ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 20000-6— 2021

Информационные технологии

МЕНЕДЖМЕНТ СЕРВИСОВ

Часть 6

Требования к органам, осуществляющим аудит и сертификацию систем менеджмента сервисов

(ISO/IEC 20000-6:2017, IDT)

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Ассоциацией по сертификации «Русский Регистр» (Ассоциация «Русский Регистр») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 декабря 2021 г. № 1773-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 20000-6:2017 «Информационные технологии. Менеджмент сервисов. Часть 6. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента сервисов» (ISO/IEC 20000-6:2017 «Information technology — Service management — Part 6: Requirements for bodies providing audit and certification of service management systems» IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© ISO, 2017
© IEC, 2017
© Оформление. ФГБУ «РСТ», 2022

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Принципы 2
5 Общие требования 2
6 Требования к структуре 2
7 Требования к ресурсам 2
8 Требования к информации 3
9 Требования к процессу 4
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам 11
Библиография 12

Введение

Настоящий стандарт предназначен для использования органами по сертификации, осуществляющими аудит и сертификацию систем менеджмента сервисов (СМС) в соответствии с ИСО/МЭК 20000-1. Он также может быть использован органами по аккредитации при оценке органов по сертификации. Стандарт предназначен для использования совместно с ИСО/МЭК 17021-1, в котором установлены критерии для органов по сертификации, осуществляющих аудит и сертификацию систем менеджмента. Настоящий стандарт содержит требования, дополняющие требования ИСО/МЭК 17021-1.

Корректное применение настоящего стандарта позволит органам по сертификации гармонизировать применение ИСО/МЭК 17021-1 для оценок на соответствие требованиям ИСО/МЭК 20000-1. Оно также позволит органам по аккредитации гармонизировать применение стандартов, используемых ими для оценки органов по сертификации.

Текст настоящего стандарта насколько это возможно повторяет структуру ИСО/МЭК 17021-1, а дополнительные требования, помимо требований ИСО/МЭК 17021-1 указаны в качестве подпунктов.

В ИСО/МЭК 17021-1 и настоящем стандарте термин «клиент» используется для обозначения организации, желающей пройти сертификацию.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕНЕДЖМЕНТ СЕРВИСОВ

Часть 6

Требования к органам, осуществляющим аудит и сертификацию систем менеджмента сервисов

Information technology. Service management. Part 6. Requirements for bodies providing audit and certification of service management systems

Дата введения — 2022—04—30

1 Область применения

Настоящий стандарт устанавливает требования и руководство для органов по сертификации, осуществляющих аудит и сертификацию систем менеджмента сервисов (СМС) в соответствии с ИСО/МЭК 20000-1. Настоящий стандарт не изменяет требования, указанные в ИСО/МЭК 20000-1. Он также может использоваться органами по аккредитации для аккредитации органов по сертификации.

Любой орган, осуществляющий сертификацию СМС, должен быть способен продемонстрировать выполнение требований, содержащихся в настоящем стандарте, помимо требований, указанных в ИСО/МЭК 17021-1.

2 Нормативные ссылки

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

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

ISO/IEC 20000-1, Information technology — Service management — Part 1: Service management system requirements (Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов)

ISO/IEC TR 20000-10[1)], Information technology — Service management — Part 10: Concepts and terminology (Информационные технологии. Менеджмент сервисов. Часть 10. Понятия и термины)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 17021-1 и ISO/IEC TR 20000-10.

ИСО и МЭК поддерживают терминологическую базу данных, используемую в стандартизации по следующим адресам:

[1)] Заменен на ISO/IEC 20000-10. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

Издание официальное

- Электропедия МЭК: доступна по адресу gost.e-ecolog.ru ;
- платформа онлайн-просмотра ИСО: доступна по адресу gost.e-ecolog.ru .

4 Принципы

Настоящий стандарт основан на принципах ИСО/МЭК 17021-1:2015, раздел 4.

5 Общие требования

5.1 Юридические и договорные вопросы

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

5.2 Обеспечение беспристрастности

Применяются требования ИСО/МЭК 17021-1:2015, 5.2. Кроме того, применяются следующие требования и положения.

5.2.1 Конфликты интересов

Органы по сертификации могут выполнять следующие обязанности, не считающиеся консультационными или потенциально влекущими конфликт интересов:

a) организацию курсов обучения и участие в них в качестве преподавателя при условии, что, если эти курсы связаны с менеджментом сервисов, связанными с ним системами менеджмента или с проведением аудита, то органам по сертификации необходимо ограничиваться предоставлением общей информации и рекомендациями, являющимися общедоступными, т. е. они не должны предоставлять консультацию конкретной компании;

b) предоставление или публикацию по запросу информации, описывающей толкование органом по сертификации требований стандартов по сертификационному аудиту;

c) проведение мероприятий до проведения аудита, направленных исключительно на определение готовности к сертификационному аудиту; однако подобные мероприятия не должны приводить к предоставлению рекомендаций или консультации, противоречащих настоящему пункту. Орган по сертификации должен быть в состоянии подтвердить, что подобные действия не противоречат данным требованиям, и не используются для обоснования уменьшения окончательной продолжительности сертификационного аудита;

d) проведение аудитов второй и третьей стороны в соответствии со стандартами или положениями, кроме тех, которые являются частью области аккредитации;

e) добавление ценности во время сертификационных аудитов и посещений в рамках надзора, например, путем идентификации возможностей для улучшения, которые становятся очевидными в процессе аудита без рекомендации конкретных решений.

Орган по сертификации не должен предоставлять услуг по внутреннему анализу со стороны руководства системы менеджмента сервисов сертифицируемой СМС. Кроме того, орган по сертификации должен быть независим от органа или органов (включая любых лиц), осуществляющих внутренний аудит СМС.

5.3 Ответственность и финансирование

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

6 Требования к структуре

Применяются требования ИСО/МЭК 17021-1:2015, раздел 6.

7 Требования к ресурсам

7.1 Компетентность персонала

7.1.1 Общие положения

Применяются требования ИСО/МЭК 17021-1:2015, 7.1.1.

7.1.2 Определение критериев компетентности

Применяются требования ИСО/МЭК 17021-1:2015, 7.1.2. Кроме того, применяются следующие требования и положения.

7.1.2.1 Термин «техническая область»

Согласно ИСО/МЭК 20000-1 все требования являются общими и предназначены для применения всеми клиентами, вне зависимости от типа, размера и характера предоставляемых сервисов. В контексте аудитов по ИСО/МЭК 20000-1 термин «техническая область» относится к СМС, включая процессы менеджмента сервисов и услуги в рамках области СМС. «Техническая область» не относится к базовой технологии, используемой для обеспечения предоставления услуг.

7.1.3 Процессы оценки

Применяются требования ИСО/МЭК 17021-1:2015, 7.1.3.

7.1.4 Другие факторы

Применяются требования ИСО/МЭК 17021-1:2015, 7.1.4.

7.2 Персонал, участвующий в сертификационной деятельности

Применяются требования ИСО/МЭК 17021-1:2015, 7.2. Кроме того, применяются следующие требования и положения.

7.2.1 Компетентность персонала, участвующего в сертификационной деятельности

Орган по сертификации должен определить критерии для подготовки и повышения компетентности аудиторов и персонала, участвующего в управлении и поддержании деятельности по сертификации. В отношении каждой функции, если это применимо, орган по сертификации должен обеспечить знания:

a) требований, указанных в ИСО/МЭК 20000-1;

b) соответствующих частей ИСО/МЭК 20000, в особенности ИСО/МЭК 20000-2, ИСО/МЭК 20000-3 и ISO/IEC TR 20000-10.

Орган по сертификации должен обеспечить, что аудиторы и персонал, участвующие в управлении и поддержании деятельности по сертификации, надлежащим образом осведомлены о влиянии законодательных и регулирующих требований, относящихся к аудиту СМС, в соответствии с юрисдикцией в рамках области сертификации. Осведомленность о законодательных и регулирующих требованиях не подразумевает глубоких юридических знаний: сертификационный аудит системы менеджмента не является аудитом соответствия законодательным требованиям.

Орган по сертификации должен обеспечить, что аудиторы поддерживают актуальность знаний и навыков в отношении менеджмента сервисов и проведения аудита посредством постоянного профессионального развития.

7.3 Привлечение внешних аудиторов или внешних технических экспертов

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

7.4 Записи данных по персоналу

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

7.5 Аутсорсинг

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

8 Требования к информации

8.1 Общедоступная информация

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

8.2 Документы по сертификации

Применяются требования ИСО/МЭК 17021-1:2015, 8.2. Кроме того, применяются следующие требования и положения.

8.2.1 Определение области

При определении области используется руководство ИСО/МЭК 20000-3.

8.3 Ссылка на сертификацию и использование знаков

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

8.4 Конфиденциальность

Применяются требования ИСО/МЭК 17021-1:2015, 8.4. Кроме того, применяются следующие требования и положения.

8.4.1 Доступ к документам организации, включая записи

До проведения сертификационного аудита орган по сертификации должен запросить клиента сообщить, есть ли какая-либо информация или записи в отношении СМС, которые не могут быть доступны для проверки группе аудиторов, т. к. содержит конфиденциальную или секретную информацию. Орган по сертификации должен определить, может ли быть адекватно проведен аудит СМС при отсутствии таких документов или записей. Если аудит не может быть проведен при наличии каких-либо документов или записей, орган по сертификации должен предупредить клиента, что аудит не может быть проведен до тех пор, пока не будет обеспечен доступ к ним.

8.5 Обмен информацией между органом по сертификации и его клиентами

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

9 Требования к процессу

9.1 Предсертификационная деятельность

9.1.1 Заявка

Применяются требования ИСО/МЭК 17021-1:2015, 9.1.1.

9.1.2 Анализ заявки

Применяются требования ИСО/МЭК 17021-1:2015, 9.1.2. Кроме того, применяются следующие требования и положения.

9.1.2.1 Анализ заявки

Орган по сертификации должен проанализировать заявку от клиента для обеспечения четкого понимания областей деятельности клиента и вероятных рисков для СМС и услуг.

9.1.3 Программа аудитов

Применяются требования ИСО/МЭК 17021-1:2015, 9.1.3.

9.1.4 Определение продолжительности аудита

Применяются требования ИСО/МЭК 17021-1:2015, 9.1.4. Кроме того, применяются следующие требования и положения.

9.1.4.1 Определение продолжительности аудита для первоначального аудита

Орган по сертификации должен использовать фактическое количество сотрудников организации-клиента в качестве основы определения продолжительности для первоначального сертификационного аудита. Орган по сертификации должен использовать таблицу 1 при определении продолжительности аудита. Согласно таблице 1 берется за основу 8-часовой день. Значения могут быть уточнены, если количество рабочих часов в день более или менее 8 ч.

Фактическое количество сотрудников клиента рассчитывается как эквивалент в полных рабочих днях (full-time equivalent, FTE). Расчет фактического количества сотрудников клиента должен быть основан на количестве сотрудников, охваченных областью СМС. Орган по сертификации должен быть в состоянии предоставить обоснование связи между фактическим количеством сотрудников клиента, поддерживающих СМС и сервисы, и продолжительностью аудита.

Если фактическое количество сотрудников клиента, поддерживающих СМС и сервисы, превышает 1175, процедуры органа по сертификации должны содержать расчет продолжительности аудита, следуя прогрессии, указанной в таблице 1, и определять количество дней методом экстраполяции за рамками последней графы в таблице 1.

Планы проведения первоначального аудита органа по сертификации должны быть основаны на минимальной продолжительности аудита 2,5 дня, после уточнений, вне зависимости от количества сотрудников клиента.

Продолжительность аудита должна составлять не менее 80 % времени аудита. Если на планирование или составление отчетных документов по аудиту требуется дополнительное время, оно не должно уменьшать продолжительность самого аудита.

Таблица 1 — Взаимоотношение между фактическим количеством сотрудников и временем аудита до уточнения (первоначальный аудит)

Фактическое количество сотрудников клиента	Время аудита: этап 1 + этап 2 (в днях)
1—15	3,5
16—25	4,5
26—45	5,5
46—65	6
66—85	7
86—125	8
126—175	9
176—275	10
276—425	11
426—625	12
626—875	13
876—1175	15

Примечание — Временем аудита считается время, необходимое на планирование и проведение полного результативного аудита системы менеджмента клиента. Время аудита включает в себя все время, проведенное на площадке в местоположении клиента (физическом или виртуальном) и время, проведенное за пределами площадки, затраченное на планирование, анализ документов, взаимодействие с сотрудниками клиента и подготовку отчета. Продолжительностью сертификационных аудитов системы менеджмента считается та часть времени аудита, которая отводится на осуществление деятельности по аудиту с момента проведения вступительного совещания до момента проведения заключительного совещания включительно.

Фактическое количество сотрудников включает в себя весь персонал, участвующий в деятельности в рамках области сертификации, включая сотрудников, работающих посменно. При включении сотрудников в область сертификации необходимо также учитывать временных сотрудников (например, подрядчиков) и работников с частичной занятостью. В зависимости от продолжительности рабочего времени, количество работников с частичной занятостью и сотрудников, деятельность которых частично входит в область, может быть уменьшено или увеличено и преобразовано в эквивалентное количество сотрудников с полной занятостью. Когда высокий процент сотрудников выполняют деятельность или функции, которые считаются повторяющимися, допускается уменьшение количества сотрудников, которое связано и систематически применяется по отношению к каждому клиенту в рамках области сертификации.

9.1.4.2 Изменение времени аудита

Необходимо учитывать все свойства СМС и услуг клиента, а также изменения в первоначальном расчете времени аудита в отношении этих факторов, которые могут служить обоснованием увеличения или уменьшения времени. Независимо от факторов изменения орган по сертификации должен обеспечивать, что для проведения полного результативного аудита СМС клиента отведено достаточное количество времени. Орган по сертификации должен документировать и быть в состоянии обосновать увеличение или уменьшение времени аудита.

Таблицы 2 и 3 демонстрируют, как соответствующие факторы могут воздействовать на время аудита, указанное в таблице 1. Термин «смена» обозначает передачу выполнения и взаимодействия в различных местоположениях и/или группы, выполняющие функции в последовательные периоды выполнения работ.

Максимальное уменьшение времени аудита составляет 30 % от времени, указанного в таблице 1.

Таблица 2 — Факторы, которые могут уменьшать время аудита

Факторы потенциального уменьшения времени	
1	Низкая скорость изменения СМС и сервисов
2	Продемонстрированное ранее результативное функционирование СМС, например, предыдущая сертификация другим аккредитованным органом по сертификации
3	Комбинированный аудит СМС с одной или несколькими другими соответствующими системами менеджмента
4	Предварительные знания об организации, например, наличие сертификации по другому стандарту тем же органом по сертификации
5	Единственный, простой сервис
6	Идентичные виды деятельности, выполняемые во всех сменах, с надлежащими свидетельствами эквивалентного выполнения во всех сменах, например, служба поддержки
7	Значительная часть персонала, осуществляющего менеджмент сервисов, выполняет одинаковые простые функции
8	Одна площадка с небольшим количеством персонала
9	Низкий уровень зависимости от других сторон, таких как поставщики, внутренние группы или потребителей, выступающих в роли поставщиков, участвующих в предоставлении услуг

Таблица 3 — Факторы, которые могут увеличивать время аудита

Факторы потенциального увеличения времени	
1	Сложная логистика, включающая несколько юрисдикций, несколько площадок в одной или нескольких часовых поясах
2	Сложность, связанная с различиями языков в различных местоположениях, например, персонал, разговаривающий на нескольких языках (требуется переводчик или невозможность работы каждого аудитора индивидуально)
3	Большой объем или сложность области СМС, например, большое количество сервисов, персонала или местоположений, специальные сервисы, сложные для понимания и поддержания в рабочем состоянии
4	Высокая степень законодательного и нормативного регулирования, влияющего на СМС клиента, например, права интеллектуальной собственности, персональная информация, законодательство в области пищевых продуктов, лекарственных средств, аэрокосмоса, ядерной энергетики
5	Различные виды деятельности, осуществляемые в различные смены
6	Наличие временных площадок в рамках области СМС, подлежащих определенному аудиту
7	Сложные бизнес-процессы, осуществляемые в рамках области СМС
8	Высокий уровень зависимости от других сторон, таких как поставщики, внутренние группы или потребители, выступающие в роли поставщиков, участвующие в предоставлении услуг
9	Частое дополнение новых сервисов, удаление сервисов, перенос или значительное изменение сервисов

9.1.4.3 Изменение продолжительности для сертификаций по другим стандартам систем менеджмента

Если клиент сертифицирован на соответствие требованиям других стандартов по системам менеджмента, например, ИСО 9001 и/или ИСО/МЭК 27001, орган по сертификации может уменьшить первоначальное время аудита.

Уменьшение времени аудита в результате наличия сертификации на соответствие требованиям других стандартов систем менеджмента допускается только при соблюдении следующих условий:

a) другой стандарт системы менеджмента относится к проверяемой СМС;

b) имеющийся сертификат действителен и был проверен аккредитованным органом по сертификации как минимум один раз в течение последних 12 мес;

c) области других сертификаций совпадают или шире, чем область сертификации по ИСО/МЭК 20000-1.

Сокращение времени аудита должно зависеть от степени интегрированности системы менеджмента клиента с другими системами менеджмента.

Независимо от других соответствующих стандартов систем менеджмента, орган по сертификации должен обеспечить, чтобы было отведено достаточное количество времени для проведения полного и результативного аудита СМС клиента.

Примечание — Для обозначения одновременной проверки двух или более систем менеджмента по различным дисциплинам используется термин «комбинированный аудит». В случаях, когда эти системы интегрированы в единую систему менеджмента, используются те же принципы и процедуры для проведения аудита, что и для комбинированного аудита.

9.1.4.4 Определение времени аудита для надзорных и ресертификационных аудитов

Время, необходимое для проведения надзорных и ресертификационных аудитов, должно быть рассчитано с использованием следующих факторов:

a) продолжительность аудита должна составлять не менее 80 % от общего времени аудита;

b) надзорные аудиты должны составлять минимум одну треть от времени аудита, ежегодно затрачиваемого на первоначальный аудит, проводимый в виде одного или нескольких проверок;

c) ресертификационные аудиты должны составлять минимум две трети от времени аудита, затрачиваемого на первоначальный аудит;

d) минимальное время аудита, затрачиваемое на надзорные аудиты, после внесенных изменений должно составлять один день;

e) минимальное время аудита, затрачиваемое на ресертификационные аудиты, после внесенных изменений должно составлять два дня.

9.1.4.5 Удаленный аудит

Аудиты, проводимые без личного присутствия в одном местоположении, а осуществляемые из другого местоположения называются удаленными аудитами. План аудита должен идентифицировать методы проведения удаленного аудита, которые будут использоваться.

Приемлемые и неприемлемые практики проведения удаленных аудитов указаны в таблице 4. Орган по сертификации не должен использовать неприемлемые практики, приведенные в таблице 4 и может использовать приемлемые практики.

Удаленные аудиты не должны уменьшать время аудита, ниже рассчитанного согласно таблице 1, с соответствующими изменениями.

При подготовке органом по сертификации плана аудита, согласно которому удаленная деятельность по аудиту составляет более 30 % от запланированного времени аудита на площадке, орган по сертификации должен документировать обоснование.

Таблица 4 — Приемлемые и неприемлемые практики проведения удаленных аудитов

Приемлемые	
1	Телеконференция: видео и аудио, вэб-семинар, интерактивная связь через Интернет
2	Удаленный доступ к инструментам, используемым для поддержания СМС
3	Удаленный доступ к архиву документов и записей по СМС
Неприемлемые	
4	Проверка исключительно документации
5	Предположение о том, что во всех местоположениях выполняются одинаковые функции без подтверждающих предположение свидетельств
6	Аудиты, проводимые без опроса персонала

Примечание — Термин «общая продолжительность аудита» означает общую продолжительность аудита, распределяемую по отдельным объектам. Электронный аудит удаленных объектов считается удаленным аудитом даже в том случае, если электронный аудит физически выполняется на территории или в помещениях организации-заказчика.

9.1.5 Выборка для организаций с несколькими площадками

Применяются требования ИСО/МЭК 17021-1:2015, 9.1.5. Кроме того, применяются следующие требования и положения.

9.1.5.1 Критерии выборки для организаций с несколькими площадками

Если организация-клиент имеет несколько площадок, для проведения сертификационных аудитов нескольких площадок органы по сертификации могут использовать подход, основанный на выборке, если все площадки:

a) работают в рамках одной и той же СМС, которая администрируется централизованно;

b) включены в программу внутреннего аудита клиента;

c) включены в программу анализа со стороны руководства клиента.

9.1.6 Стандарты на комплексные системы менеджмента

Применяются требования ИСО/МЭК 17021-1:2015, 9.1.6. Кроме того, применяются следующие требования и положения.

9.1.6.1 Совмещение аудитов систем менеджмента

Аудит СМС может быть совмещен с аудитами других систем менеджмента. Комбинированный или интегрированный аудит должен обеспечивать, что свидетельства аудита удовлетворяют требованиям ИСО/МЭК 20000-1 в рамках области аудита. Все наблюдения, относящиеся к ИСО/МЭК 20000-1, должны быть легко идентифицированы в отчетах по аудиту.

Совмещение аудитов не должно неблагоприятно влиять на качество аудита по ИСО/МЭК 20000-1.

9.1.6.2 Совмещение аудитов систем менеджмента по ИСО/МЭК 20000-1 и ИСО/МЭК 27001

При совмещении аудитов по ИСО/МЭК 27001 и ИСО/МЭК 20000-1 необходимо проводить аудит процесса менеджмента информационной безопасности по ИСО/МЭК 20000-1 для обеспечения того, что:

a) политика информационной безопасности относится к СМС и сервисам;

b) соответствующие риски в области информационной безопасности идентифицированы, а средства контроля информационной безопасностью внедрены для поддержания СМС и сервисов.

Аудитор может обнаружить некоторые подтверждающие свидетельства системы менеджмента информационной безопасности (СМИБ).

Если область СМИБ не входит в рамки области СМС, процесс менеджмента информационной безопасности в ИСО/МЭК 20000-1 должен проверяться как отдельный процесс без поддержки СМИБ.

Политика, риски и средства контроля информационной безопасности должны проверяться для обеспечения их соответствия сервисам в рамках области СМС клиента.

9.2 Планирование аудитов

9.2.1 Определение целей, области и критериев аудита

Применяются требования ИСО/МЭК 17021-1:2015, 9.2.1. Кроме того, применяются следующие требования и положения.

9.2.1.1 Определение целей аудита

Цели аудита должны включать в себя проверку идентификации и управления взаимосвязями с другими сторонами, участвующими в функционировании СМС, в границах СМС. Орган по сертификации также должен обеспечивать что, клиент осведомлен и осуществляет управление всеми рисками для СМС и сервисов, возникающими в результате этих взаимосвязей.

9.2.2 Отбор и назначение группы аудиторов

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

9.2.3 План аудита

Применяются требования ИСО/МЭК 17021-1:2015, 9.2.3. Кроме того, применяются следующие требования и положения.

9.2.3.1 Точность выборки

Орган по сертификации должен разработать процедуры для обеспечения следующего:

a) адекватный уровень выборки должен определяться на этапе первоначального анализа договора и последующей деятельности по аудиту, с идентификацией разницы между:

1) местоположениями, например, разница в размерах площадок или временных площадках, охваченных СМС, но не входящих в область сертификации;

2) услугами;

3) потребителями;

4) другими сторонами (внутренними группами, поставщиками, потребителями, выступающими в виде поставщиков), участвующих в предоставлении сервисов;

5) языками;

6) системностью подхода, используемого во всех сменах. На аудит клиента, высокий процент персонала которого работает в сменах, может потребоваться меньшее количество времени, если каждая смена функционирует одинаково. Процедура включает в себя анализ записей с целью подтверждения системности подхода в отношении всех смен. Если деятельность смен одинакова, все смены могут рассматриваться как совокупность деятельности, а для выборки в рамках аудита может использоваться одна смена;

7) местными особенностями СМС;

8) законодательными и нормативными требованиями;

b) показательная выборка осуществляется из всех площадок в рамках области СМС клиента. Выбор должен основываться на суждении органа по сертификации, чтобы отразить факторы, представленные в перечислении a), а также на элементе случайности;

c) проект плана аудита должен учитывать требования, указанные в перечислениях a) и b). План должен включать в себя показательную выборку всей области СМС в течение трехлетнего периода между сертификационными аудитами.

9.3 Первоначальная сертификация

Применяются требования ИСО/МЭК 17021-1:2015, 9.3. Кроме того, применяются следующие требования и положения.

9.3.1 Идентификация других сторон

Орган по сертификации должен иметь доступ к свидетельствам идентификации других сторон, участвующих в предоставлении сервисов клиенту и свидетельствам того, что они управляются в соответствии с требованиями ИСО/МЭК 20000-1.

9.3.2 Интеграция документации СМС с документацией других систем менеджмента

Орган по сертификации должен учитывать, что клиент может интегрировать документацию СМС с документацией других систем менеджмента, например, системы менеджмента качества или системы менеджмента информационной безопасности.

При объединении документации нескольких систем менеджмента СМС клиента должна быть четко идентифицирована.

9.4 Проведение аудитов

9.4.1 Общие положения

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.1.

9.4.2 Проведение вступительного совещания

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.2.

9.4.3 Обмен информацией в ходе аудита

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.3.

9.4.4 Получение и верификация информации

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.4.

9.4.5 Идентификация и документирование наблюдений по аудиту

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.5.

9.4.6 Подготовка заключений по аудиту

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.6.

9.4.7 Проведение заключительного совещания

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.7.

9.4.8 Отчет по аудиту

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.8. Кроме того, применяются следующие требования и положения.

9.4.8.1 Отчет по аудиту

Отчет по аудиту должен быть достаточно подробным для обоснования решения о сертификации. Он должен содержать формулировку области сертификации со ссылкой на любые изменения в области, описания значимых следов аудита и использованные методологии аудита.

Отчет должен включать в себя рекомендации группы аудиторов в отношении сертификации СМС клиента, с указанием информации, обосновывающей данную рекомендацию. Обоснование должно включать краткое описание несоответствий и возможностей для улучшения в отношении внедрения и результативности СМС.

9.4.9 Анализ причин несоответствий

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.9.

9.4.10 Результативность коррекций и корректирующих действий

Применяются требования ИСО/МЭК 17021-1:2015, 9.4.10.

9.5 Решение о сертификации

Применяются требования ИСО/МЭК 17021-1:2015, 9.5.

9.6 Подтверждение сертификации

Применяются требования ИСО/МЭК 17021-1:2015, 9.6.

9.7 Апелляции

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

9.8 Жалобы

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

9.9 Записи в отношении клиентов

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

9.10 Требования системы менеджмента к органам по сертификации

Применяются требования ИСО/МЭК 17021-1:2015, 10.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 17021-1:2015	IDT	ГОСТ Р ИСО/МЭК 17021-1—2017 «Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования»
ISO/IEC 20000-1	IDT	ГОСТ Р ИСО/МЭК 20000-1—2013 «Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами»
ISO/IEC TR 20000-10	IDT	ГОСТ Р 57392—2017/ISO/IEC TR 20000-10:2015 «Информационные технологии. Управление услугами. Часть 10. Основные понятия и терминология»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1]	ISO/IEC 17011	Conformity assessment — General requirements for accreditation bodies accrediting conformity assessment bodies
[2]	ISO/IEC 19011	Guidelines for auditing management systems
[3]	ISO/IEC 20000-1	Information technology — Service management — Part 1: Service management system requirements
[4]	ISO/IEC 20000-2	Information technology — Service management — Part 2: Guidance on the application of service management systems
[5]	ISO/IEC 20000-3	Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1
[6]	ISO/IEC 20000-4	Information technology — Service management — Part 4: Process reference model
[7]	ISO/IEC 20000-5	Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1
[8]	ISO/IEC TR 20000-9	Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services
[9]	ISO/IEC TR 20000-10	Information technology — Service management — Part 10: Concepts and terminology
[10]	ISO/IEC TR 20000-11	Information technology — Service management — Part 11: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: ITIL®
[11]	ISO/IEC TR 20000-12	Information technology — Service management — Part 12: Guidance on the relationship between ISO/IEC 20000-1:2011 and service management frameworks: CMMI-SVC
[12]	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
[13]	ISO/IEC 27006	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
[14]	ISO/IEC 27013	Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
[15]	ISO/IEC TR 90006	Information technology — Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1

УДК 004.05:006.354 ОКС 35.020

Ключевые слова: информационная технология, управление сервисами, система управления сервисами, оценка соответствия

Редактор *Е.В. Якубова*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 17.12.2021. Подписано в печать 11.01.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «РСТ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru