МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 27006

Первое издание
2007-03-01

Информационные технологии. Методы и средства обеспечения безопасности. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Ответственность за подготовку русской версии несёт GOST R (Российская Федерация) в соответствии со статьёй 18.1 Устава ISO

Ссылочный номер
ISO/IEC 27006:2007(R)

Содержание

Страница

Предисловие

Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) формируют специализированную систему по мировой стандартизации. Национальные организации, являющиеся членами ISO или IEC, принимают участие в разработке международных стандартов через технические комитеты, созданные соответствующей организацией для рассмотрения вопросов конкретных сфер технической деятельности. Технические комитеты ISO и IEC сотрудничают в сферах, представляющих взаимный интерес. Другие международные организации, государственные и негосударственные, взаимодействующие с ISO и IEC, тоже принимают участие в работе. В сфере информационной технологии ISO и IEC создали совместный технический комитет ISO/IEC JTC 1.

Международные стандарты составляются в соответствии с правилами, приведенными в Директивах ISO/IEC, Часть 2.

Основной задачей Совместного Технического комитета является подготовка международных стандартов. Проекты международных стандартов, принятые Техническими комитетами, распространяются среди орга-низаций-членов для голосования. Публикация в качестве международного стандарта требует одобрения, по крайней мере, 75 % организаций-членов, принимающих участие в голосовании.

Следует обратить внимание на возможность того, что некоторые элементы данного документа могут быть объектом патентного права. ISO не должна нести ответственность за установление любого или всех таких патентных прав.

ISO/IEC 27006 был подготовлен Совместным Техническим комитетом ISO/IEC JTC 1, *Информационные технологии*, Подкомитетом SC 27, *Методы и средства обеспечения безопасности*.

Введение

ISO/IEC 17021 — это международный стандарт, содержащий критерии для органов, осуществляющих аудит и сертификацию систем менеджмента организаций. Если эти органы должны быть аккредитованы как соответствующие ISO/IEC 17021 с целью проведения аудита и сертификации систем менеджмента информационной безопасности (СМИБ) в соответствии с ISO/IEC 27001:2005, то необходимы дополнительные требования и руководства к ISO/IEC 17021. Они представлены в настоящем международном стандарте.

Текст настоящего международного стандарта повторяет структуру ISO/IEC 17021, а дополнительные требования, характерные для СМИБ, и руководство по применению ISO/IEC 17021 для сертификации СМИБ обозначаются аббревиатурой "ИБ".

Термин "должен" используется в этом международном стандарте для указания тех условий, которые, отражая требования ISO/IEC 17021 и ISO/IEC 27001, являются обязательными. Термин "должен" используется для обозначения условий, которые, хотя и являются руководством по применению этих требований, предполагается, что будут приняты органом сертификации.

Цель настоящего международного стандарта — дать возможность органам аккредитации более эффективно согласовывать применение ими стандартов, в отношении которых они обязаны оценивать органы сертификации. В этом контексте любое отклонение органа сертификации от руководства является исключением. Такие отклонения будут разрешены только на основе рассмотрения каждого случая по отдельности, после того как орган сертификации докажет органу аккредитации, что это исключение удовлетворяет каким-то эквивалентным образом пункт соответствующих требований ISO/IEC 17021, ISO/IEC 27001 и настоящего международного стандарта.

ПРИМЕЧАНИЕ В данном международном стандарте термины "система менеджмента" и "система" используются, заменяя друг друга. Определение системы менеджмента можно найти в ISO/IEC 9000:2005. Систему менеджмента, использующуюся в этом международном стандарте, не следует путать с другими типами системы, такими как системы информационных технологий.

Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

1 Область распространения

В настоящем стандарте устанавливаются требования и дополнительно к требованиям, содержащимся в ISO/IEC 17021 и ISO/IEC 27001, дается руководство для органов, осуществляющих аудит и сертификацию СМИБ. Главным образом он предназначен для поддержки аккредитации органов сертификации, осуществляющих сертификацию СМИБ.

Любой орган, осуществляющий сертификацию СМИБ, должен предъявлять требования, содержащиеся в настоящем стандарте на основе компетентности и надёжности, а в руководстве предоставляется дополнительное разъяснение этих требований к органу, осуществляющему сертификацию СМИБ.

ПРИМЕЧАНИЕ Настоящий стандарт может использоваться в качестве документа, содержащего критерии для аккредитации, экспертной оценки или других процессов аудита.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ISO/IEC 17021:2006, *Оценка соответствия. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента*

ISO/IEC 27001:2005*, Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования*

ISO/IEC 19011:2002, *Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента*

3 Термины и определения

В настоящем стандарте применены термины по ISO/IEC 17021, ISO/IEC 27001, а также следующие термины с соответствующими определениями.

3.1
сертификат
certificate
документ, выданный органом сертификации, в соответствии с условиями его аккредитации и имеющий подтверждение аккредитации.

3.2
орган сертификации
certification body
третья сторона, оценивающая и сертифицирующая СМИБ организации-клиента на соответствие действующим стандартам СМИБ и любой дополнительной документации, устанавливаемый в соответствии с требованиями системы

3.3
документ сертификации
certification document
документ, указывающий, что СМИБ организации-клиента соответствует стандартам СМИБ и дополнительной документации, требуемой в соответствии с этой системой

3.4
маркировка
mark
юридически зарегистрированный фирменный знак или защищенным образом символ, который выпускается по правилам органа аккредитации или органа сертификации, указывающий на то, что орган достаточно уверен в системах или, что соответствующие продукты или субъекты отвечают требованиям определенного стандарта

3.5
организация
organization
государственная или частная компания, корпорация, фирма, предприятие, управление или учреждение или их часть, или их комбинация, имеющая собственные функции и администрацию, и способная обеспечить информационную безопасность.

4 Принципы

Применяются принципы ISO/IEC 17021:2006, Раздел 4.

5 Общие требования

5.1 Юридические и договорные вопросы

Применяются требования ISO/IEC 17021:2006, 5.1.

5.2 Менеджмент беспристрастности

Применяются требования ISO/IEC 17021:2006, 5.2. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения

5.2.1 ИБ 5.2 Конфликты интересов

Органы сертификации могут выполнять следующие обязанности, не рассматривая их как консультации или имеющие потенциальный конфликт интересов:

a) сертификацию, включая информационные совещания, совещания по планированию, изучение документов, проведение аудита (не внутренних аудитов СМИБ или внутренних проверок безопасности) и последующую деятельность в отношении несоответствий;

b) организацию курсов обучения и участие в них в качестве преподавателя при условии, что если эти курсы связаны с менеджментом информационной безопасности, взаимосвязанными системами менеджмента или с проведением аудита, то органам сертификации необходимо ограничиваться предоставлением общей информации и рекомендациями, являющимися легко доступными для всеобщего достояния, т.е. они не должны предоставлять консультацию конкретной компании, которая противоречит требованиям c), ниже;

c) предоставление или публикацию по запросу информации, описывающей интерпретацию органом сертификации требований стандартов по сертификации аудита;

d) проведение мероприятий, осуществляющихся до проведения аудита, направленные исключительно на определение готовности к сертификационному аудиту; однако подобные действия не должны приводить к предоставлению рекомендаций или консультации,

противоречащих этому пункту, и орган сертификации должен суметь подтвердить, что подобные действия не противоречат этим требованиям, и не используются для оправдания возможной продолжительности сертификационного аудита;

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

f) увеличение значимости во время сертификационных аудитов и посещений в рамках надзора, например, путём определения возможностей для улучшения, которые становятся очевидными в процессе аудита без рекомендации конкретных решений.

Орган сертификации должен быть независим от органа или органов (включая любых лиц), осуществляющих внутренний аудит подлежащей сертификации СМИБ организации-клиента.

5.3 Обязательства и финансирование

Применяются требования ISO/IEC 17021:2006, 5.3.

6 Требования к структуре

6.1 Структура организации и высшее руководство

Применяются требования ISO/IEC 17021:2006, 6.1.

6.2 Комитет по обеспечению защиты беспристрастности

Применяются требования ISO/IEC 17021:2006, 6.2.

7 Требования к ресурсам

7.1 Компетентность руководства и персонала

Применяются требования ISO/IEC 17021:2006, 7.1. Кроме того, применяются следующие, характерные для СМИБ, требования и руководство.

7.1.1 ИБ 7.1 Компетентность руководства

Основные элементы компетентности, требующиеся для проведения сертификации СМИБ, должны выбирать, обеспечивать и стоять во главе тех индивидуальных лиц, чьи навыки и общая компетентность подходят для осуществления аудита и решения вопросов, связанных с информационной безопасностью.

7.1.1.1 Анализ компетентности и проверка договора

Орган сертификации должен обеспечивать уверенность в том, что он обладает знанием технологических и правовых вопросов, относящихся к СМИБ организации-клиента, которую он оценивает.

Орган сертификации должен обладать эффективной системой для анализа компетентности в сфере менеджмента информационной безопасности, которую ему нужно поддерживать доступной по отношению ко всем техническим сферам, в которых он действует.

Для каждого клиента орган сертификации должен быть способен продемонстрировать осуществление анализа и компетентности (оценка навыков в ответ на оцененные потребности) в отношении требований каждого уместного сектора до осуществления проверки договора. Затем орган сертификации должен осуществить проверку договора с организацией-клиентом, основываясь на результатах анализа компетентности. В частности, орган сертификации должен быть способен

продемонстрировать, что он обладает компетентностью для выполнения следующих видов деятельности:

a) понимание сфер деятельности организации-клиента и связанных с ними бизнес-рисков;

b) определение компетентности, необходимой органу сертификации для осуществления сертификации в отношении определенной деятельности, связанной с информационной безопасностью, угрозами активов, уязвимостями и влияниями на организацию-клиента;

c) подтверждение наличия требуемой компетентности.

7.1.1.2 Ресурсы

Руководство органа сертификации должно располагать необходимыми процессами и ресурсами для определения компетентности отдельных аудиторов в отношении решения задач, которые они должны выполнить в области сертификации, в которой они действуют. Компетентность аудиторов можно повысить путем повышения квалификации, специальной полготовки и инструктажа (см. также Приложение B). Орган сертификации должен быть способен эффективно поддерживать связь с клиентами, которым он предоставляет услуги.

7.2 Персонал, участвующий в деятельности по сертификации

Применяются требования ISO/IEC 17021:2006, 7.2. Кроме того, применяются следующие, характерные для СМИБ, требования и положения.

7.2.1 ИБ 7.2 Компетентность персонала органа сертификации

Органы сертификации должны иметь персонал, обладающий компетентностью в вопросах:

a) выбора и проверки компетентности аудиторов СМИБ для групп аудита, предназначенных для проведения аудита;

b) инструктажа аудиторов СМИБ и организации любого необходимого обучения;

c) принятия решения о разрешении, поддержке, отмене, приостановке, продлении или сокращении сроков действия сертификации;

d) организации работы, связанной с апелляциями и жалобами.

7.2.1.1 Обучение аудиторских групп

У органа сертификации должны быть критерии обучения аудиторских групп, обеспечивающие:

a) знание стандарта, относящегося к СМИБ, и других уместных нормативных документов;

b) понимание обеспечения информационной безопасности;

c) понимание оценки риска и менеджмента риска, исходя из перспективы бизнеса;

d) техническое знание деятельности, подлежащей аудиту;

e) общее знание регулирующих требований, имеющих отношение к СМИБ;

f) знание систем менеджмента;

g) понимание принципов аудита, основанных на ISO 19011;

h) знание проверки эффективности СМИБ и измерения эффективности средств контроля.

Эти требования к обучению применяются ко всем членам аудиторской группы за исключением требований (d), которые можно распределить между членами аудиторской группы.

7.2.1.1.1 При выборе аудиторской группы, которая будет назначена для конкретного сертификационного аудита, орган сертификации должен обеспечить, чтобы навыки, представленные для каждого задания, были соответствующими. Группа должна:

a) обладать соответствующими техническими знаниями по конкретной деятельности в области действия СМИБ, для которой проводится сертификация и, если необходимо, с взаимосвязанными процедурами и их потенциальными рисками информационной безопасности (эту функцию могут выполнять технические эксперты, не являющиеся аудиторами);

b) обладать достаточным уровнем понимания работы организации-клиента для проведения надежного аудита сертификации ее СМИБ в вопросе менеджмента, связанного с аспектами информационной безопасности ее деятельности, продуктов и услуг;

c) обладать соответствующим пониманием регулирующих требований, применяемых к СМИБ организации-клиента.

7.2.1.1.2 При необходимости аудиторская группа может дополняться техническими экспертами, которые могут продемонстрировать специальные знания в области технологии, подлежащей аудиту. Необходимо отметить, что технических экспертов нельзя использовать вместо аудиторов СМИБ, но они могут консультировать аудиторов по вопросам технической адекватности в контексте системы менеджмента, подвергающейся аудиту. У органа по сертификации должна быть процедура по:

a) выбору аудиторов и технических экспертов на основе их компетентности, обучения, квалификации и опыта;

b) первоначальной оценке поведения аудиторов и технических экспертов во время проведения аудитов сертификации и последующего мониторинга деятельности аудиторов и технических экспертов.

7.2.1.2 Менеджмент процесса принятия решений

Управленческая функция должна подразумевать наличие технической компетентности для управления процессом принятия решений относительно разрешения, поддержки, продления, сокращения, приостановки и отмены в сертификации СМИБ по требованиям ISO/IEC 27001.

7.2.1.3 Необходимые уровни образования, профессионального опыта, аудиторского обучения и аудиторского опыта для аудиторов, проводящих аудиты СМИБ

7.2.1.3.1 Приведенные ниже критерии должны применяться к каждому аудитору из аудиторской группы, осуществляющей аудит СМИБ. Аудитор должен:

a) иметь среднее образование;

b) иметь, по крайней мере, четырехлетний опыт практической работы в режиме полной занятости в сфере информационной технологии, из которой, по крайней мере, два года [аудитор] должен выполнять роль или функцию, связанную с информационной безопасностью;

c) успешно завершить пятидневное обучение, сфера которого охватывает аудиты СМИБ, и менеджмент аудитов должен считаться соответствующим;

d) приобрести опыт, касающийся всего процесса оценки информационной безопасности, до принятия на себя ответственности за деятельность в качестве аудитора. Этот опыт должен быть приобретен посредством участия, как минимум, в четырех сертификационных аудитах общей продолжительностью, по крайней мере, двадцать дней, включая проверку документации и анализ риска, оценку реализации и составление отчета о результатах аудита;

e) обладать достаточно современным опытом;

f) быть способным представить сложные операции в широкой перспективе и понимать роль отдельных подразделений в больших организациях-клиентах;

g) поддерживать свои знания и навыки в сфере информационной безопасности и аудита на современном уровне путем постоянного повышения профессионального уровня.

Технические эксперты должны соответствовать критериям (a), (b), (e) и (f).

7.2.1.3.2 В дополнении к требованиям из 7.2.1.3.1 начальники групп аудита должны удовлетворять следующим требованиям, которые должны быть продемонстрированы в аудитах под руководством и наблюдением:

a) обладать знаниями и характерными чертами для управления процессом аудита сертификации;

b) быть аудитором, по крайней мере, в трёх полных аудитах СМИБ;

c) продемонстрировать способность эффективно общаться и в письменной, и в устной форме.

7.3 Привлечение отдельных внешних аудиторов и внешних технических экспертов

Применяются требования ISO/IEC 17021:2006, 7.3. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения.

7.3.1 ИБ 7.3 Привлечение внешних аудиторов или внешних технических экспертов в качестве членов аудиторской группы

При привлечении внешних аудиторов или внешних технических экспертов в качестве членов аудиторской группы, орган сертификации должен гарантировать, что они компетентны и не вовлекаются ни напрямую, ни через своего работодателя в проектирование, внедрение или обслуживание СМИБ или связанной с ней системой (системами) управления таким образом, что это могло бы скомпрометировать беспристрастность.

7.3.1.1 Привлечение технических экспертов

Технические эксперты со специальными знаниями, касающимися процесса и проблем информационной безопасности, а также законодательства, затрагивающей организацию-клиента, но не удовлетворяющие всем критериям 7.2, могут быть членами группы аудита. Технические эксперты должны работать под наблюдением аудитора.

7.4 Записи данных о персонале

Применяются требования ISO/IEC 17021:2006, 7.4.

7.5 Аутсорсинг

Применяются требования ISO/IEC 17021:2006, 7.5.

8 Требования к информации

8.1 Общедоступная информация

Применяются требования ISO/IEC 17021:2006, 8.1. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения.

8.1.1 ИБ 8.1 Процедуры разрешения, поддержания, продления, сокращения, приостановления и отказа в сертификации

Орган сертификации должен потребовать от организации-клиента наличия документально оформленной и внедренной СМИБ, которая соответствует ISO/IEC 27001 и другим документам, необходимым для сертификации.

У органа сертификации должны быть документально подтверждённые процедуры для:

a) начального сертификационного аудита СМИБ организации-клиента в соответствии с положениями ISO 19011, ISO/IEC 17021 и другими необходимыми документами;

b) надзора и повторных сертификационных аудитов СМИБ организации-клиента в соответствии с ISO 19011 и ISO/IEC 17021 на периодической основе для непрерывного соответствия релевантным требованиям, а также для подтверждения и записи, что организация-клиент своевременно предпринимает корректирующие действия по исправлению всех несоответствий.

8.2 Документы по сертификации

Применяются требования ISO/IEC 17021:2006, 8.2. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения.

8.2.1 ИБ 8.2 Документы по сертификации СМИБ

Орган сертификации должен предоставить каждой из своих организаций-клиентов, чья СМИБ сертифицируется, документы по сертификации, такие как: письмо или сертификат, подписанный уполномоченным должностным лицом. Для организации-клиента и каждой из его сертифицирующихся информационных систем эти документы должны определять область действия сертификации и ISO/IEC 27001 по СМИБ, по которому эта СМИБ сертифицируется. Кроме того, в сертификате должна быть ссылка на определённую версию заявления (утверждения) о применимости.

8.3 Список сертифицированных клиентов

Применяются требования ISO/IEC 17021:2006, 8.3.

8.4 Ссылка на сертификацию и использование маркировки

Применяются требования ISO/IEC 17021:2006, 8.4. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения.

8.4.1 ИБ 8.4 Контроль за маркировками сертификации

Орган сертификации должен установить надлежащий контроль за правом собственности, использованием и отражением своих сертификационных знаков СМИБ. Если орган сертификации даёт право использовать знак для обозначения сертификации СМИБ, то он должен быть уверен, что организация-клиент использует специальный знак только так, как санкционировано в письменном разрешении органа сертификации. Орган сертификации не дает право организации-клиенту использовать этот знак на продукте или таким способом, что он может интерпретироваться в качестве обозначения соответствия продукта требованиям.

8.5 Конфиденциальность

Применяются требования ISO/IEC 17021:2006, 8.5. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения.

8.5.1 ИБ 8.5 Доступ к документам организации

До проведения сертификационного аудита орган сертификации должен попросить организацию-клиента сообщить о том, что какие-то документы СМИБ не могут быть доступными для проверки аудиторской группе, т.к. они содержат конфиденциальную или секретную информацию. Орган сертификации должен определить, может ли быть адекватно проведён аудит СМИБ при отсутствии этих документов. Если орган сертификации приходит к выводу, что невозможно адекватно провести аудит СМИБ без проверки определенных конфиденциальных или секретных документов, он должен предупредить организацию-клиента, что сертификационный аудит не может иметь место до тех пор, пока не будет обеспечен доступ к ним.

8.6 Обмен информацией между органом сертификации и его клиентами

Применяются требования ISO/IEC 17021:2006, 8.6.

9 Требования к процессу

9.1 Общие требования

Применяются требования ISO/IEC 17021:2006, 9.1. Кроме того, применяются следующие, конкретные для СМИБ, требования и положения.

9.1.1 ИБ 9.1.1 Общие требования к аудиту СМИБ

9.1.1.1 Критерии аудита сертификации

Критерии, по которым осуществляется аудит СМИБ организации-клиента, должны быть те, которые приняты в стандарте ISO/IEC 27001 по СМИБ и других документах, требующихся для сертификации, относящихся к выполняемой функции. Если требуется объяснение, как применять эти документы к специальной программе сертификации, то подобное объяснение должно даваться соответствующей беспристрастной комиссией или лицами, обладающими необходимой технической компетентностью, и опубликовываться органом по сертификации.

9.1.1.2 Политики и процедуры

Документация органа по сертификации должна включать политику и процедуры осуществления процесса сертификации, включая проверки использования и применения документов, применяемых при сертификации систем СМИБ, а также процедуры проведения аудита и сертифицирования СМИБ организации-клиента.

9.1.1.3 Аудиторская группа

Аудиторская группа должна официально назначаться и обеспечиваться соответствующими рабочими документами. План и время аудита должны согласовываться с организацией-клиентом. Мандат, данный аудиторской группе, должен быть четко определен и понятен организации-клиенту и должен требовать от аудиторской группы проверки структуры, политики и процедур организации-клиента, а также подтверждения того, что они [структуры, политики и процедуры] отвечают всем требованиям, относящимся к области действия сертификации и, что указанные процедуры выполняются и можно быть уверенным в СМИБ организации-клиента.

9.1.2 ИБ 9.1.2 Область действия сертификации

Аудиторская группа должна проверить СМИБ организации-клиента, охватывая определенную область действия по отношению ко всем применяемым требованиям сертификации. Орган сертификации должен гарантировать, что область действия и границы СМИБ организации-клиента чётко определены на основе характеристик бизнеса, организации, ее расположения, активов и технологии. Орган сертификации должен подтвердить, что в области действия СМИБ организации-клиенты выполняют требования, изложенные в ISO/IEC 27001:2005, 1.2.

Органы сертификации должны гарантировать, что оценка риска информационной безопасности и обработка риска организации-клиенты надлежащим образом отражают свою деятельность и распространяют границы ее деятельности, как определено в стандарте ISO/IEC 27001 по СМИБ. Органы сертификации должны подтвердить, что это отражается в области действия их СМИБ и заявлении о применимости организации-клиента.

Органы сертификации должны гарантировать, что взаимодействие с услугами или видами деятельности, которые не полностью включены в сферу действия СМИБ, было рассмотрено в подвергающейся сертификации СМИБ и включено в оценку риска информационной безопасности организации-клиента. Пример подобной ситуации — совместное использование средств (например, системы ИТ, базы данных и системы телекоммуникации) с другими организациями.

9.1.3 ИБ 9.1.3 Время аудита

Органы сертификации должны предоставлять аудиторам достаточное время для осуществления всех действий, связанных с первоначальным аудитом, надзором или повторным сертификационным аудитом. Время должно базироваться на таких факторах как:

a) размер СМИБ (например, количество используемых информационных систем, количество сотрудников);

b) сложность СМИБ (например, критичность информационных систем, ситуация риска СМИБ), см. также Приложение A;

c) вид(ы) деловой деятельности, осуществляемой в области действия СМИБ;

d) уровень и разнообразие технологии, использованной при внедрении различных компонентов СМИБ (таких как, внедрённые средства контроля, документация и/или контроль процесса, корректирующие/превентивные действия и т.д.);

e) количество узлов сети;

f) ранее продемонстрированное функционирование СМИБ;

g) объём аутсорсинга и мероприятия третьей стороны, использованные в масштабе СМИБ;

h) стандарты и положения, применяющиеся к сертификации.

В Приложении C представлено руководство по продолжительности аудита. Орган сертификации должен быть готов обосновать или объяснить продолжительность времени, затраченное на первоначальный аудит, надзорные аудиты или повторный сертификационный аудит.

9.1.4 ИБ 9.1.4 Множественные объекты (площадки)

9.1.4.1 Решения по выборке объектов (площадок) в области сертификации СМИБ, являются более сложными, чем те же самые решения в системах управления качеством. Там, где организация-клиент имеет количество объектов сертификации, удовлетворяющее критериям от a) до c), органы сертификации могут использовать основанный на выборке подход к сертификационному аудиту многочисленных объектов:

a) все объекты работают в рамках одной и той же СМИБ, которая централизованно администрируется, проверяется аудитом и подлежит проверке центрального управления;

b) все объекты включаются в программу внутреннего аудита СМИБ организации-клиента;

c) все объекты включаются в программу проверки менеджмента СМИБ организации-клиента.

9.1.4.2 У органа сертификации, желающего использовать подход, основанный на выборке, должны быть процедуры для гарантии следующего: