | незрелые процессы постоянного улучшения, выполнение процессов ad hoc) |
| d) объем и разнообразие технологий, используемых при внедрении различных компонентов СУИБ (например, количество различных ИТ-платформ, количество отдельных сетей) | - Высокостандартизированная среда с низким разнообразием (мало ИТ-платформ, серверов, операционных систем, баз данных, сетей и т. д.) | - Стандартизированные, но разнообразные ИТ-платформы, серверы, операционные системы, базы данных, сети | - Высокая степень разнообразия или сложности ИТ (например, множество различных сегментов сетей, типов серверов или баз данных, количество ключевых приложений) |
| e) объем аутсорсинга и сторонних соглашений, используемых в рамках СУИБ | - Отсутствие аутсорсинга и малая зависимость от поставщиков или  - Четко определенные, управляемые и контролируемые соглашения об аутсорсинге  - Аутсорсер имеет сертифицированную СМИБ  - Имеются соответствующие независимые отчеты о гарантиях | - Несколько частично управляемых соглашений об аутсорсинге | - Высокая зависимость от аутсорсинга или поставщиков с большим влиянием на важные бизнес-процессы, или  - Неизвестный объем или степень аутсорсинга, или Несколько неуправляемых соглашений об аутсорсинге |
| f) объем разработки информационной системы | - Отсутствие внутренней разработки системы  - Использование стандартизированных программных платформ | - Использование стандартизированных программных платформ со сложной конфигурацией/параметризацией  - (Высоко) настраиваемое программное обеспечение  - Некоторые виды деятельности по разработке (внутрифирменные или аутсорсинговые) | - Обширная внутренняя деятельность по разработке программного обеспечения с несколькими текущими проектами для важных бизнес-целей |
| g) количество сайтов и количество сайтов аварийного восстановления (DR) | - Низкие требования к доступности и отсутствие или наличие одного сайта DR | - Требования к средней или высокой доступности и отсутствие или один сайт DR | - Требования высокой доступности, например, круглосуточные услуги  - Несколько площадок DR  - Несколько центров обработки данных |

***Окончание Таблица D.1***

|  |  |  |  |
| --- | --- | --- | --- |
|  | Влияние на усилия | | |
| Сниженные усилия | Нормальные усилия | Повышенные усилия |
| h) количество и сложность элементов управления | - Меньшее, чем обычно, количество элементов управления, при этом некоторые общие области контроля не включены — например, отсутствуют элементы управления разработкой систем или физические элементы управления | - Типичное количество и сложность элементов управления | - Больше, чем обычно, количества подробных и сложных элементов управления, например, много элементов управления, связанных с сетевыми протоколами или криптографией |
| i) для аудита надзора или повторной сертификации: объем и объем изменений, относящихся к СМИБ в соответствии с ISO/IEC 17021-1:2015, 8.5.3 | - Никаких изменений с момента последнего аудита повторной сертификации | - Незначительные изменения в области действия или SoA СМИБ, например, некоторые политики, документы  - Незначительные изменения в факторах, указанных выше | - Значительные изменения в области действия или SoA СМИБ, например, новые процессы, новые бизнес-подразделения, области, методология управления оценкой рисков, политики, документация, обработка рисков  - Значительные изменения в факторах, указанных выше |

**D.3 Пример расчета продолжительности аудита**

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

Шаг 1: Определение факторов, связанных с бизнесом и организацией (кроме ИТ): Определите подходящую оценку для каждой из категорий, указанных в Таблице D.2, и просуммируйте результаты.

Шаг 2: Определение факторов, связанных с ИТ-средой: Определите подходящую оценку для каждой из категорий, указанных в Таблице D.3, и просуммируйте результаты.

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

Шаг 4: Окончательный расчет: Количество дней, определенное путем применения диаграммы времени аудита (Таблица C.1), умножается на коэффициент, полученный в результате Шага 3. При использовании многосайтовой выборки рассчитанные дни аудита увеличиваются на основе усилий, необходимых для выполнения плана многосайтовой выборки.

Данный результат — окончательное количество дней аудита.

**Таблица D.2 — Факторы, связанные с бизнесом и организацией (кроме ИТ)**

|  |  |
| --- | --- |
| **Категория** | **Уровень** |
| Тип(ы) бизнеса и нормативные требования | 1. Организация работает в некритических секторах бизнеса и нерегулируемых секторах a  2. Организация имеет клиентов в критических секторах бизнеса a  3. Организация работает в критических секторах бизнеса a |
| Процесс и задачи | 1. Стандартные процессы со стандартными задачами; небольшое количество продуктов или услуг  2. Стандартные, но неповторяющиеся процессы с большим количеством продуктов или услуг  3. Сложные процессы, большое количество продуктов и услуг, много бизнес-единиц, включенных в область сертификации (СМИБ охватывает очень сложные процессы или относительно большое количество или уникальные виды деятельности) |
| Уровень создания системы менеджмента | 1. СМИБ уже хорошо внедрена и/или существуют другие системы менеджмента  2. Некоторые элементы других систем менеджмента внедрены, другие нет  3. Никакая другая система менеджмента не внедрена вообще, СМИБ новая и не внедрена |
| a Критически важные секторы бизнеса — это секторы, которые могут повлиять на критически важные государственные услуги, создать риск для здоровья, безопасности, экономики, репутации и способности правительства функционировать, а также могут оказать существенное негативное воздействие на страны. | |

**Таблица D.3 — Факторы, связанные с ИТ-средой**

|  |  |
| --- | --- |
| **Категория** | **Уровень** |
| Сложность ИТ-инфраструктуры | 1. Мало или очень стандартизировано ИТ-платформ, серверов, операционных систем, баз данных, сетей и т. д.  2. Несколько различных ИТ-платформ, серверов, операционных систем, баз данных, сетей  3. Множество различных ИТ-платформ, серверов, операционных систем, баз данных, сетей |
| Зависимость от аутсорсинга и поставщиков, включая облачные сервисы | 1. Незначительная или нулевая зависимость от аутсорсинга или поставщиков  2. Некоторая зависимость от аутсорсинга или поставщиков, связанная с некоторыми, но не со всеми важными видами деятельности  3. Высокая зависимость от аутсорсинга или поставщиков, большое влияние на важные виды деятельности |
| Разработка информационных систем | 1. Отсутствие или очень ограниченная внутренняя разработка систем/приложений  2. Некоторая внутренняя или аутсорсинговая разработка систем/приложений для некоторых важных бизнес-целей  3. Обширная внутренняя или аутсорсинговая разработка систем/приложений для важных бизнес-целей |

**Таблица D.4 — Влияние факторов на время аудита**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **IT-сложность** | | |
| **Низкая (от 3 до 4)** | **Средняя (от 5 до 6)** | **Высокая (от 7 до 9)** |
| **Бизнес-сложность** | Высокий (от 7 до 9) | от +5 % до +20 % | от +10 % до +50 % | от +20 % до +100 % |
| Средний (от 5 до 6) | от -5 % до -10 % | 0 % | от +10 % до +50 % |
| Низкий (от 3 до 4) | от -10 % до -30 % | от -5 % до -10 % | от +5 % до +20 % |

Пример 1 - Организация, подлежащая аудиту, насчитывает 700 сотрудников, поэтому, согласно Таблице C.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 и 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 даст никакой корректировки для времени аудита.

Пример 2 - Используя ту же организацию, что и в примере 1, за исключением того, что несколько систем менеджмента уже внедрены и СМИБ уже хорошо отлажена, можно изменить расчет согласно таблице D.2 на 1+1+1 = 3. Согласно таблице D.4, это приведет к сокращению времени аудита на 5–10 %, т. е. время аудита сократится на 1–1,5 дня, что в общей сложности составит 16–16,5 дней.

**Приложение E**

*(информативное)*

**Руководство по обзору внедренных элементов управления ISO/IEC 27001:2022, Приложение A**

**E.1 Цель**

В соответствии с требованием в 9.3.2.2 f), реализация элементов управления, которые были определены как необходимые клиентом для СМИБ (согласно Заявлению о применимости), должна быть проверена на этапе 2 первоначального аудита и во время надзора или повторной сертификации. Обзоры предназначены для определения того, внедрены ли элементы 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 элементы управления необходимы организации, или даже если они описаны с использованием того же текста элемента управления, что и в ISO/IEC 27001:2022, Приложение A. Орган по сертификации также не знает взаимосвязи между элементами управления информационной безопасностью или взаимосвязи между элементами управления информационной безопасностью и процессами организации. Таким образом, первоначальный аудит может быть ограничен аудитом отдельных элементов управления, тогда как последующие аудиты могут использовать более эффективный подход аудита элементов 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 элементы управления с теми, что указаны в ISO/IEC 27001:2022, Приложение A, и, следовательно, существует связь между необходимыми элементами управления организации и теми, что указаны в ISO/IEC 27001:2022, Приложение A. Руководство, приведенное в Таблице E.1, призвано помочь органу по сертификации в разработке планов аудита для учета необходимых элементов управления, определенных клиентом, с учетом их связи с элементами управления в ISO/IEC 27001:2022, Приложение A.

**E.2 Как использовать Таблицу E.1**

**E.2.1 Общие положения**

В Таблице E.1 приведены примеры рекомендаций по проверке необходимых элементов управления. Здесь использованы средства контроля, перечисленные в ISO/IEC 27001:2022, Приложение A, но аудиторы должны использовать взаимосвязь между этими средствами контроля и необходимыми средствами контроля организации для интерпретации руководства, приведенного в Таблице E.1, для сбора аудиторских доказательств с целью демонстрации эффективности средств контроля.

Примечание Таблица E.1 не предназначена для предоставления руководства по проверке средств контроля, не связанных с теми, которые указаны в ISO/IEC 27001:2022, Приложение A.

Большинство средств контроля содержат организационные аспекты, которые могут быть подтверждены, например, путем изучения документации клиента по средствам контроля, процессам или процедурам, интервью или наблюдения.

Многие средства контроля основаны на правилах, установленных организацией-клиентом. Такие правила могут быть в форме политик, специфичных для конкретных тем, требований к процессам или процедурам или других типов правил, которые доводятся до сведения персонала. В Таблице E.1 используется общий термин «правила» для обозначения таких требований или ожиданий, установленных руководством организации-клиента.

Многие средства контроля можно проверить путем выборочного тестирования, т. е. путем проверки выборки результатов контрольной деятельности.

**E.2.2 Столбец «тестирование системы»**

Многие элементы управления в ISO/IEC 27001:2022, Приложение A, реализованы как технологические элементы управления, например, через определенные системные настройки, конфигурации или функциональность технологии. Доказательства эффективности технологических элементов управления часто можно собрать с помощью системного тестирования или с помощью специализированных инструментов аудита или отчетности. Системное тестирование означает прямой обзор информационных систем: аудитор может просматривать системные настройки и конфигурации или оценивать результаты инструментов тестирования. Если у клиента есть инструменты, которые известны аудитору, они также могут использоваться для поддержки аудита, или аудитор может просматривать результаты оценки, выполненной клиентом.

В столбце «тестирование системы» в Таблице E.1 приведены рекомендации по обзору технологических элементов управления:

— «пусто» означает, что системное тестирование обычно неприменимо или не является необходимым при аудите СМИБ;

— «возможно» означает, что системное тестирование обычно возможно для оценки внедрения элемента управления, но может не быть необходимым при аудите СМИБ;

— «рекомендуется» означает, что системное тестирование обычно необходимо при аудите СУИБ.

**E.2.3 Столбец «визуальный осмотр»**

Другие элементы управления в ISO/IEC 27001:2022, Приложение A, могут быть рассмотрены посредством «визуального осмотра» на месте для оценки их внедрения и эффективности. Полагаться на рассмотрение соответствующей документации на бумаге или интервью недостаточно, поэтому аудитор должен рассмотреть возможность проверки элемента управления на месте, где он внедрен.

Примечание Визуальный осмотр на месте также может быть достигнут с использованием методов удаленного осмотра, например, при наличии человека на месте с видеопотоком в реальном времени для аудитора.

Столбец «визуальный осмотр» в Таблице E.1 содержит руководство по проверке физических доказательств элементов управления:

— «пусто» означает, что визуальный осмотр обычно не применим или не требуется при аудите СМИБ;

**Таблица E.1 — Оценка средств контроля**

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 5 Организационный контроль |  |  |  |
| 5.1 Политика информационной безопасности |  |  | - Политика информационной безопасности  - Политики информационной безопасности по конкретным темам, которые организация считает необходимыми  - Распространение политик среди соответствующего персонала и заинтересованных сторон |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение******Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 5.2 Роли и обязанности по информационной безопасности |  |  | - Распределенные роли и обязанности по внедрению, эксплуатации и менеджменту информационной безопасности |
| 5.3 Разделение обязанностей |  |  | - Выявлены конфликтующие обязанности или сферы ответственности и соответствующие правила разделения |
| 5.4 Управленческие обязанности |  |  | - Заявления руководства и поддержка целей, политик, процедур информационной безопасности и т. д.  - Упоминание личной ответственности персонала за информационную безопасность |
| 5.5 Контакты с органами власти |  |  | - Определенные контактные лица с соответствующими органами  - Правила сообщения об инцидентах  - Содержание информационного потока от и к соответствующим органам |
| 5.6 Контакты с группами особых интересов |  |  | - Членство и определенные контактные лица с группами особых интересов или другими форумами и ассоциациями [например, группы реагирования на компьютерные чрезвычайные ситуации (CERT), агентства по кибербезопасности]  - Правила относительно того, что может обсуждаться в таких организациях  - Содержание информационного потока от таких организаций и в них |
| 5.7 Анализ угроз |  |  | - Подход к сбору соответствующей информации об угрозах  - Анализ информации об угрозах в отношении организации и ее распространение среди соответствующих сторон |
| 5.8 Информационная безопасность в управлении проектами |  |  | - Установленная информационная безопасность в управлении проектами на протяжении всего жизненного цикла проекта, например, при определении требований, тестировании  - Для выборки проектов выявлены риски информационной безопасности и соответствующая обработка рисков |
|  |  |  |  |
| ***Продолжение******Таблица E.1*** | | | |
| 5.9 Инвентаризация информации и других связанных активов | возможно |  | - Инвентаризации информации и других связанных активов, поддерживаемые СМИБ  - Поддерживаемые права собственности на активы в инвентаризациях активов  - Правила для обязанностей владельца активов, например, классификация |
| 5.10 Допустимое использование информации и других связанных активов |  |  | - Документированные правила приемлемого 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 трудовых отношений, контракта или соглашения  - Образец задокументированных записей о возврате |
| 5.12 Классификация информации |  |  | - Правила и схема классификации информации, например, в тематической политике  - Образец информации из различных источников, которая должна быть классифицирована |
| 5.13 Маркировка информации |  | возможно | - Правила маркировки информации и других связанных активов  - Процедуры маркировки определенных типов информации и других связанных активов |
| 5.14 Передача информации | возможно |  | - Правила передачи информации, например, в тематической политике  - Определение вариантов использования передачи информации, определенных в СМИБ, и соответствующих правил, процедур или соглашений, охватывающих, например, физическую, электронную или устную передачу  - Примеры реализованных процедур или соглашений по передаче информации |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение******Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 5.15 Контроль доступа | возможно |  | - Правила контроля физического и логического доступа к информации и другим связанным активам, например, в тематической политике контроля доступа  - Выдержки (образцы) прав доступа для высокорискованного физического или логического доступа к информации и другим активам, проверенные на соответствие вышеуказанным правилам |
| 5.16 Управление идентификацией |  |  | - Процедуры управления идентификациями, присвоенными лицам или нечеловеческим сущностям на протяжении жизненного цикла |
| 5.17 Информация об аутентификации | рекомендуется |  | - Описание процесса распределения и управления информацией аутентификации  - Инструкции для пользователей по правильному обращению с информацией, используемой для аутентификации  - При использовании паролей настройки безопасности (например, длина, сложность, ротация) систем управления паролями |
| 5.18 Права доступа | рекомендуется |  | - Правила контроля доступа, например, в тематической политике контроля доступа (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 тематической политике по использованию 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) |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение******Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 5.20 Решение вопросов информационной безопасности в соглашениях с поставщиками |  |  | - Реестр соглашений с внешними сторонами, связанных с типом отношений с поставщиками  - Договоры с поставщиками (пример) с соответствующими требованиями по информационной безопасности и Соглашениями об уровне обслуживания |
| 5.21 Менеджмента информационной безопасности в цепочке поставок информационно-коммуникационных технологий (ИКТ) |  |  | - Правила обеспечения информационной безопасности при приобретении продуктов или услуг ИКТ  - Практики управления рисками информационной безопасности цепочки поставок ИКТ  - Результаты проведенного анализа рисков, т. е. смягчающие меры контроля для выборки конкретных цепочек поставок ИКТ |
| 5.22 Мониторинг, обзор и управление изменениями в услугах поставщиков |  |  | - Процессы управления изменениями в практиках информационной безопасности поставщиков и предоставлении услуг  - Планы регулярного мониторинга, проверки, оценки практики информационной безопасности поставщиков (например, посредством отчетов об услугах, аудитов поставщиков)  - Результаты мониторинга и проверки деятельности, включая планы действий |
| 5.23 Информационная безопасность при использовании облачных сервисов |  |  | - Правила управления рисками информационной безопасности в облачных сервисах, например, в тематической политике использования 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 |
| ***Продолжение Таблица E.1*** | | | |
| 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 соответствующие им меры реагирования на инциденты |
| 5.27 Извлечение уроков из инцидентов информационной безопасности |  |  | - Записи произошедших инцидентов информационной безопасности, включая типы, объемы и понесенные затраты  - Уроки, извлеченные из анализа инцидентов информационной безопасности, например, усовершенствования плана управления инцидентами, улучшение контроля и мероприятий по повышению осведомленности |
| 5.28 Сбор доказательств |  |  | - Процедуры работы с доказательствами, связанными с инцидентами информационной безопасности, например, для идентификации, сбора, приобретения и сохранения |
| 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 на основе анализа влияния на бизнес  - Планы непрерывности ИКТ  - Результаты регулярных тестов непрерывности ИКТ |
| 5.31 Юридические, законодательные, нормативные и договорные 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 договорные требования, имеющие отношение к информационной безопасности, в частности, в отношении использования криптографии в любой форме |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | | Ч |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 5.32 Права интеллектуальной собственности |  |  | - Правила управления правами интеллектуальной собственности, например, в тематической политике  - Процедуры обработки авторских прав на документы, прав на дизайн, товарных знаков, патентов и лицензий на исходный код и соответствующих инвентарей |
| 5.33 Защита записей | рекомендуется |  | - Правила управления записями, связанные с применимыми законами, нормативными актами и договорными требованиями, например, в тематической политике  - Процедуры хранения, обработки цепочки поставок, сохранения и утилизации записей  - Конфигурация систем хранения данных для обеспечения требований к управлению записями (например, сохранение, сохранение) |
| 5.34 Конфиденциальность и защита персональной идентифицируемой информации (PII) |  |  | - Правила обработки персонально идентифицируемой информации (PII), например, в тематической политике  - 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 договорные 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 |
| 5.35 Независимая проверка информационной безопасности |  |  | - Планы проведения независимых проверок информационной безопасности  - Отчетность о результатах независимых проверок (выборка) высшему руководству  - Корректирующие действия, предпринимаемые в случаях, когда подход организации к менеджменту информационной безопасности оказывается неадекватным |
| 5.36 Соблюдение политик, правил и стандартов информационной безопасности |  |  | - Планы проверки соответствия организации политике информационной безопасности, тематически-специфическим политикам, правилам и стандартам  - Результаты таких проверок (выборка) и предпринятые корректирующие действия |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 5.37 Документированные рабочие процедуры |  |  | - Процедуры эксплуатации объектов обработки информации, имеющие отношение к информационной безопасности |
| 6 Контроль персонала |  |  |  |
| 6.1 Проверка |  |  | - Правила и процесс проверки биографических данных с учетом применимых законов, правил и этики  - Проверка биографических данных, проводимая для выборки новых сотрудников и текущего персонала по мере необходимости (например, повышение по службе, конфиденциальные профили должностей) |
| 6.2 Условия трудоустройства |  |  | - Общие правила или общие положения и условия, связанные с обязанностями по обеспечению информационной безопасности, например, кодекс поведения  - Принятие положений и условий, касающихся информационной безопасности персоналом  - Пример конкретных обязанностей по обеспечению информационной безопасности, согласованных персоналом с критически важными ролями (например, имеющим доступ к конфиденциальной информации или привилегированный доступ к системам) |
| 6.3 Осведомленность, образование и обучение в области информационной безопасности |  |  | - Программа повышения осведомленности, образования и обучения в области информационной безопасности, включающая специальное содержание для важных целевых групп  - Список участников проведенных тренингов по информационной безопасности  - Ответы из интервью с выборкой участников об ожидаемом поведении |
| 6.4 Дисциплинарный процесс |  |  | - Официальная дисциплинарная процедура, доведенная до сведения персонала и других заинтересованных сторон |
| 6.5 Обязанности после увольнения или смены работы |  |  | - Подписанное принятие персоналом конкретных обязанностей и ответственности, действительное после ухода из компании или смены работы |
| 6.6 Соглашения о конфиденциальности или неразглашении |  |  | - Подписанные соглашения о конфиденциальности персоналом и другими соответствующими заинтересованными сторонами |
| ***Продолжение Таблица E.1*** | | | |
| 6.7 Удаленная работа | возможно |  | - Правила удаленной работы, например, в тематической политике  - Примеры мер физической и коммуникационной безопасности  - Проектирование защищенных устройств обработки информации, разрешенных для удаленного использования [например, «Принеси свое устройство» (BYOD), ноутбуки] |
| 6.8 Отчетность о событиях информационной безопасности |  |  | - Механизм сообщения о событиях информационной безопасности, которые могут быть идентифицированы персоналом  - Инструкции или сообщения для повышения осведомленности о сообщениях о событиях информационной безопасности |
| **7 Physical controls** |  |  |  |
| 7.1 Физические периметры безопасности |  | возможно | - Правила построения безопасных зон и прочности физических барьеров  - Физический периметр безопасности и проектирование безопасной зоны для каждого соответствующего места |
| 7.2 Физический вход | возможно | рекомендуется | - Система авторизации доступа (физическая или электронная) для точек входа в защищенные 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 конфиденциальной информации |
| 7.4 Мониторинг физической безопасности | возможно | возможно | - Проектирование систем физического наблюдения для обнаружения несанкционированного физического доступа  - Защита систем мониторинга  - Журналы, генерируемые при работе систем физического наблюдения |
| 7.5 Защита от физических и экологических угроз |  | рекомендуется | - Результаты оценки рисков физических и экологических угроз  - Разработка соответствующих мер защиты от физических и экологических угроз |
| 7.6 Работа в безопасных зонах |  | возможно | - Правила работы в безопасных зонах (с указанием конкретных мер безопасности)  - Реализованные меры безопасности для безопасных зон |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 7.7 Чистый стол и чистый экран |  | рекомендуется | - Правила для чистого стола и чистого экрана, например, в тематической политике  - Выборочные проверки поведения чистого стола и чистого 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 принципы BYOD)  - Результаты интервью или опросов, проведенных среди персонала, использующего активы за пределами помещений организации |
| 7.10 Носители информации | возможно |  | - Правила использования съемных носителей информации, например, в тематической политике  - Конфигурации устройств для ограничения или защиты передачи информации со съемных носителей информации и на них (включая, например, шифрование)  - Процессы безопасной утилизации и записи таких процессов |
| 7.11 Поддерживающие коммунальные услуги |  | рекомендуется | - Установленные меры защиты коммунальных служб, особенно в центрах обработки данных (например, температура, электроснабжение, водоснабжение)  - Аварийные положения для отключения электроэнергии, воды, газа или других коммунальных служб |
| 7.12 Безопасность кабелей |  | Возможно | * Физическая прокладка и защита кабелей |
| 7.13 Техническое обслуживание оборудования |  |  | - Процедуры обслуживания различных типов оборудования  — Записи по обслуживанию оборудования |
| 7.14 Безопасная утилизация или повторное использование оборудования | возможно | возможно | - Правила утилизации или повторного использования оборудования, содержащего носители информации  - Записи о физическом или логическом уничтожении информации или оборудования |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 8 Технологические средства контроля |  |  |  |
| 8.1 Пользовательские конечные устройства | возможно |  | - Правила безопасной конфигурации и обработки пользовательских конечных устройств, например, в тематической политике  - 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 тематической политике  - Процессы авторизации и проверки для управления привилегированными правами доступа |
| 8.3 Ограничение доступа к информации | рекомендуется |  | - Правила ограничения доступа к информации и другим связанным активам, например, в тематической политике  - Методы и процессы управления доступом для защиты доступа к конфиденциальной информации на протяжении всего ее жизненного цикла (т. е. создание, обработка, хранение, передача, утилизация) |
| 8.4 Доступ к исходному коду | рекомендуется |  | - Процедуры управления доступом на чтение и запись к исходному коду, инструментам разработки и библиотекам программного обеспечения |
| 8.5 Безопасная аутентификация | рекомендуется |  | — Правила по технологиям аутентификации и процедурам контроля доступа, например, в тематической политике  — Решения на основе риска и соответствующие  –– Реализации процедур входа в систему для систем или приложений  — Использование строгой или многофакторной аутентификации для критически важных информационных систем |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 8.6 Управление емкостью | возможно |  | - Текущие и ожидаемые требования к мощности  - Измерения использования ресурсов, например, средств обработки информации, человеческих ресурсов, офисов и других объектов  - Процедуры либо обеспечения достаточной мощности, либо снижения требований к мощности |
| 8.7 Защита от вредоносных программ | рекомендуется |  | - Правила защиты от вредоносных программ  - Покрытие активов на основе риска и соответствующая конфигурация программного обеспечения для обнаружения вредоносных программ  - 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 | рекомендуется |  | - Сбор и управление информацией о технических уязвимостях используемых информационных систем  - Результаты сканирования уязвимостей (регулярно выполняемого) или тестов на проникновение  - Оценки, выполненные в отношении подверженности организации техническим уязвимостям и запланированные меры по их смягчению  - Процесс обновления программного обеспечения для обеспечения установки самых последних одобренных исправлений и обновлений приложений |
| 8.9 Управление конфигурацией | рекомендуется |  | - Правила конфигураций, включая конфигурации безопасности, оборудования, программного обеспечения, услуг и сетей  - Процессы управления, внедрения или применения, мониторинга и проверки конфигураций  - Стандартные шаблоны для безопасной конфигурации оборудования, программного обеспечения, услуг и сетей (т. е. укрепление) |
| 8.10 Удаление информации |  |  | - Правила своевременного удаления информации, хранящейся в информационных системах, устройствах или на любых других носителях, например, в соответствии с политикой по хранению данных, относящейся к конкретной теме |
| ***Продолжение Таблица E.1*** | | | |
|  |  |  | - Процедуры безопасного удаления конфиденциальной информации в системах, приложениях и службах  - Соглашения со сторонними организациями с положениями об удалении информации, где третьи стороны хранят информацию организации |
| 8.11 Маскировка данных |  |  | - Правила маскировки данных, например, в соответствии с политикой организации по контролю доступа, относящейся к конкретной теме  - Результаты анализов, проведенных для определения того, где защита конфиденциальной информации (например, PII) требует таких методов, как маскировка данных, псевдонимизация или анонимизация  - Методы, используемые для маскировки данных, псевдонимизации или анонимизации |
| 8.12 Предотвращение утечки данных | возможно |  | - Правила по мерам предотвращения 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 | рекомендуется |  | - Правила резервного копирования информации, программного обеспечения и систем, например, в тематической политике резервного копирования  - Планы резервного копирования, основанные на установленных бизнес-требованиях организации  - Операционные процедуры для мониторинга своевременного и правильного выполнения резервного копирования и устранения сбоев  - Тесты восстановления резервных копий, проводимые через регулярные промежутки времени |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
| 8.14 Резервирование средств обработки информации |  |  | - Определены требования к доступности бизнес-сервисов и информационных систем  - Архитектура систем с высокими требованиями, обеспечивающая соответствующую избыточность  - Результаты проведенных испытаний отказоустойчивости |
| 8.15 Ведение журнала | рекомендуется |  | - Правила относительно цели создания журналов, какие данные собираются, и любые специфические для журналов требования к обработке данных журнала, например, в тематической политике по ведению журналов  - Список журналов, имеющих отношение 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 Мониторинговая деятельность | возможно |  | - Правила мониторинга сетей, систем и приложений на предмет аномального поведения  - Установленные базовые показатели нормального поведения и выведенные критерии для срабатывания оповещений  - Журналы мониторинга, поддерживаемые в течение определенных периодов хранения  - Результаты анализа, выполненного для выявления аномального поведения |
| 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 контроля таких служебных программ |
| 8.19 Установка программного обеспечения на операционные системы | возможно |  | — Процедуры и меры, используемые для управления установкой программного обеспечения в операционных системах, включая инвентаризацию установленного программного обеспечения с версиями |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
|  |  |  | - Правила относительно того, какие типы программного обеспечения могут устанавливать пользователи  - Ограничения на установку программного обеспечения лицами, не являющимися обученными администраторами |
| 8.20 Безопасность сетей | рекомендуется |  | - Правила обеспечения безопасности информации в сетях и защиты подключенных услуг от несанкционированного доступа  - Меры и функции безопасности, реализованные для защиты информации в сетях и поддерживающих их средствах обработки информации, например, шаблоны конфигурации, конфигурация криптографических средств управления, наборы правил шлюзов, пример конфигурации сетевых устройств  - Документация по архитектуре сети (схемы, файлы конфигурации, сегрегация)  - Правила аутентификации подключений систем к сети |
| 8.21 Безопасность сетевых служб |  |  | - Правила безопасного использования сетей и сетевых служб  - Список сетей и сетевых служб, используемых с механизмами безопасности и уровнями обслуживания  - Гарантии, полученные от поставщиков сетевых услуг |
| 8.22 Разделение сетей |  |  | - Правила разделения сетевых доменов, основанные, например, на уровнях доверия, критичности и чувствительности, а также в соответствии с политикой управления доступом, специфичной для данной темы  - Топология сети (включая беспроводную) и разделение зон с описанием назначения и правил  - Определения периметров безопасности сетевых доменов  - Процессы управления периметрами безопасности сетевых доменов, а также правила брандмауэра |
| 8.23 Веб-фильтрация | возможно |  | - Правила безопасного и надлежащего использования онлайн-ресурсов, включая любые ограничения на нежелательные или ненадлежащие веб-сайты |
| ***Продолжение Таблица E.1*** | | | |
|  |  |  | - 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 | рекомендуется |  | - Правила эффективного использования криптографии, включая приемлемые шифры и управление ключами, например, в тематической политике по криптографии  - Список криптографических методов, используемых организацией  - Стандарты, процедуры и методы управления ключами, включая генерацию, хранение, архивацию, извлечение, распространение, изъятие и уничтожение криптографических ключей |
| 8.25 Безопасный жизненный цикл разработки | возможно |  | - Правила безопасной разработки программного обеспечения для обеспечения того, чтобы информационная безопасность была разработана и реализована в рамках безопасного жизненного цикла разработки  - Разделение между средами разработки, тестирования и производства  - Процессы безопасности и контрольные точки, обеспечивающие адекватное покрытие требований информационной безопасности в течение всей разработки программного обеспечения  - Получение гарантий надлежащего выполнения требований информационной безопасности, когда разработка программного обеспечения передается на аутсорсинг |
| 8.26 Требования безопасности приложений |  |  | - Процесс определения требований безопасности приложений на основе оценки конкретных рисков  - Проведенные оценки рисков приложений, в которых указаны конкретные требования информационной безопасности  - Требования, определенные для выборки последних разработок/реализаций приложений, в частности для транзакционных услуг, приложений электронного заказа и оплаты |
| 8.27 Безопасная архитектура системы и принципы проектирования |  |  | - Архитектура и принципы проектирования безопасности, установленные для обеспечения безопасности информационных систем, разработанных, внедренных и эксплуатируемых в рамках жизненного цикла разработки |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Продолжение Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
|  |  |  | - Интеграция принципов проектирования безопасности в разработку программного обеспечения  - Пример реализации безопасности 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 обеспечения применения принципов безопасного кодирования во время планирования и перед кодированием, во время кодирования, а также во время проверки и обслуживания  - Применение конкретных принципов безопасного кодирования для образцов недавних разработок, включая методы сканирования кода  - Механизмы защиты кода, включая ограничения доступа |
| 8.29 Тестирование безопасности при разработке и приемке | рекомендуется |  | - Правила тестирования безопасности для проверки соблюдения требований информационной безопасности при развертывании приложений или кода в производственной 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 о том, как меры информационной безопасности, требуемые организацией, должны быть реализованы при разработке аутсорсинговых систем  - Процедуры, внедренные для руководства, мониторинга и проверки деятельности, связанной с разработкой аутсорсинговых систем |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

***Окончание Таблица E.1***

|  |  |  |  |
| --- | --- | --- | --- |
| Средства контроля в ISO/IEC 27001:2022, Приложение A a | Системное тестирование | Визуальный осмотр | Возможные доказательства разработки и внедрения средств контроля |
|  |  |  | - Результаты мониторинга или проверки поставщиков для обеспечения соответствия ожиданиям |
| 8.31 Разделение сред разработки, тестирования и производства | возможно |  | - Правила для уровня разделения между средами производства, тестирования и разработки, включая особые требования к различным средам разработки  - Разделение между средами разработки, тестирования и производства  - Защита сред тестирования и производства (например, ограничения доступа, сетевое разделение, обеспечение того, чтобы не использовалась конфиденциальная производственная информация) |
| 8.32 Управление изменениями | рекомендуется |  | - Правила управления изменениями для сохранения информационной безопасности  - Процедуры контроля изменений, например, документация, спецификация, тестирование, контроль качества и управляемая реализация  - 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 при ее использовании в целях тестирования (например, маскировка)  - Примеры удаления информации из тестовых сред |
| 8.34 Защита информационных систем во время аудиторского тестирования | возможно |  | - Список запросов на аудиторские тесты или другие мероприятия по обеспечению гарантий, включающие оценку операционных систем  - Примеры проведенных аудиторских тестов и то, как они были согласованы и проведены |
| a Числа, указанные в этом столбце, соответствуют контрольным числам в ISO/IEC 27001:2022, Приложение A. | | | |

**Приложение В.А**

*(информационное)*

**Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств**

**Таблица В.А.1 - Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств**

|  |  |  |
| --- | --- | --- |
| Обозначение и наименование ссылочного международного, стандарта | Степень соответствия | Обозначение и наименование национального стандарта, межгосударственного стандарта |
| ISO/IEC 17021-1:2015, Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1: Требования | IDT | СТ РК ISO/IEC 17021-1-2015 «Оценка соответствия требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования» (ISO/IEC 17021-1:2015) |
| ISO/IEC 27001:2022, Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования | IDT | СТ РК ISO/IEC 27001-2023 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования.  (ISO/IEC 27001:2022) |

**Библиография**

[1] ISO 19011 Руководство по аудиту систем управления (Guidelines for auditing management systems).

[2] ISO/IEC 27000 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь (Information technology — Security techniques — Information security management systems — Overview and vocabulary).

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

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

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

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

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

[8] ISO Guide 731) Управление рисками. Словарь (Risk management — Vocabulary).

[9] IAF MD5 Определение времени аудита качества, окружающей среды и Системы управления охраной труда и техникой безопасности, https://iaf.nu/en/iaf-documents/?cat\_id = 7, Последний просмотр: 2023-07-31 (Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems).

**МКС 35.030; 03.120.20 (IDT)**

**Ключевые слова:** информационная технология, аудит, система менеджмента, качество, безопасность

**МКС 35.030; 03.120.20 (IDT)**

**Ключевые слова:** информационная технология, аудит, система менеджмента, качество, безопасность

**Разработчик:**

**РГП на ПХВ «Казахстанский институт стандартизации и метрологии» Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан**

Руководитель

Департамента разработки

стандартов и фонда НТД А. Сопбеков

Заместитель Руководителя

Департамента разработки

стандартов и фонда НТД Е. Ялынская

Ведущий специалист

Департамента разработки

стандартов и фонда НТД Н. Жакиш