ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27013— 2014

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1

ISO/IEC 27013:2012
Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 16 сентября 2014 г. № 1084-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27013:2012 «Информационная технология. Методы обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1» (ISO/IEC 27013:2012 «Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1»).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

В Российской Федерации 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, определения и сокращения 2
4 Обзор ИСО/МЭК 27001 и ИСО/МЭК 20000-1 2
4.1 Понимание стандартов 2
4.2 Концепции ИСО/МЭК 27001 2
4.3 Концепции ИСО/МЭК 20000-1 2
4.4 Сходства и различия 3
5 Подходы к совместному использованию 4
5.1 Общая информация 4
5.2 Рассмотрение области применения 4
5.3 Предварительно используемые сценарии 5
6 Факторы, касающиеся совместного использования 7
6.1 Общая информация 7
6.2 Возможные проблемы 7
6.3 Потенциальные выгоды 12
Приложение А (справочное) Соответствие между ИСО/МЭК 27001:2005 и ИСО/МЭК 20000-1:2011 16
Приложение В (справочное) Сравнение терминов ИСО/МЭК 27000:2009 и ИСО/МЭК 20000-1:2011 19
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 42
Библиография 43

Введение

ИСО/МЭК 27013 был подготовлен совместным техническим комитетом ИСО/МЭК СТК 1, *Информационная технология*, подкомитетом 27, *Методы и средства обеспечения безопасности*, в сотрудничестве с совместным техническим комитетом ИСО/МЭК СТК 1, *Информационная технология*, подкомитетом 7, *Проектирование программного обеспечения и систем*.

Взаимосвязь между информационной безопасностью и менеджментом услуг является настолько тесной, что многие организации уже осознали выгоды применения обоих стандартов: ИСО/МЭК 27001 — для обеспечения информационной безопасности и ИСО/МЭК 20000-1 — для менеджмента услуг. Обычно организация совершенствует методы своей работы для соответствия требованиям одного стандарта, а затем проводит дальнейшие совершенствования, чтобы соответствовать требованиям другого стандарта.

Реализация интегрированной системы менеджмента, учитывающей не только предоставляемые услуги, но также и защиту информационных активов, дает ряд выгод. Эти выгоды можно получить независимо от того, вводятся ли стандарты последовательно или их ввод в действие происходит одновременно. В частности, менеджмент и организационные процессы могут получить выгоду из сходства стандартов и их общих целей.

Основные выгоды совместного введения в действие этих стандартов:

a) уверенность внутренних или внешних клиентов организации в эффективных и безопасных услугах;

b) более низкая стоимость интегрированной программы двух проектов, в которой достижения менеджмента услуг и информационной безопасности являются частью стратегии организации;

c) уменьшение времени реализации за счет интегрированной разработки процессов, общих для обоих стандартов;

d) устранение ненужного дублирования;

e) лучшее понимание персоналом, отвечающим за менеджмент услуг и обеспечение безопасности, точек зрения друг друга;

f) организации, прошедшей сертификацию по ИСО/МЭК 27001, намного легче выполнять требования по обеспечению информационной безопасности подраздела 6.6 ИСО/МЭК 20000-1:2011, поскольку оба стандарта дополняют требования друг друга.

Настоящий стандарт основан на опубликованных версиях обоих стандартов, т. е. ИСО/МЭК 27001:2005 и ИСО/МЭК 20000-1:2011.

Настоящий стандарт предназначен для использования лицами, знающими содержание обоих стандартов (ИСО/МЭК 27001 и ИСО/МЭК 20000-1), одного из них или не знающими ни того, ни другого стандарта.

Предполагается, что всем читателям доступны экземпляры обоих стандартов. Поэтому настоящий стандарт не воспроизводит части ни одного из стандартов. Также он не описывает полностью все части каждого стандарта. Подробно описываются только те части, в которых предметы обсуждения совпадают.

Настоящий стандарт не дает рекомендаций, связанных с разными правовыми и нормативными актами, регулирующими деятельность организации извне. Данные акты могут варьироваться в зависимости от страны и влиять на планирование системы менеджмента организации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1

Information technology. Security techniques.
Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Дата введения — 2015—09—01

1 Область применения

Настоящий стандарт предоставляет руководство по совместному использованию ИСО/МЭК 27001 и ИСО/МЭК 20000-1 для организаций, планирующих:

a) реализовать ИСО/МЭК 27001, когда стандарт ИСО/МЭК 20000-1 уже принят, или наоборот;

b) реализовать одновременно оба стандарта: ИСО/МЭК 27001 и ИСО/МЭК 20000-1;

c) объединить существующие системы менеджмента в соответствии с ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

Настоящий стандарт сосредоточен исключительно на совместном использовании ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

На практике ИСО/МЭК 27001 и ИСО/МЭК 20000-1 могут быть также интегрированы в другие системы менеджмента, представленные, например, в ИСО 9001 и ИСО 14001.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных документов используют только указанное издание. Для недатированных документов используют самое последнее издание ссылочного документа (с учетом всех его изменений).

ИСО/МЭК 20000-1:2011 Информационная технология. Менеджмент услуг. Требования к системе менеджмента услуг (ISO/IEC 20000-1:2011, Information technology – Service management – Service management system requirements)

ИСО/МЭК 27000:2009[1)] Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология (ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary)

[1)] ИСО/МЭК 27000:2009 заменен на ИСО/МЭК 27000:2014. Однако для однозначного соблюдения требований настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

Издание официальное

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

3 Термины, определения и сокращения

В настоящем стандарте применены термины по ИСО/МЭК 27000:2009 и ИСО/МЭК 20000-1:2011. В настоящем стандарте применены следующие сокращения:

СМИБ система менеджмента информационной безопасности (information security management system – ISMS) (из ИСО/МЭК 27001);

СМУ система менеджмента услуг (service management system – SMS) (из ИСО/МЭК 20000-1).

В приложении А настоящего стандарта приведено сравнение содержания ИСО/МЭК 27001:2005 и ИСО/МЭК 20000-1:2011 на уровне структурных элементов.

В приложении В настоящего стандарта приведено сравнение терминов:
- определенных в ИСО/МЭК 27000:2009, являющемся глоссарием для ИСО/МЭК 27001:2005;
- использованных в ИСО/МЭК 27001;
- определенных или использованных в ИСО/МЭК 20000-1:2011.

4 Обзор ИСО/МЭК 27001 и ИСО/МЭК 20000-1

4.1 Понимание стандартов

Прежде чем планировать интегрированную систему менеджмента, организации следует достичь полного понимания характерных особенностей, сходств и различий ИСО/МЭК 27001 и ИСО/МЭК 20000-1. Это позволяет оптимизировать время и ресурсы, доступные для реализации. В 4.2 - 4.4 настоящего стандарта представлены основные концепции, лежащие в основе обоих стандартов, но их не следует использовать взамен детального рассмотрения указанных стандартов.

4.2 Концепции ИСО/МЭК 27001

ИСО/МЭК 27001 представляет модель для установления, реализации, эксплуатации, мониторинга, проверки, поддержки и совершенствования СМИБ, используемой для защиты информационных активов. Информационные активы охватывают информацию любого вида, хранимую в любой форме и используемую для любых целей организации или в ее рамках.

Для достижения согласованности с ИСО/МЭК 27001 организация должна реализовать СМИБ на основе процесса оценки риска, чтобы определить риски информационных активов. Как часть этой работы, организация должна сделать выбор, реализовать, провести мониторинг и проверить разнообразные меры для осуществления менеджмента этих рисков. Эти меры известны как меры и средства контроля и управления. Организации необходимо определять допустимые уровни риска, учитывая требования бизнеса и налагаемые внешние требования. Примерами налагаемых внешних требований являются законодательные и нормативные требования или договорные обязательства.

ИСО/МЭК 27001 предназначен для использования организацией любого вида и величины.

4.3 Концепции ИСО/МЭК 20000-1

ИСО/МЭК 20000-1 предназначен для применения организациями или частями организаций, использующих или предоставляющих услуги. Это добавляет значимости, как клиенту, так и поставщику услуг. Тем не менее, все процессы, охватываемые стандартом, контролируются поставщиком услуг, и только поставщик услуг может добиться соответствия ИСО/МЭК 20000-1. Стандарт в первую очередь

[1)] ИСО/МЭК 27001:2005 заменен на ИСО/МЭК 27001:2013. Однако для однозначного соблюдения требований настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

нацелен на обеспечение уверенности в том, что услуги удовлетворяют требованиям по обслуживанию и обеспечивают выгоду, как для клиента, так и для поставщика услуг.

Менеджмент услуг управляет и контролирует деятельности и ресурсы поставщика услуг при проектировании, разработке, развитии, предоставлении и совершенствовании услуг с целью выполнения требований к услугам, согласованных со своим клиентом(ами).

Для выполнения требований этого стандарта поставщиком услуг должен быть реализован ряд определенных процессов менеджмента услуг. Они включают, среди прочего, менеджмент инцидентов, менеджмент изменений и менеджмент проблем. Менеджмент информационной безопасности считается одним из процессов менеджмента услуг ИСО/МЭК 20000-1.

ИСО/МЭК 20000-1 может быть использован организацией любого вида и величины.

4.4 Сходства и различия

Менеджмент услуг и менеджмент информационной безопасности часто рассматривают так, будто они не связаны и даже не зависимы один от другого. Условием такого разделения является то, что менеджмент услуг, бесспорно, может иметь отношение к эффективности и рентабельности, тогда как менеджмент информационной безопасности часто не рассматривается как основа для эффективного оказания услуг. В результате менеджмент услуг часто реализуется в первую очередь. Однако, как показано на рисунке 1, многие цели управления, а также меры и средства контроля и управления из приложения А ИСО/МЭК 27001:2005, также включены в требования менеджмента услуг из ИСО/МЭК 20000-1.



Рисунок 1 — Сравнение концепций ИСО/МЭК 27001 и ИСО/МЭК 20000-1

Очевидно, что менеджмент информационной безопасности и менеджмент услуг рассматривают очень похожие процессы и деятельности, даже несмотря на то, что одна система менеджмента выделяет некоторые детали больше чем другая. Дополнительную информацию см. в приложении А настоящего стандарта. При работе с двумя стандартами необходимо понимать, что они различаются по некоторым аспектам. Например, их области действия различны, см. 5.2 настоящего стандарта. К тому

же у них разные цели. ИСО/МЭК 20000-1 предназначен для обеспечения уверенности в том, что организация предоставляет эффективные услуги, тогда как ИСО/МЭК 27001 предназначен для того, чтобы дать возможность организации осуществлять менеджмент риска информационной безопасности и предотвращать инциденты безопасности.

5 Подходы к совместному использованию

5.1 Общая информация

Организация, планирующая реализацию ИСО/МЭК 27001 и ИСО/МЭК 20000-1, может находиться в одном из трех состояний:

- существуют совместные соглашения по менеджменту, которые охватывают и менеджмент информационной безопасности и менеджмент услуг (формально системы менеджмента могут также существовать для других областей, например, менеджмент качества);
- существует система менеджмента, основанная на одном из стандартов;
- существуют отдельные системы менеджмента, основанные на обоих стандартах, но они не интегрированы.

Организация, планирующая реализацию интегрированной системы менеджмента, должна учитывать, по крайней мере, следующее:

a) другую, уже используемую систему(ы) менеджмента (например, систему менеджмента качества);

b) все услуги, процессы и их взаимозависимости в контексте интегрированной системы менеджмента;

c) элементы каждого стандарта, которые могут быть объединены, и то, каким образом они могут быть объединены;

d) элементы, которые должны остаться разъединенными;

e) влияние интегрированной системы менеджмента на клиентов, поставщиков и другие стороны;

f) влияние на используемую технологию;

g) влияние на услуги и менеджмент услуг или риски в отношении услуг и менеджмента услуг;

h) влияние на информационную безопасность и менеджмент информационной безопасности или риски в отношении информационной безопасности и менеджмента информационной безопасности;

i) образование и профессиональную подготовку кадров, связанные с интегрированной системой менеджмента;

j) переходные этапы и последовательность действий по реализации.

5.2 Рассмотрение области применения

Одной из областей, где отмечается существенное различие двух стандартов, является объект их области применения, а именно, активы, процессы и роли, которые должна включать система менеджмента организации.

ИСО/МЭК 20000-1 рассматривает требования к проектированию, развитию, предоставлению и совершенствованию услуг, направленных на удовлетворение требований. Это осуществляется через совокупность процессов. Поэтому область применения ИСО/МЭК 20000-1 охватывает процессы менеджмента в организации и предоставляемые услуги. Для ИСО/МЭК 27001 важно осуществление менеджмента риска информационной безопасности. Область применения ИСО/МЭК 27001 охватывает те элементы ее деятельности, которые организация хочет защитить. В этом отношении области применения двух стандартов описываются по-разному. В результате можно реализовать ИСО/МЭК 27001 для той же области, что и ИСО/МЭК 20000-1, но ИСО/МЭК 20000-1 не может быть применен ко всей организации, если только эта организация полностью не является поставщиком услуг.

Таким образом, некоторые процессы, активы и роли в организации могут быть исключены из области действия СМИБ, разработанной в соответствии с ИСО/МЭК 27001. Что касается ИСО/МЭК 20000-1, то они не могут быть исключены из области действия, если являются частью услуги или способствуют услуге в области действия СМУ. Область действия СМИБ также может быть определена исключительно четкими физическими границами, такими как периметр безопасности.

В некоторых случаях оба стандарта не могут быть реализованы для всей или даже части деятельности организации. Например, когда организация не может отвечать требованиям ИСО/МЭК 20000-1, поскольку она может не управлять всеми процессами, осуществляемыми другими сторонами.

Организация может реализовать СМУ и СМИБ с некоторым перекрытием различных областей их действия. Там, где деятельность находится в пределах области применения, как ИСО/МЭК 27001, так и ИСО/МЭК 20000-1, для интегрированной системы менеджмента следует учитывать требования обоих стандартов, см. приложение А настоящего стандарта. Несовпадение областей применения может привести к тому, что некоторые услуги, включенные в СМУ, будут исключены из СМИБ. Равным образом, из СМУ могут быть исключены процессы и функции СМИБ. Например, некоторые организации выбирают к реализации СМИБ только для своих рабочих и коммуникационных функций наряду с тем, что услуги по менеджменту приложений включены в их СМУ. В качестве альтернативы СМИБ может охватывать все услуги, в то время как СМУ может охватывать только услуги для отдельного клиента или часть услуг для всех клиентов. Организации следует, насколько возможно, согласовать области применения стандартов, чтобы обеспечить уверенность в том, что системы менеджмента могут быть успешно интегрированы.

Примечание — Руководство по определению области действия ИСО/МЭК 20000-1 можно найти в ИСО/МЭК 20000-3:2012 «Руководство по определению области действия и применимости ИСО/МЭК 20000-1».

5.3 Предварительно используемые сценарии

5.3.1 Общая информация

Организация, планирующая интегрированную систему менеджмента, может находиться в одном из трех состояний, как описано в 5.3.2 – 5.3.4 настоящего стандарта. Во всех случаях в организации будет применяться несколько разновидностей менеджмента процессов, иначе она не смогла бы существовать. В нижеследующих пунктах даются предложения по реализации для каждого из трех состояний, также описанных в 5.1 настоящего стандарта.

5.3.2 Ни один из стандартов в настоящее время не используется в качестве основы для системы менеджмента

Легко предположить, что когда ни один из стандартов в настоящее время не реализован, не существует политик, процессов и процедур и поэтому ситуация разрешается проще. К сожалению, это неверное представление. У организаций, не имеющих систем менеджмента, основанных либо на ИСО/МЭК 27001, либо на ИСО/МЭК 20000-1, вероятно, существует какая-то разновидность системы менеджмента. Ее необходимо будет адаптировать для достижения соответствия с каждым или обоими стандартами.

Решение, касающееся последовательности реализации двух систем менеджмента, должно быть основано на потребностях бизнеса. Решения могут приниматься в зависимости от того, существует ли конкурентоспособный мотив использования одного или другого стандарта, или существует необходимость продемонстрировать выполнение требований одного или другого стандарта для существующих или новых клиентов.

Другое важное решение касается того, будет ли реализована система менеджмента, основанная на обоих стандартах с самого начала, или следует реализовать систему менеджмента, основанную на одном стандарте, а позднее расширить ее, чтобы включить требования другого стандарта, см. 5.3.3 настоящего стандарта. Оба стандарта могут быть реализованы одновременно. Однако в зависимости от особенностей организации может быть более целесообразным начать с одного стандарта, а затем приступить к реализации другого.

Эти рассуждения поясняются следующими сценариями:

a) организация, которая предоставляет услуги, должна начать с реализации ИСО/МЭК 20000-1, а затем, исходя из уроков, извлеченных из его применения, расширить систему менеджмента, учитывая ИСО/МЭК 27001;

b) организация, использующая поставщиков, в том числе другие стороны для поставки некоторых элементов услуг, должна сначала сосредоточиться на ИСО/МЭК 20000-1. Это предоставляет дополнительные требования к другим сторонам, включая управление поставщиками. Это дает возможность принимать решения относительно управления поставщиками и вопросов управления процессом. Затем организация должна перейти к ИСО/МЭК 27001;

c) небольшая организация может сосредоточиться либо на ИСО/МЭК 27001, либо на ИСО/МЭК 20000-1, исходя из ее уровня уверенности в менеджменте услуг или информационной безопасности;

d) крупная организация, предоставляющая внутренние услуги, должна управлять реализацией как одним проектом. Если это невозможно, ей следует разделить реализацию на два параллельных подпроекта в рамках общей программы работ. В рамках каждого подпроекта следует осуществлять реализацию менеджмента согласно одному стандарту и интегрировать её с реализацией следующего подпроекта. В случае выбора такого подхода крайне важно обеспечить уверенность в совместимости проектов при их разработке. В результате это может приводить к дополнительным накладным расходам и дополнительному риску, так что к этому сценарию следует прибегать только при отсутствии альтернативы;

e) любая организация, придающая большое значение обеспечению информационной безопасности, должна сначала реализовать СМИБ, в соответствии с требованиями ИСО/МЭК 27001. Следующим шагом, поддерживающим информационную безопасность, должно быть расширение этой системы менеджмента с целью соответствия требованиям ИСО/МЭК 20000-1.

Объединенная рабочая группа / регулярные совещания в течение внедрения обоих стандартов будут способствовать обеспечению уверенности в том, что требования обоих стандартов согласованы.

5.3.3 Существует система менеджмента, удовлетворяющая требованиям одного из стандартов

Если система менеджмента уже соответствует одному из двух стандартов, то основной целью должна быть интеграция с требованиями другого стандарта. Это должно выполняться, не приводя ни к каким потерям в отношении услуг или опасностям для информационной безопасности услуг. Однако существующая система менеджмента должна быть подразделена на отдельные элементы. Это следует тщательно планировать заранее с проверкой существующей документации специалистами по применению стандарта, который будет вводиться, и специалистами по применению стандарта, который уже реализован.

Организация должна идентифицировать атрибуты установленной системы менеджмента, включающие, по меньшей мере, следующее:

a) область действия;
b) организационная структура;
c) политики;
d) деятельности по планированию;
e) полномочия и ответственности;
f) практические приемы;
g) методики, касающиеся менеджмента риска;
h) процессы;
i) процедуры;
j) термины и определения;
k) ресурсы.

Эти атрибуты необходимо рассматривать, чтобы установить, как их можно использовать в интегрированной системе менеджмента. Если выбирается двухступенчатый подход с применением одной системы менеджмента в качестве первой ступени, то второй ступенью является реализация другой системы менеджмента. Область действия каждой ступени должна быть определена и согласована до начала каких-либо действий по реализации.

5.3.4 Существуют отдельные системы менеджмента, удовлетворяющие требованиям каждого из стандартов

Этот последний случай является, вероятно, наиболее сложным. Он поясняет области применения настоящего стандарта, см. 5.2. Возможно, что организация реализовала стандарт ИСО/МЭК 27001 применительно к одной области деятельности, а стандарт ИСО/МЭК 20000-1 — к другой. Затем организация может принять решение о применении одного или другого стандарта к более широкой области деятельности. В какой-то момент времени системы менеджмента будут реализовываться для одних и тех же областей деятельности. В качестве альтернативы может быть запланировано слияние двух областей деятельности организаций. В одной области деятельности организации демонстрируется соответствие требованиям ИСО/МЭК 27001, в то время как в другой области деятельности демонстрируется соответствие требованиям ИСО/МЭК 20000-1.

Отправной точкой должен стать анализ, направленный на достижение следующего:

a) определение и документирование существующих и предполагаемых областей деятельности, в которых применяется каждый стандарт, обращая особое внимание на их различия;

b) сравнение существующих систем менеджмента и установление наличия любых взаимно несовместимых аспектов;

c) инициирование взаимодействия причастных сторон друг с другом в обеих системах менеджмента;

d) планирование наилучшего подхода к интегрированной системе менеджмента:

1) начать с общего развернутого обзора;

2) осуществлять обзор на различных уровнях организации для добавления деталей;

3) направлять замечания и предложения лицам с соответствующим уровнем полномочий для принятия необходимых решений.

Несмотря на то, что существует много способов интеграции систем менеджмента при сохранении согласованности, должен быть выполнен этап широкомасштабного планирования.

6 Факторы, касающиеся совместного использования

6.1 Общая информация

Во всех случаях целью организации должно быть создание жизнеспособной интегрированной системы менеджмента, позволяющей обеспечить согласованность с обоими стандартами. Целью не является сравнение стандартов или определение того, какой стандарт лучше или правильнее. При наличии конфликта точек зрения его следует разрешать способом, удовлетворяющим требованиям обоих стандартов, и обеспечивать уверенность в достижении организацией постоянного совершенствования СМИБ и СМУ. Идеальная интегрированная система менеджмента должна базироваться на наиболее действенном подходе, основанном на требованиях обоих стандартов, примененных соответствующим образом. Это поддерживается также путем дополнения частей одного стандарта к частям другого. Следует проявлять внимание, чтобы сохранить все необходимое для соответствия обоим стандартам.

Между интегрированной системой менеджмента и требованиями каждого отдельного стандарта должна поддерживаться документированная прослеживаемость. С целью уменьшения объема работ для интегрированной системы менеджмента может быть создан единый комплект документации. В поддержку этого организация может создать документацию прослеживания, например, таблицу прослеживаемости. Это детально покажет, как интегрированная система менеджмента согласуется с требованиями каждого стандарта. Преимущества этого подхода заключаются в возможности более простого подтверждения соответствия во время аудитов и проверок. Эти преимущества также включают возможности отслеживания того, какие деятельности являются необходимыми для подтверждения соответствия каждому стандарту.

6.2 Возможные проблемы

6.2.1 Использование и значение актива

Актив, рассматриваемый в ИСО/МЭК 20000-1, отличается от информационного актива ИСО/МЭК 27001. В ИСО/МЭК 20000-1 актив не определяется как термин, поэтому он употребляется в значении обычном для английского языка, означающем нечто ценное. В некоторых пунктах ИСО/МЭК 20000-1:2011 использование активов связано с финансовыми активами, такими как лицензии на программные средства. В отличие от этого стандарт ИСО/МЭК 27001 основывается на концепции защиты информации и имеет формальное определение информационного актива. В последующей части 6.2 настоящего стандарта обсуждаются сходства и различия использования понятий двух стандартов. Включены предложения, касающиеся того, как привести в соответствие два стандарта.

В стандарте ИСО/МЭК 20000-1 используется термин «элемент конфигурации (configuration item – CI)», определяемый как элемент, подлежащий управлению, для предоставления услуги или услуг. Организации следует определить, что такое CI для ее собственных целей с учетом ее потребностей в эффективности. «Информационный актив» может быть включен в это определение. В ИСО/МЭК 20000-1 база данных управления конфигурацией является хранилищем данных всех CI и их взаимосвязей. Некоторые организационные активы не могут входить в базу данных управления конфигурацией (например, персональные компьютеры, не используемые для поставки услуг). Равным

образом, в рамках стандарта ИСО/МЭК 20000-1 некоторые CI не могут рассматриваться как активы, например, люди. Обычно активы в ИСО/МЭК 20000-1 обладают денежной ценностью.

В ИСО/МЭК 27001 информационные активы определены как знания или данные, имеющие ценность для организации независимо от их формы, например, бумажная, электронная и т. д. В результате информационные активы могут быть CI, но CI необязательно являются информационными активами. Например, кабель для передачи данных может быть CI, хотя обычно он не является информационным активом. На рисунке 2 представлены взаимосвязи CI и информационных активов. Для интегрированной системы менеджмента информационный актив по ИСО/МЭК 27001 может быть использован в услуге или может являться частью услуги по ИСО/МЭК 20000-1.

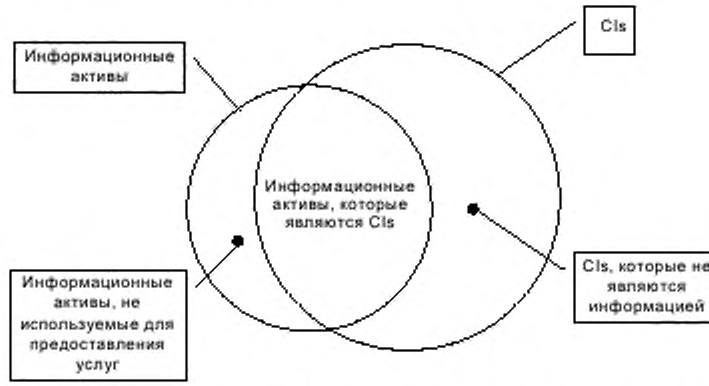


Рисунок 2 — Взаимосвязь информационных активов в ИСО/МЭК 27001 и CI в ИСО/МЭК 20000-1

Ни один из указанных стандартов не требует перечисления каждого CI или информационного актива в отдельности. Они могут быть сгруппированы по типам, таким как аппаратные средства или документы. В рамках этого процесса их описание должно быть как можно более согласованным, упрощая соответствие обоим стандартам. Например, в начале любой деятельности по интеграции должно быть принято решение о способе идентификации и классификации активов. Это необходимо для обеспечения уверенности в том, что на активы могут быть сделаны однозначные ссылки. Если термин «информационные активы» используется в изложении ИСО/МЭК 27001, то особые активы должны быть дополнительно помечены, чтобы обеспечить уверенность в признании их статуса в качестве CI или финансовых активов по ИСО/МЭК 20000-1, см. приложение В настоящего стандарта.

6.2.2 Планирование и развитие услуг

Раздел 5 ИСО/МЭК 20000-1 включает требования к планированию и развитию новых или измененных услуг. В ИСО/МЭК 27001 полностью эквивалентного раздела нет, хотя некоторые аспекты, связанные с планированием, развитием и предоставлением услуг, охвачены приложением А ИСО/МЭК 27001:2005. Однако интегрированная система менеджмента должна обеспечивать уверенность в том, что информационная безопасность детально рассматривается на запланированных этапах проектирования и развития новых или измененных услуг. Требующие рассмотрения вопросы включают оценку влияния новой или измененной услуги, как на услугу, так и меры и средства контроля и управления информационной безопасности, см. пункт 6.6.2 ИСО/МЭК 20000-1:2011. Также это должно быть выполнено для прекращения предоставления услуги.

Планирование всех новых или измененных услуг должно включать рассмотрение последствий для информационной безопасности. Это должно быть выполнено независимо от того попадает ли услуга в область действия СМИБ.

6.2.3 Оценка риска и менеджмент

Пункты 4.5.2 и 4.5.3 ИСО/МЭК 20000-1:2011 содержат требования к оценке риска и к обработке рисков, связанных со СМУ.

Пункт 4.2.1 ИСО/МЭК 27001:2005 содержит требования для менеджмента всех аспектов рисков, связанных с информационной безопасностью. Требования не ограничиваются рисками, связанными с самой СМИБ, и включают оценку рисков, их обработку и иные аспекты, связанные с менеджментом риска информационной безопасности.

Даже если риски рассматриваются как в ИСО/МЭК 27001, так и в ИСО/МЭК 20000-1, природа этих рисков различна. В ИСО/МЭК 20000-1 рассматриваются риски, касающиеся СМУ и услуг, тогда как в ИСО/МЭК 27001 рассматриваются риски информационной безопасности и их влияние на организацию. Критерии оценивания и обработки рисков могут быть различны в зависимости от того, связаны ли риски с предоставлением услуг, или конкретно с информационной безопасностью. Тем не менее, метод, использованный для идентификации рисков, может быть одним и тем же в обоих случаях. Некоторые риски, рассматриваемые в ИСО/МЭК 20000-1, например, риски поставщика, не касающиеся затрат связанных со SLA[1)], не будут считаться рисками с точки зрения ИСО/МЭК 27001. Таким образом, риски, идентифицированные при использовании ИСО/МЭК 20000-1, нельзя считать имеющими отношение к информационной безопасности, и наоборот.

Владение риском может различаться для двух подходов. Например, согласно ИСО/МЭК 20000-1, организация очень редко владеет всеми рисками. От клиента могут ожидать одобрения остаточных рисков, как часть своего SLA или плана обеспечения непрерывности услуг. В ИСО/МЭК 27001 вопрос владения риском подробно не обсуждается, но на практике организация считается владельцем всех рисков информационной безопасности.

Несовпадение вариантов менеджмента риска происходит по причине различий между двумя стандартами относительно требований к менеджменту риска. Когда планируется совместная реализация обоих стандартов, организации должны быть внимательны к любым различиям критериев риска и к влиянию, которое эти различия будут оказывать на обработку риска.

Организация должна принять один из двух подходов, представленных ниже:

a) использование для обоих стандартов единого подхода к менеджменту риска, включая оценку риска, избегая при этом дублирования. Например, риск потери пригодности информационного актива может быть общим для различных частей интегрированной системы менеджмента. Это является наиболее эффективным подходом, поскольку он избегает дублирования попыток;

b) использование отдельных методик оценки риска для двух стандартов. Если выбирается этот вариант, то организация должна использовать терминологию, которая отличает оценку риска СМУ и услуг от оценки риска информационной безопасности и СМИБ.

Там, где оценка риска и менеджмент риска являются определяющими для организации, приоритетной должна быть реализация ИСО/МЭК 27001, чтобы воспользоваться его оценкой риска и руководством по менеджменту риска. Какой бы вариант не использовался, организации следует использовать согласованную и четкую терминологию. Это может потребовать формулирования требований одного или обоих стандартов иначе, чем в опубликованной(ых) версии(й). Тем не менее, организация по-прежнему должна обеспечивать уверенность в прослеживаемости требований обоих стандартов.

6.2.4 Различия в уровнях принятия риска

Если клиент доверил свои данные или системы заботам третьей стороны, то будут существовать различия между уровнем допустимого риска клиента и третьей стороны. Детально этот вопрос не рассматривается ни одним стандартом, но организации необходимо осознавать проблемы и принимать четкое решение об уровнях риска, которые могут контролироваться разными сторонами.

Ниже описываются базовые проблемы:

a) клиент имеет мнение об уровне безопасности, приемлемом для его информации, находящейся под контролем третьей стороны. Это может не совпадать с уровнем безопасности, который третья сторона считает достаточным;

b) третья сторона также имеет собственную информацию, например, финансовую документацию. Третья сторона имеет мнение об уровне безопасности, приемлемом для этой информации;

c) клиент и третья сторона, возможно, будут вовлечены в разные обязательные к применению правовые и нормативные условия, которые будут различаться в зависимости от страны или сектора рынка. Это может приводить к различиям в их ожиданиях относительно информационной безопасности или риска.

Связанные с информационной безопасностью ожидания и обязанности клиентов организации и третьих сторон следует обсудить при первом возможном случае. Такие обсуждения важны как для согласования области действия реализуемого проекта, так и для установления эксплуатационных мер и средств контроля и управления для существующих услуг. В идеальном случае любые потенциальные конфликты должны быть идентифицированы, а решения приняты и согласованы до их реализации.

[1)] SLA — service level agreement (соглашение об уровне услуг).

6.2.5 Менеджмент инцидентов и проблем

Первым, что требуется обсудить, является терминология. В ИСО/МЭК 27001 существует единственный термин для значимых нежелательных событий: инцидент информационной безопасности. В отличие от этого в ИСО/МЭК 20000-1 существует несколько специальных терминов, связанных с менеджментом инцидентов. Например, инцидент, инцидент информационной безопасности, проблема, известная ошибка и серьезный инцидент, см. приложение В настоящего стандарта. Согласно ИСО/МЭК 27001 каждый из них может означать инцидент информационной безопасности в зависимости от их характеристик.

В ИСО/МЭК 27001 определен единый процесс, рассматривающий все инциденты информационной безопасности.

В ИСО/МЭК 20000-1 приведены не только различные термины, но и различные механизмы осуществления менеджмента событий, например, менеджмент запроса услуг и менеджмент инцидентов, менеджмент процедур серьезных инцидентов и менеджмент проблем. В ИСО/МЭК 20000-1 одно событие в течение его жизненного цикла может управляться посредством более чем одного из этих процессов и процедур. В ИСО/МЭК 20000-1 использован термин «процедура» из ИСО 9000:2005, определенный как «специфицированный способ выполнения действия или процесса». Для ИСО/МЭК 20000-1 процесс относится к более высокому уровню в сравнении с процедурой, причем процедуры поддерживают процесс.

На рисунке 3 показана взаимосвязь между менеджментом инцидентов информационной безопасности в ИСО/МЭК 27001 и менеджментом инцидентов в ИСО/МЭК 20000-1.



Рисунок 3 — Иллюстрация взаимосвязи между стандартами, касающаяся менеджмента инцидентов

Существуют события, которые в ИСО/МЭК 27001 будут классифицированы как инциденты информационной безопасности, но которые не будут классифицированы как инциденты в ИСО/МЭК 20000-1. Ниже приведены два примера:

a) после окончания рабочего дня на столе обнаружен конфиденциальный документ по продаже продукта в нарушение политики информационной безопасности. В любом случае этот документ не имеет отношения к предоставлению услуг;

b) обнаружен взлом замка двери в офисе клиента. Согласно ИСО/МЭК 27001 это событие можно рассматривать как инцидент. Однако оно вообще не будет подпадать под область действия ИСО/МЭК 20000-1, если не было доступа к информации, имеющей отношение к требованиям подраздела 6.6 ИСО/МЭК 20000-1:2011.

В равной степени существуют события, которые в ИСО/МЭК 20000-1 будут классифицированы как инцидент, но которые находятся вне области действия ИСО/МЭК 27001. Например:

a) ограничения SLA, выходящие за пределы запланированной поддержки;

b) отчеты пользователя об инцидентах, обусловленных медленным выполнением услуги.

Основное частичное совпадение между определениями инцидента заключается в том, что ИСО/МЭК 20000-1 может отнести их к «инциденту информационной безопасности», который может привести к потере конфиденциальности, целостности и доступности, связанных с определенной услугой.

Чтобы согласовать эти точки зрения, организация должна решить, как осуществлять менеджмент инцидентов, которые находятся в области действия обеих систем менеджмента.

Менеджмент проблем определяется в ИСО/МЭК 20000-1 как процесс определения основной причины возникновения одного или нескольких инцидентов, чтобы свести к минимуму влияние инцидентов или избежать его. В ИСО/МЭК 20000-1 это является отдельным процессом. В ИСО/МЭК 27001 менеджмент проблем явно не раскрыт, хотя на него ссылаются в требованиях к менеджменту инцидентов информационной безопасности, обработке риска и корректирующим мерам.

В интегрированной системе менеджмента процесс менеджмента проблем должен быть надлежащим образом определен. Если СМИБ реализуется до интеграции со СМУ, то может быть полезна, по возможности, самая ранняя интеграция лучших практических приемов менеджмента проблем СМУ, как части СМИБ, благодаря ее пользе для всех систем менеджмента.

Оба стандарта требуют от организации анализа данных и изменений по инцидентам.

Инциденты, которые вызывают риск информационной безопасности, должны классифицироваться как инциденты информационной безопасности. Не менее важно для соответствия обоим стандартам, чтобы процесс менеджмента инцидентов отражал необходимое соответствие дополнительным требованиям информационной безопасности в ИСО/МЭК 27001.

Следует отметить, что мера и средство контроля и управления из А13.2.2 ИСО/МЭК 27001:2005 охватывает изучение инцидентов безопасности, и это частично совпадает с менеджментом проблем из подраздела 8.2 ИСО/МЭК 20000-1:2011. Кроме того, идентификацию и оценку уязвимостей, необходимую по ИСО/МЭК 27001 для оценки риска информационной безопасности, следует рассматривать как процесс анализа данных, которые могут быть использованы в качестве входной информации для менеджмента проблем.

Следующей проблемой, требующей описания, является проблема реагирования на инциденты. Целью любой организации должно быть быстрое восстановление услуги после инцидента информационной безопасности, затронувшего услугу. Однако это может уменьшить вероятность расследования инцидента безопасности с целью выяснения его причины. При интеграции СМУ и СМИБ следует заботиться об обеспечении уверенности в соответствии требованиям менеджмента инцидентов информационной безопасности. Например, меры и средства контроля и управления информационной безопасности могут включать сбор, хранение и предоставление свидетельств для дисциплинарных и правовых целей. Более того, оба стандарта требуют соответствия правовым и нормативным требованиям.

Необходимо осознавать, что в случае инцидента информационной безопасности требование получения свидетельств может означать, что затронутая услуга может быть не восстановлена в запланированные сроки. ИСО/МЭК 20000-1 требует от поставщика услуг учитывать срочность обработки инцидента и его последствия. Это может означать, что потребуется дополнительное время, прежде чем будет принято решение в отношении инцидента информационной безопасности. При определении приоритетности разрешения проблемы следует учитывать важность получения свидетельств информационной безопасности, иначе они могут быть утрачены при восстановлении услуги.

В некоторых случаях инциденты информационной безопасности могут быть отнесены к серьезным инцидентам, на основании определения серьезного инцидента, согласованного с клиентом в соответствии с подразделом 8.1 ИСО/МЭК 20000-1:2011. Согласно требованиям отчетности по услугам, приведенным в подразделе 6.2 ИСО/МЭК 20000-1:2011 и требованиям менеджмента серьезных инцидентов в подразделе 8.1 ИСО/МЭК 20000-1, высшее руководство должно быть информировано обо всех серьезных инцидентах. К ним относят также и инциденты информационной безопасности. Это обеспечивается надлежащей подготовкой ответственного лица, назначенного для осуществления менеджмента инцидентов информационной безопасности. Следовательно, в рамках интегрированной системы менеджмента таким происшествием следует управлять, как серьезным инцидентом.

О серьезных инцидентах не следует заявлять, как о допускающих задержку принятия решения о сборе свидетельств в отношении инцидентов информационной безопасности. Например, если установлено, что через веб-сайт осуществляется обработка платежей клиентов, то он может быть скомпрометирован. Время сбора свидетельств и восстановления услуг должно быть адекватным образом включено в требования услуг, каталог услуг и в соглашения об уровне услуг (SLA).

В определении информационной безопасности ИСО/МЭК 20000-1 использует понятие «досягаемость (accessibility)», а ИСО/МЭК 27001 использует понятие «доступность (availability)». Это различие существует, потому что понятие «доступность» определено по-разному в двух стандартах (см. приложение В).

6.2.6 Менеджмент изменений

В пунктах А.10.1.2 и А.12.5.1 ИСО/МЭК 27001:2005 рассматривается менеджмент изменений. Пункты А.10.1.2 и А.12.5.1 позволяют организации разрабатывать процедуры для удовлетворения своих конкретных потребностей.

Пункт 9.2 «Менеджмент изменений» ИСО/МЭК 20000-1:2011 содержит требования, относящиеся к риску. Требования дополнены пунктом 6.6.3 «Инциденты и изменения информационной безопасности». Пункт 6.6.3 содержит требования к оценке влияния запрашиваемых изменений для учета их влияния на существующие меры и средства контроля и управления информационной безопасности.

Чтобы обеспечить уверенность в том, что требования менеджмента изменений выполняются, должен быть разработан контрольный перечень оценок влияния или проверок после реализации проекта, как часть интегрированной системы менеджмента на основе ИСО/МЭК 20000-1. Это должно обеспечить уверенность в том, что все типы рисков информационной безопасности анализируются, как часть процесса менеджмента изменений.

6.3 Потенциальные выгоды

6.3.1 Использование цикла Планирование-Осуществление-Проверка-Действие

ИСО/МЭК 27001 и ИСО/МЭК 20000-1 явно ссылаются на цикл Планирование-Осуществление-Проверка-Действие (Plan-Do-Check-Act – PDCA). Это может быть удобно, так как организация сможет следовать одним и тем же принципам независимо от того, какой стандарт будет реализован в первую очередь.

PDCA является основой постоянного совершенствования в обоих стандартах, таким образом, постоянное совершенствование должно быть основой деятельности по применению любого из двух или обоих стандартов. Следует отметить, что циклы PDCA могут действовать в разных временны́х отрезках, но если такое возможно, то организация должна использовать единый интегрированный цикл для обеспечения общего периода проверки или внутреннего аудита.

6.3.2 Отчетность и менеджмент уровня услуг

Отчетность по услугам охватывает больше основных деятельностей, чем требуется для менеджмента уровня услуг. Однако отчетность по услугам может поддерживать менеджмент информационной безопасности исходя из целей услуг для инцидентов информационной безопасности, которые оцениваются, прогнозируются и используются в отчетности по услугам.

В перечислении b) подраздела 6.2 ИСО/МЭК 20000-1:2011 изложено, что в процессе составления отчетов по услугам следует учитывать соответствующую информацию о значимых событиях, таких как серьезные инциденты и несоответствия. Данные, полученные в процессе составления отчетов по услугам в соответствии с ИСО/МЭК 20000-1, могут дать большое преимущество для поддержки и совершенствования информационной безопасности.

При реализации ИСО/МЭК 27001 определяются детали мер и средств контроля и управления информационной безопасности, и должна быть измерена их эффективность, см. пункт 4.2.3 «Мониторинг и анализ СМИБ» ИСО/МЭК 27001:2005. Это делает возможной интеграцию с процессом составления отчетов по услугам согласно требованиям подраздела 6.2 ИСО/МЭК 20000-1:2011, чтобы надлежащая и своевременная информация могла использоваться для поддержки или совершенствования информационной безопасности. Клиенты будут лучше понимать истинное функционирование услуг и СМУ, включая процессы менеджмента услуг, если важная информация об уровнях соответствия применимых мер и средств контроля и управления безопасности и статистические данные по инцидентам будут включены в отчеты.

Отчеты, составленные в соответствии с ИСО/МЭК 27001 и ИСО/МЭК 20000-1, как для внутреннего использования, так и предназначенные для клиентов, должны разрабатываться с учетом этих соображений.

6.3.3 Обязательства руководства

ИСО/МЭК 27001 описывает обеспечение информационной безопасности по отношению к причастным сторонам. Упоминаемыми причастными сторонами являются стороны, обладающие определенными правами в организации, реализующей СМИБ. Эти стороны могут включать персонал, акционеров, клиентов и, возможно, даже регулирующие органы или общественность. В ИСО/МЭК 20000-1 дается ссылка на клиентов и заинтересованные стороны. Заинтересованными сторонами являются человек или группа людей, особо заинтересованных в эффективности или успехе деятельности или деятельностей поставщика услуг. Вследствие этого термин «заинтересованные стороны» сходен с термином «причастные стороны», используемым в ИСО/МЭК 27001.

Обязательства высшего руководства необходимы, чтобы сделать СМУ эффективной. Это добавляет уверенности в том, что взаимоотношения с клиентом и другими заинтересованными сторонами являются успешными. Как таковые, обязательства руководства, сформулированные в ИСО/МЭК 27001, поддерживают ориентированный на клиента подход, изложенный в ИСО/МЭК 20000-1.

ИСО/МЭК 20000-1:2011 включает конкретные требования к обязательствам руководства и ответственности руководства, например, требования пунктов 4.1.1 и 4.1.4. В отличие от этого ИСО/МЭК 27001:2005 является менее конкретным в определении ответственности и подотчетности ролей в отношении СМИБ, например, требования подраздела 5.1 и пункта 5.2.2. Интегрированная система менеджмента должна выиграть от специфики стандарта ИСО/МЭК 20000-1 и использования его требований для обеспечения уверенности в том, что более широкая ответственность за обеспечение информационной безопасности воспринимается так же серьезно, как и ответственность, связанная с менеджментом услуг.

В ИСО/МЭК 20000-1 установлено, что при существовании менеджмента улучшений, организации следует возложить ответственность по управлению процессом совершенствования на определенную роль. В сравнении с этим ИСО/МЭК 27001:2005 ссылается в пункте 4.2.4 и подразделе 8.1 на организацию выполнения этой задачи, хотя в подраздел 5.1 включены требования, в соответствии с которыми организация устанавливает роли и ответственности по обеспечению информационной безопасности. Требование ИСО/МЭК 20000-1 по четкому распределению ответственности в отношении обеспечения менеджмента улучшений должно быть использовано для обеспечения уверенности в том, что для менеджмента улучшений информационной безопасности также установлена определенная роль.

6.3.4 Менеджмент возможностей

Менеджмент возможностей в подразделе 6.5 ИСО/МЭК 20000-1:2011 включает более широкий круг возможностей, чем ИСО/МЭК 27001, так что некоторые требования ИСО/МЭК 20000-1 могут использоваться для поддержки реализации ИСО/МЭК 27001. Например, описанный в ИСО/МЭК 20000-1 менеджмент возможностей использует технические возможности и возможности персонала. Кроме того, подраздел 5.2 «Управление ресурсами» в ИСО/МЭК 27001:2005 можно считать связанным с менеджментом возможностей, так как возможность является выражением доступа к достаточному количеству ресурсов, чтобы принимать разумные меры в предсказуемых обстоятельствах.

В подразделе 3.2 ИСО/МЭК 27001:2005 доступность определяется для обозначения, как досягаемости, так и используемости. Процесс менеджмента возможностей в подразделе 6.5 ИСО/МЭК 20000-1:2011поддерживает аспект доступности. Например, если недостаточно возможностей, то услуга или компонент услуги могут быть недоступны, т. е., когда невозможно сохранить файл, поскольку слишком мало памяти. Кроме того, услуга или компоненты услуги могут быть слишком медленными, что непригодно для использования, например, время отклика, из-за недостаточной пропускной способности сети.

Организация должна осознавать различия, когда требуются перекрестные ссылки между двумя стандартами. Организация должна учитывать необходимость перекрестных ссылок между подразделом 4.3 и подразделом 6.5 ИСО/МЭК 20000-1:2011 и соответствующими разделами ИСО/МЭК 27001:2005, см. приложение А настоящего стандарта. Например, требование по включению возможных влияний законодательных, нормативных, договорных или организационных изменений в план возможностей, изложенное в подразделе 6.5 ИСО/МЭК 20000-1:2011, следует сопровождать перекрестной ссылкой с подразделом А.10.1 ИСО/МЭК 27001:2005.

6.3.5 Менеджмент риска третьей стороны

Согласно ИСО/МЭК 27001 третья сторона, такая как клиент, поставщик или независимая внутренняя группа, находится вне области действия СМИБ и рассматривается как потенциальный источник риска. В приложении В настоящего стандарта содержится сравнение этих терминов, а в пунктах А.6.2.1 и А.6.2.3 ИСО/МЭК 27001 описываются меры и средства контроля и управления, которые могли бы быть использованы для менеджмента безопасности в отношении этих третьих сторон.

В отличие от ИСО/МЭК 20000-1, другие стороны являются сущностями, не находящимися под непосредственным контролем поставщика услуг, но способствующими предоставлению услуги в области действия СМУ. Другими сторонами являются поставщики, внутренние группы или клиенты (исполняющие обязанности поставщиков). Другие стороны могут вносить свой вклад в основную часть услуги, см. подраздел 4.2 «Менеджмент услуг, осуществляемых другими сторонами» ИСО/МЭК 20000-1:2011. В подразделе 6.6 ИСО/МЭК 20000-1 изложены требования менеджмента

информационной безопасности. К нему относится менеджмент риска, связанный с поставщиком, который может непосредственно воздействовать на информационную безопасность клиентской организации. Подраздел 8.1 ИСО/МЭК 20000-1:2011 также касается инцидентов и процесса запроса услуг для менеджмента инцидентов информационной безопасности, а также оценки всех изменений с целью проверки влияния на меры и средства контроля и управления информационной безопасности.

При проектировании интегрированной системы менеджмента существуют два основных фактора, влияющих на отношения бизнеса и процессы управления поставщиками в отношении осуществления менеджмента рисков третьей стороны. Эти два фактора изложены ниже:

a) договорные обязательства по обеспечению информационной безопасности должны служить исходными данными для процесса оценки риска. Этот процесс должен способствовать выполнению требований ИСО/МЭК 20000-1 к поставщику услуг в отношении реагирования на потребности бизнеса;

b) информационная безопасность должна быть учтена в процессе деловых отношений с другими сторонами, включая клиентов, исполняющих обязанности поставщиков. Ее следует учитывать при проектировании новых или изменении существующих услуг и при обсуждении SLA.

Другие охваченные подразделом 7.1 ИСО/МЭК 20000-1:2011 концепции, такие как проверки качества деятельности, изменения услуг, менеджмент удовлетворения потребностей клиента и рассмотрение претензий, могут быть применены к интегрированной системе менеджмента для усиления ее в целом.

Таким образом, интегрированная система менеджмента должна следовать подходу к управлению взаимоотношениями с поставщиками, согласно ИСО/МЭК 27001, а также соблюдать требования пункта 6.6.2 «Меры и средства контроля и управления информационной безопасности» ИСО/МЭК 20000-1:2011 в отношении риска поставщика. В тех случаях, когда активы организации находятся в рамках области действия СМИБ, но некоторые или все эти активы контролируются другой стороной, организация должна согласовывать это адекватными договорами, SLA или другими документированными соглашениями. Этот подход должен обеспечить уверенность в том, что другая сторона применяет соответствующие меры и средства контроля и управления.

6.3.6 Менеджмент непрерывности и доступности

В подразделе 6.3 «Менеджмент непрерывности и доступности услуг» ИСО/МЭК 20000-1:2011 подробно рассматривается только одна из проблем по обеспечению информационной безопасности. Деятельности по обеспечению непрерывности и доступности в рамках существующей системы менеджмента следует проанализировать, чтобы понять, могут ли они быть соответствующим образом расширены для охвата менеджмента целостности и конфиденциальности и, следовательно, осуществления менеджмента информационной безопасности любой услуги. Подробности можно почерпнуть из ИСО/МЭК 20000-1, а общие принципы – из А.14 ИСО/МЭК 27001:2005.

6.3.7 Менеджмент отношений с поставщиками

ИСО/МЭК 27001:2005 рассматривает менеджмент отношений с поставщиками в различных пунктах, например, в А.6.2.1, А.6.2.3, А.10.2, А.8 для кадровых ресурсов, включая подрядчиков. Подраздел 4.2 ИСО/МЭК 20000-1:2011 содержит требования к управлению процессами, выполняемыми другими сторонами, а подраздел 7.2 содержит требования для менеджмента отношений с поставщиками. Менеджмент отношений с поставщиками, отвечающий требованиям обоих стандартов, может быть очень эффективным.

В 6.3.5 настоящего стандарта содержится дополнительная информация по менеджменту рисков, связанных с поставщиками. Например, оценка риска в ИСО/МЭК 20000-1 может быть расширена с использованием концепции ИСО/МЭК 27001 для рассмотрения того, не будет ли безопасность организации скомпрометирована при добавлении или отказе от услуги поставщика или при конкретном изменении услуги, предоставляемой поставщиком.

Это следует рассматривать даже в том случае, если организация решает реализовать только один из стандартов.

6.3.8 Управление конфигурацией

Реестр активов в ИСО/МЭК 27001 представляет собой репозиторий всего, что имеет ценность (денежную или иную) для организации и находится в области действия СМИБ, например, информация, базы данных или процессы.

Понятие базы данных управления конфигурацией (configuration management database – CMBD) стандарта ИСО/МЭК 20000-1 очень сходно с реестром активов стандарта ИСО/МЭК 27001, однако

области применения и, как следствие, перспективы различны. Установление области применения обсуждается в пункте 4.5.1 ИСО/МЭК 20000-1:2011.

Требования подраздела 9.1 ИСО/МЭК 20000-1:2011 могут быть использованы при создании и управлении СМИБ. С точки зрения ИСО/МЭК 27001, организация должна осуществлять менеджмент безопасности CMBD, так как ее следует рассматривать в качестве информационного актива.

Подраздел 9.1 ИСО/МЭК 20000-1 также требует безопасности для CMBD, чтобы защитить точность содержащихся в ней данных. Сюда входит требование поддержки целостности услуг и компонентов услуг. Однако ИСО/МЭК 20000-1 не проводит различия между разными уровнями целостности. Здесь может быть полезен стандарт ИСО/МЭК 27001, требующий, чтобы оценивались риски для систем, услуг и компонентов услуг и определялись допустимые уровни риска. Основной вопрос заключается в том, могут ли изменения менять уровень риска и, если да, то какие изменения повысят риск до недопустимого уровня.

Требования ИСО/МЭК 20000-1 в отношении базовых уровней конфигурации и эталонных копий конфигурации, фактически являются мерами и средствами контроля и управления с точки зрения ИСО/МЭК 27001. Эти требования следует учитывать при интегрированном подходе к менеджменту риска. Некоторые из них будут влиять на решения о том, реализовывать или нет некоторые меры и средства контроля и управления.

6.3.9 Менеджмент выпуска изменений и их использования

Соответствие требованиям ИСО/МЭК 20000-1:2011 к менеджменту выпуска изменений и их использованию не обеспечивает уверенности в соответствии требованиям ИСО/МЭК 27001 к выпуску изменений. Если не следовать требованиям ИСО/МЭК 27001, на этом этапе могут быть случайно внесены проблемы с обеспечением безопасности. Например:

a) в работе действующей системы (систем) могут быть произведены изменения, вносящие недостатки в обеспечение информационной безопасности, если менеджмент выпуска изменений и их использования не учитывает возможности вредоносных действий;

b) управление тестовой и производственной средой часто может осуществляться различными группами, вследствие этого процесс выпуска изменений должен обеспечивать уверенность в том, что данные от группы тестирования получает соответствующая производственная роль, чтобы избежать рисков нарушения конфиденциальности данных.

Это особенно важно во время выпуска экстренных изменений. В таких ситуациях из-за временных ограничений и (или) ограничений ресурсов часто используется иной и, возможно, упрощенный процесс выпуска и использования изменений. Соответственно, возрастают риски компрометации информационной безопасности. Всегда необходимо осуществлять надлежащий менеджмент рисков информационной безопасности, следуя утвержденным процессам обеспечения информационной безопасности, независимо от используемого процесса выпуска и использования изменений.

Менеджмент выпуска и использования изменений может быть усовершенствован в результате выбора мер и средств контроля и управления из пункта А.10.1.4 «Разделение средств разработки, тестирования и функционирования» и пункта А.10.3.2 «Приемка систем» ИСО/МЭК 27001:2005.

6.3.10 Составление бюджета и учет

Требования по составлению бюджета и учету в подразделе 6.4 ИСО/МЭК 20000-1:2011 не могут быть непосредственно сопоставлены с каким-либо требованием ИСО/МЭК 27001. В ИСО/МЭК 27001 требование «предоставления ресурсов» и выходные данные от проводимой руководством проверки (которые требуют принятия решения о «потребностях в ресурсах»), могут быть полезны в процессе рассмотрения финансовых ресурсов и определенного бюджета.

Приложение А
(справочное)

Соответствие между ИСО/МЭК 27001:2005 и ИСО/МЭК 20000-1:2011

А.1 Общие положения

В приложении А дается сравнение содержания ИСО/МЭК 27001:2005 и ИСО/МЭК 20000-1:2011 на уровне их структурных элементов.

Структурные элементы ИСО/МЭК 27001 и ИСО/МЭК 20000-1, где отмечается совпадение большинства требований и деталей, выделены светло-серым цветом.

Структурные элементы ИСО/МЭК 20000-1 и приложения А ИСО/МЭК 27001, где отмечается совпадение большинства требований и деталей, выделены темно-серым цветом.

Области, где нет существенного совпадения, не выделены цветом.

Таблица А.1 — Соответствие между ИСО/МЭК 27001 и ИСО/МЭК 20000-1:2011

ИСО/МЭК 27001	ИСО/МЭК 20000-1
Введение	Введение
Общие положения	Нет прямого эквивалента
Процессный подход	Нет прямого эквивалента
Совместимость с другими системами менеджмента	Нет прямого эквивалента
1 Область применения	1 Область применения
1.1 Общие положения	1.1 Общие положения
1.2 Применение	1.2 Применение
2 Нормативные ссылки	2 Нормативные ссылки
3 Термины и определения	3 Термины и определения
4 Система менеджмента информационной безопасности	4 Общие требования системы менеджмента услуг
4.1 Общие требования	Нет прямого эквивалента
4.2 Создание и управление СМИБ	4.5 Создание и совершенствование СМУ
Нет прямого эквивалента Нет прямого эквивалента	4.5.1 Определение области применения; 4.5.2 Планирование СМУ (Планирование)
4.2.2 Внедрение и функционирование СМИБ	4.5.3 Внедрение и функционирование СМУ (Осуществление)
4.2.3 Мониторинг и анализ СМИБ	4.5.4 Мониторинг и анализ СМУ (Проверка)
4.2.4 Поддержка и улучшение СМИБ	4.5.5 Поддержка и совершенствование СМУ (Действие)
4.3 Требования к документации	4.3 Менеджмент документации
4.3.1 Общие положения	4.3.1 Создание и поддержка документации
4.3.2 Управление документами	4.3.2 Управление документами
4.3.3 Управление записями	4.3.3 Управление записями

Продолжение таблицы А.1

ИСО/МЭК 27001	ИСО/МЭК 20000-1
5 Ответственность руководства	4.1 Ответственность руководства
5.1 Обязательства руководства	4.1.1 Обязательства руководства
Нет прямого эквивалента	4.1.2 Политика менеджмента услуг
Нет прямого эквивалента	4.1.3 Ответственность, полномочия и обмен информацией
Нет прямого эквивалента	4.1.4 Представитель руководства
Нет прямого эквивалента	4.2 Управление процессами, осуществляемыми другими сторонами
5.2 Управление ресурсами	4.4 Управление ресурсами
5.2.1 Обеспечение ресурсами	4.4.1 Обеспечение ресурсами
5.2.2 Подготовка, осведомленность и квалификация персонала	4.4.2 Кадровые ресурсы
6 Внутренние аудиты СМИБ	4.5.4.2 Внутренний аудит
7 Анализ СМИБ со стороны руководства	4.5.4.3 Анализ со стороны руководства
7.1 Общие положения	4.5.4.3 Анализ со стороны руководства
7.2 Входные данные анализа СМИБ	4.5.4.3 Анализ со стороны руководства
7.3 Выходные данные анализа СМИБ	4.5.4.3 Анализ со стороны руководства
8 Улучшение СМИБ	4.5.5 Поддержка и совершенствование СМУ (Действие)
8.1 Постоянное улучшение	4.5.5.1 Общие положения 4.5.5.2 Менеджмент улучшений
8.2 Корректирующие действия	4.5.5.1 Общие положения 4.5.5.2 Менеджмент улучшений
	8 Процессы решения проблем
8.3 Предупреждающие действия	4.5.5.1 Общая информация 4.5.5.2 Менеджмент улучшений 8 Процессы решения проблем
Нет прямого эквивалента	5 Проектирование и развитие новых или измененных услуг
Нет прямого эквивалента	5.1 Общие положения
Нет прямого эквивалента	5.3 Проектирование и внедрение новых или измененных услуг
Нет прямого эквивалента	5.4 Развитие новых или измененных услуг
Нет прямого эквивалента	6 Процессы предоставления услуг
A.10.2.1 Предоставление услуг	6.1 Менеджмент уровня услуг
A.10.2.2 Мониторинг и анализ услуг третьей стороны	6.2 Отчетность по услугам

Окончание таблицы А.1

ИСО/МЭК 27001	ИСО/МЭК 20000-1
Нет прямого эквивалента	6.3 Менеджмент непрерывности и доступности услуг
Нет прямого эквивалента	6.4 Составление бюджета и учет в отношении услуг
A.10.2.3 Управление изменениями услуг третьей стороны A.10.3.1 Управление производительностью	5.2 Планирование новых или измененных услуг 6.5 Менеджмент возможностей
ИСО/МЭК 27001	6.6 Менеджмент информационной безопасности
Нет прямого эквивалента	7 Процессы взаимоотношений
Нет прямого эквивалента	7.1 Менеджмент деловых отношений
Нет прямого эквивалента	7.2 Менеджмент отношений с поставщиками
A.13 Менеджмент инцидентов информационной безопасности	8.1 Менеджмент инцидентов и менеджмент запроса услуг
Нет прямого эквивалента	8.2 Менеджмент проблем
Нет прямого эквивалента	9 Процессы управления
Нет прямого эквивалента (только частично в отношении некоторых мер и средств контроля и управления)	9.1 Менеджмент конфигурации
A.12.5.1 Процедуры управления изменениями	9.2 Менеджмент изменений
Нет прямого эквивалента	9.3 Менеджмент выпуска изменений и их использования
Приложение А. Цели управления и меры и средства контроля и управления	(частично охвачено выше, см. детальную разбивку)
Приложение В. Принципы OECD и настоящий международный стандарт	Нет прямого эквивалента
Приложение С. Соответствие между ИСО 9001:2000, ИСО 14001:2004 и данным международным стандартом	Нет прямого эквивалента

Приложение В
(справочное)

Сравнение терминов ИСО/МЭК 27000:2009 и ИСО/МЭК 20000-1:2011

Для краткости в таблице В.1 настоящего стандарта в столбце «Комментарии по использованию терминов в обоих стандартах» даются ссылки на стандарты без указания года выпуска. В таблице В.1 приводится сравнение терминов, использованных в ИСО/МЭК 27001 и определенных в ИСО/МЭК 27000:2009, который является глоссарием для ИСО/МЭК 27001:2005, и терминов, определенных или используемых в ИСО/МЭК 20000-1:2011. Области, где термины ИСО/МЭК 27000 и ИСО/МЭК 20000-1 определены по-разному, выделены светло-серым цветом.

Таблица В.1 — Сравнение терминов

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
Управление доступом (access control)	2.1 Средство обеспечения уверенности в том, что доступ к активам (2.3) санкционирован и ограничен на основе требований бизнеса и требований безопасности	Не определен	Нет прямого эквивалента
Подотчетность (accountability)	2.2 Ответственность сущности за свои действия и решения	Не определен	Слово «подотчетность» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: ответственность, необходимость объяснения или отстаивания своих действий или поведения, признание и принятие ответственности. Слово «подотчетность» является важным для требований подраздела 4.2 ИСО/МЭК 20000-1, т. е. «... путем ... a) демонстрации подотчетности в отношении процессов и полномочий требовать соблюдения процессов;»
Актив (asset)	2.3 Все, что имеет ценность для организации. Примечание — Существует много видов активов, включая: a) информацию (2.18); b) программные средства, такие как компьютерные программы; c) физические активы, такие как компьютеры; d) услуги; e) кадры и их квалификация, навыки и опыт; и f) нематериальные активы,	Не определен	Слово «актив» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: все, что считается ценным или полезным, например, навыки, качество, индивидуум и т. д.. В ИСО/МЭК 20000-1 слово «актив» используется очень редко: - пункт 4.1.4: «Представитель руководства наделен обязанностями и полномочиями, включающими: d) обеспечение уверенности в том, что активы, вклю-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
	такие как репутация и имидж		чая лицензии, используемые для предоставления услуг, управляются в соответствии с законодательными и регулирующими требованиями и договорными обязательствами»; - подраздел 6.4: «Должны существовать политики и документально оформленные процедуры для: а) составления бюджета и учета компонентов услуг, включая, по крайней мере: 1) активы, в том числе и лицензии, используемые для обеспечения услуг»; - пункт 6.6.2: «Поставщик услуг должен реализовывать физические, административные и технические меры и средства контроля и управления безопасностью для: а) сохранения конфиденциальности, целостности и досягаемости (accessibility) информационных активов»; - подраздел 9.1: «Должно существовать определенное взаимодействие между процессом управления конфигурацией и процессом менеджмента финансовых активов. Примечание — Менеджмент финансовых активов исключен из сферы действия процесса управления конфигурацией».
Атака (attack)	2.4 Попытка разрушить, подвергнуть опасности, изменить, заблокировать, похитить актив (2.3), или получить несанкционированный доступ к активу, или несанкционированным образом использовать его	Не определен	Нет прямого эквивалента
Аутентификация (authentication)	2.5 Обеспечение уверенности в том, что заявленная характеристика сущности является верной	Не определен	Не имеет прямого отношения к рассматриваемому термину «*аутентификация*», связанному с информационной безопасностью, который используется в ИСО/МЭК 27001 в формальном значении.

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			«*Аутентификация*» не является аналогом термина «верификация» в деятельностях, связанных с жизненным циклом системы менеджмента
Аутентичность (authenticity)	2.6 Свойство, подтверждающее, что сущность идентична заявленной	3.11 Примечание 1 — Кроме того, также могут быть затронуты другие свойства, например, аутентичность, подотчетность, неотказуемость и достоверность	Упоминается в ISO/IEC 20000-1, но не используется в дальнейшем
Доступность (availability)	2.7 Свойство, определяющее досягаемость и используемость по запросу уполномоченной сущности	3.1 Способность услуги или компонента услуги выполнять свою требуемую функцию в согласованный момент или в согласованный период времени. Примечание — Доступность обычно выражается отношением или процентным отношением времени реальной доступности услуги или компонента услуги для клиента в согласованный период времени, в течение которого услуга должна быть доступна. 3.11 Примечание 1 — Дополнительно могут также затрагиваться другие свойства, такие как аутентичность, подотчетность, неотказуемость и достоверность. Примечание 2 — Термин «доступность (availability)» не был использован в этом определении, поскольку он является определяемым термином в этой части ИСО/МЭК 20000, который не соответствует этому определению. Примечание 3 — Адаптировано из ИСО/МЭК 27000:2009	См. «информационная безопасность». Доступность часто считается основой менеджмента услуг и играет значимую роль в ИСО/МЭК 20000-1 с точки зрения оценки качества предоставляемых услуг, см. подраздел 6.3 ИСО/МЭК 20000-1. Различия между двумя определениями невелики, но из-за важности, придаваемой «доступности» в менеджменте услуг, это различие заслуживает внимания. Прямым следствием различия между двумя значениями доступности является то, что определение информационной безопасности в ИСО/МЭК 27000 было приспособлено для ИСО/МЭК 20000-1 путем использования слова досягаемость (accessibility) вместо слова доступность (availability).
Обеспечение непрерывности бизнеса (business continuity)	2.8 Процессы (2.31) и (или) процедуры (2.30), обеспечивающие уверенность в непрерывности операций бизнеса	Не определен	В ИСО/МЭК 20000-1 обеспечение непрерывности услуг используется как элемент обеспечения непрерывности бизнеса. См. «обеспечение непрерывности услуг»

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
Конфиденциальность (confidentiality)	2.9 Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов (2.31)	Не определен	Нет прямого эквивалента
Базовая конфигурация (configuration baseline)	Не определен	3.2 Информация о конфигурации, формально обозначенная в конкретное время в течение срока оказания услуги или компонента услуги. Примечание 1 — Базовые конфигурации и принятые отступления от них составляют текущую информацию о конфигурации. Примечание 2 — Адаптировано из ИСО/МЭК/IEEE 24765:2010.	В ИСО/МЭК 20000-1 данный термин используется один раз, например см. подраздел 9.1: «...При вводе новой версии CI в рабочую среду нужно использовать базовые параметры конфигурации затрагиваемых CI.»
Элемент конфигурации (configuration item — CI)	Не определен	3.3 Элемент, подлежащий управлению, для того чтобы предоставить услугу или услуги	CI часто используется в ИСО/МЭК 20000-1 и рассматривается как компонент услуги. CI может быть единственным или частью компонентов услуг. См. в ИСО/МЭК 20000-1 определение 3.27 «компонент услуги»
База данных управления конфигурацией (configuration management database – CMDB)	Не определен	3.4 Хранилище данных, используемое для фиксирования атрибутов CI и взаимосвязей между CI в течение их жизненного цикла	В зависимости от подхода принятого организацией CMDB может быть использована для сохранения реестра активов. См. пункт А.7.1.1 приложения А ИСО/МЭК 27001
Постоянное совершенствование (continual improvement)	Не определен	3.5 Периодическая деятельность, направленная на расширение возможности выполнения требований к услугам. Примечание — Адаптировано из ИСО 9000:2005	Пункт 4.1.2 ИСО/МЭК 20000-1 требует наличия политики постоянного совершенствования в рамках политики менеджмента услуг. Во «Введение» к ИСО/МЭК 27001 включен цикл PDCA, очень сходный с циклом из ИСО 9001 и ИСО/МЭК 20000-1 (например, сравните пункт 4.2.4 ИСО/МЭК 27001 и пункт 4.5.5 ИСО/МЭК 20000-1)
Мера и средство контроля и управления	2.10 Средство менеджмента риска (2.34), включающее политики (2.28), процедуры (2.30), ре-	Не определен	Слово «control» используется в ИСО/МЭК 20000-1 как существительное, и как глагол, но не определяется как спе-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
(control)	комендации (2.16), практические приемы или организационные структуры, которые могут иметь административный, технический, управленческий или правовой характер. ИСО 31000:2009 2.26 Мера, которая модифицирует риск (2.1). Примечание 1 — Меры и средства контроля и управления включают любой процесс, политику, устройство, практический прием или иные действия, которые модифицируют риск. Примечание 2 — Меры и средства контроля и управления не всегда могут приводить к намеченному или предполагаемому модифицирующему результату. [ИСО Руководство 73:2009, определение 3.8.1.1]		циальный термин, поэтому применяется в обычном значении, присущем английскому языку: сущ.: полномочие или надзор; полномочие оказывать влияние или руководить; принять управление; средство ограничения (мера и средство контроля и управления), как устройство для управления, регулирования или тестирования (машина, система и т. д.); глагол: (находиться под контролем, контролировать) – иметь или осуществлять контроль над кем-то или над чем-то; регулировать; ограничивать; регламентировать; регулировать или тестировать (машина, система и т. д.). Все, кроме двух случаев использования термина «control» как существительного, приходятся на подраздел 6.6. «Менеджмент информационной безопасности» ИСО/МЭК 20000-1, другие используются в пунктах 4.3.2 и 4.4.3, где текст взят из ИСО 9001:2008 практически неизмененным. В качестве глагола «control» используется во многих местах, обычно как «контролировать XXX процесс» или «X должен находиться под контролем Y»
Цель применения мер и средств контроля и управления (control objective)	2.11 Формулировка, характеризующая, чего следует достичь в результате реализации мер и средств контроля и управления (2.10)	Не определен	Существительное «цель» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: нечто, к чему стремятся или желают; задача. Существует самая незначительная связь между понятием «цель применения мер и средств контроля и управления», используемым в ИСО/МЭК 27001, и выражениями, используемыми в ИСО/МЭК 20000-1, такими как «цели менеджмента услуг» (см. раздел 4) или «цели ме-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			неджмента информационной безопасности» (см. подраздел 6.6)
Корректирующее действие (corrective action)	2.12 Действие, предпринимаемое для устранения причины обнаруженного несоответствия или другой нежелательной ситуации. [ИСО 9000:2005]	3.6 Действие, предпринимаемое для устранения причины или снижения вероятности повторения обнаруженного несоответствия или другой нежелательной ситуации. Примечание — Адаптировано из ИСО 9000:2005	В обоих стандартах используется одинаковый термин, но существуют различия в значении. Не всегда возможно или желательно устранить причину, вместо этого может быть лучше или более рентабельно избежать повторения. См. в ИСО/МЭК 20000-1 определение 3.18 «предупреждающее действие»
Клиент (customer)	Не определен	3.7 Организация или часть организации, получающая услугу или услуги. Примечание 1 — Клиент может быть внутренним или внешним по отношению к организации-поставщику услуг. Примечание 2 — Адаптировано из ИСО 9000:2005.	В соответствии с ИСО/МЭК 20000-1 клиент дополнительно может действовать как поставщик
Документ (document)	Не определен	3.8 Информация, представленная на соответствующем носителе. [ИСО 9000:2005] ***Пример —Политики, планы, описания процессов, процедуры, соглашения об уровне услуг, договоры или записи.*** Примечание 1 — Документация может существовать в любой форме или на любом носителе данных. Примечание 2 — В ИСО/МЭК 20000, в документах за исключением записей излагается намерение, которое должно быть достигнуто	Нет прямого эквивалента
Результативность (effectiveness)	2.13 Степень реализации запланированной деятельности и достижения запланированных результатов. [ИСО 9000:2005]	3.9 Степень реализации запланированной деятельности и достижения запланированных результатов. [ИСО 9000:2005]	Идентично

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
Эффективность (efficiency)	2.14 Соотношение между достигнутыми результатами и тем, насколько рационально использовались ресурсы	Не определен	Это слово используется в обычном смысле, присущем английскому языку и только единожды, во введении к ИСО/МЭК 20000-1. Не существует требований, касающихся эффективности.
Событие (event)	2.15 Возникновение специфического набора обстоятельств. [ИСО/МЭК Руководство 73:2002]	Не определен	Слово «событие» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: что-то, что происходит или случается. Например, см. подраздел 6.2 ИСО/МЭК 27001: «значимые события» или пункт 6.3.2 «Планы обеспечения непрерывности и доступности услуг»: «если происходит событие, связанное с серьезной утратой услуг». Эти выражения аналогичны, используемым в ИСО/МЭК 27001, поэтому в целом сопоставимы. См. «событие информационной безопасности».
Рекомендация (guideline)	2.16 Описание того, что следует сделать для достижения цели	Не определен	См. другие части ИСО/МЭК 20000. Наряду с тем, что ИСО/МЭК 20000-1 содержит нормативные требования, все другие части ИСО/МЭК 20000 являются информационными стандартами или техническими отчетами
Влияние (impact)	2.17 Неблагоприятное изменение уровня достигнутых целей бизнеса	Не определен	Использование слова «влияние» в обоих стандартах является во многом сходным. «Влияние» в ИСО/МЭК 20000-1 используется 26 раз в обычном смысле, присущем английскому языку: влияние, сущ.: — сильный эффект или воздействие. Такое использование понятия «влияние» в ИСО/МЭК 20000-1 является менее конкретным, чем «влияние», используемое в ИСО/МЭК 27001. Большинство случаев использования этого понятия в ИСО/МЭК 20000-1 связано с риском или фактическими негативными обстоятельствами, например, см. опреде-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			ление 3.15 «известная ошибка» и в: - разделе 5: «Поставщик услуг должен использовать этот процесс для всех новых услуг или изменений к услугам, которые могут оказывать потенциально серьезное влияние на услуги или клиента», или; - пункте 6.3.2 «Поставщик услуг должен дать оценку влиянию запросов об изменении на план(ы) обеспечения непрерывности услуг и план(ы) обеспечения доступности»
Инцидент (incident)	См. «инцидент информационной безопасности»	3.10 Незапланированное прерывание услуги, снижение качества услуги или событие, которое еще не оказало влияние на услугу для клиента	Существует значительное различие между использованием слова «инцидент» в стандартах ИСО/МЭК 27001 и ИСО/МЭК 20000-1. Слово «инцидент» используется в ИСО/МЭК 27001 для обозначения «того, что с безопасностью в эксплуатационной среде что-то не так». В ИСО/МЭК 20000-1 слово «инцидент» имеет определенное значение и является более конкретным, чем в ИСО/МЭК 27001. В ИСО/МЭК 20000-1 «инцидент» является одним из серии родственных терминов и связан не только с инцидентами информационной безопасности. Другие родственные термины: - 3.19 Проблема (problem): Основная причина одного или нескольких инцидентов. На время создания записи о проблеме основная причина обычно неизвестна, и за дальнейшее расследование ответственность несет процесс менеджмента проблем; - 3.15 Известная ошибка (known error): Проблема, которая имеет установленную основную причину и метод снижения или устранения ее влияния на услугу путем ее обхода; - «Серьезный инцидент» (не определенный термин): Ин-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			цидент (или проблема), который(ая) рассматривается, как имеющий(ая) высшую категорию влияния. Менеджмент каждого «инцидента», «проблемы» и «серьезного инцидента» осуществляется по-разному, и к нему предъявляются разные требования. «Известная ошибка» является проблемой, в которой лежащая в ее основе причина понятна и управляема процессом менеджмента проблем, включающим требования, применяемые тогда, когда проблема становится известной ошибкой. Менеджмент «серьезного инцидента» осуществляется посредством процесса менеджмента инцидентов и менеджмента запроса услуг с требованием наличия специальной процедуры для менеджмента «серьезных инцидентов». См. «инцидент информационной безопасности»
Информационный актив (information asset)	2.18 Знания или данные, имеющие ценность для организации	Не определен	Этот термин не является определяемым термином, однако используется в ИСО/МЭК 20000-1, например, пункт 6.6.2: «Поставщик услуг должен реализовать и привести в действие физические, административные и технические меры и средства контроля и управления информационной безопасности для а) сохранения конфиденциальности, целостности и досягаемости (accessibility) информационных активов». См. «актив»
Информационная безопасность (information security)	2.19 Свойство информации сохранять конфиденциальность (2.13), целостность (2.36) и доступность (2.10) информации. Примечание — Кроме того, данный термин может также включать и дру-	3.11 Сохранение конфиденциальности, целостности и досягаемости (accessibility) информации. Примечание 1 — Дополнительно могут также затрагиваться и другие свойства, такие как аутентич-	В ИСО/МЭК 20000-1 слово «доступность (availability)» не может быть использовано в определении информационной безопасности (3.11), поскольку доступность является термином, имеющим другое значение (см. «доступность (availability)»). Таким образом,

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
	гие свойства, такие как аутентичность (2.9), подотчетность (2.2), неотказуемость (2.49) и достоверность (2.56)	ность, подотчетность, неотказуемость и достоверность. Примечание 2 — Термин «доступность (availability)» не был использован в этом определении, поскольку он является определяемым термином в этой части ИСО/МЭК 20000, который не соответствует этому определению. Примечание 3 — Адаптирован из ИСО/МЭК 27000:2009	определение понятия «информационная безопасность» было адаптировано для использования термина «досягаемость (accessibility)». Определение «досягаемость (accessibility)» взято из определения «доступность» ИСО/МЭК 27000 как «свойство досягаемости и используемости по запросу уполномоченной сущности».
Событие информационной безопасности (information security event)	2.20 Установленное проявление состояния системы, услуги или сети, указывающее на возможное нарушение информационной безопасности (2.19), политики (2.28) или неосуществление мер и средств контроля и управления (2.10), или на ранее неизвестную ситуацию, которая может иметь отношение к безопасности	Не определен	«Событие информационной безопасности» применяется в ИСО/МЭК 20000-1 только как часть понятия 3.12 «инцидент информационной безопасности». Кроме того, «событие» 2.15 (не являющееся событием информационной безопасности) также используется в: a) определении риска – см. 3.25, включающем примечания 3 и 4, в которых упоминаются события; b) определении «обеспечение непрерывности услуг» (3.28); c) подразделе 6.2 «Отчетность по услугам» ИСО/МЭК 20000-1; d) пункте 6.3.2. «Планы обеспечения непрерывности и доступности услуг» ИСО/МЭК 20000-1. См. «событие»; одно или несколько событий могут быть частью инцидента безопасности
Инцидент информационной безопасности (information security incident)	2.21 Единичное событие или серия нежелательных или неожиданных событий информационной безопасности (2.20), которые обладают значительной вероятностью компрометации операций бизнеса и создания угрозы для информационной безопасности (2.19)	3.12 Единичное событие или серия нежелательных или неожиданных событий информационной безопасности, которые обладают значительной вероятностью компрометации операций бизнеса и создания угрозы для информационной безопасности [ИСО/МЭК 27000:2009]	Определение 3.12 ИСО/МЭК 20000-1 включает формулировку «инцидент информационной безопасности» из ИСО/МЭК 27000. Пункт 6.6.3 ИСО/МЭК 20000-1 содержит требование: Инцидентами информационной безопасности следует управлять с использованием процедур менеджмента инцидентов с приоритетом, соответствующим риску информационной безопасности.

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			Это не принимает во внимание «то, что услуга не оказывается как надо», поскольку причиной является проблема, лежащая в основе одного или более инцидентов, хотя во время создания записи о проблеме основная причина обычно неизвестна, и за дальнейшее рассмотрение отвечает процесс менеджмента проблем. С проблемами справляются посредством процесса менеджмента проблем, а не процесса менеджмента инцидентов и запроса услуг. Менеджмент серьезных инцидентов информационной безопасности осуществляется посредством упомянутого процесса менеджмента инцидентов и запроса услуг. Различия в особенностях терминов, используемых в разных стандартах, более сложны, чем события или инциденты безопасности, являющиеся подклассом или определенным типом инцидентов менеджмента услуг (см. пункт 6.2.5 данного стандарта)
Менеджмент инцидентов информационной безопасности (information security incident management)	2.22 Процессы (2.31) обнаружения, сообщения, оценки, реагирования, урегулирования (2.21) и извлечения уроков из инцидентов информационной безопасности	Не определен	См.: - «инцидент»; - «инцидент информационной безопасности»; - «известная ошибка»; - «проблема»
Система менеджмента информационной безопасности (СМИБ) (information security management system – ISMS)	2.23 Часть общей системы менеджмента (2.26), основанная на подходе к рискам бизнеса, которая устанавливает, реализует, управляет, осуществляет мониторинг, проверяет, поддерживает и совершенствует информационную безопасность (2.19)	Не определен	См. «система менеджмента услуг» и «система менеджмента»
Риск информацион-	2.24 Возможность того, что угроза	Не определен	См. «риск». Риск информационной безо-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
ной безопасности (information security risk)	(2.45) будет использовать уязвимость (2.46) актива (2.3) или группы активов и, тем самым, причинит ущерб организации		пасности не определяется, но используется в разделе ИСО/МЭК 20000-1, касающемся менеджмента информационной безопасности, пункт 6.6.1
Целостность (integrity)	2.25 Свойство сохранять точность и полноту активов (2.3)	Не определен	Слово «целостность» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: свойство или состояние быть целым и неповрежденным. (Например, см. пункт 6.6.2 ИСО/МЭК 20000-1: «Поставщик услуг должен реализовать и привести в действие физические, административные и технические меры и средства контроля и управления информационной безопасности для: а) сохранения конфиденциальности, целостности и досягаемости (accessibility) информационных активов». Подраздел 9.1 ИСО/МЭК 20000-1 включает требования: - «Должны быть документально оформлены процедуры записи, управления и отслеживания версий CI. Целостность услуг и компонентов услуг, с учетом требований к услугам и риска, связанного с CI, должны поддерживаться соответствующим уровнем управления.» - «Изменения CI должны быть прослеживаемыми и проверяемыми для обеспечения уверенности в целостности CI и данных в CMDB.» Подраздел 9.3 ИСО/МЭК 20000-1 включает требования: «Изменения следует внедрять в рабочую среду так, чтобы целостность аппаратных средств, программного обеспечения и других компонентов услуг поддерживалась во время внедрения изменения»
Заинтересованная сторона (inter-	Не определен	3.13 Лицо или группа, имеющие особую заинтересованность в	См. «поставщик услуг»

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
ested party)		функционировании, успехе действия или деятельности поставщика услуг. ***Пример —клиенты, владельцы, руководство, работники организации-поставщика услуг, поставщики, банкиры, объединения или партнеры.*** Примечание 1 — Группа может включать организацию, часть организации или несколько организаций. Примечание 2 — Адаптировано из ИСО 9000:2005	
Внутренняя группа (internal group)	Не определен	3.14 Часть организации-поставщика услуг, вступающая в документально оформленное соглашение с поставщиком услуг для содействия проектированию, развитию, предоставлению и совершенствованию услуг. Примечание — Внутренняя группа находится вне сферы действия SMS поставщика услуг	См. «поставщик услуг»
Известная ошибка (known error)	Не определен	3.15 Проблема, которая имеет установленную основную причину, метод снижения или устранения ее воздействия на услуги путем ее обхода	См. «инцидент» и «проблема»
Система менеджмента (management system)	2.26 Структура, включающая политики (2.28), процедуры (2.30), рекомендации (2.16) и взаимосвязанные ресурсы для достижения целей организации	Система менеджмента определяется в примечании 1 определения системы менеджмента услуг: «Примечание 1 — Система менеджмента является совокупностью взаимосвязанных или взаимодействующих элементов для создания политики и целей, а также для достижения этих целей»	Используется в ИСО/МЭК 20000-1 для упоминания «других систем менеджмента», в ИСО/МЭК 20000-1 называется как «система менеджмента услуг»
Неотказуемость (non-repudiation)	2.27 Возможность подтвердить происхождение заявленного события (2.15) или действия и наличие сущностей, от которых оно исходит, с целью	Не определен или не используется	Нет прямого эквивалента

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
	разрешения споров о возникновении или не возникновении события (2.15) или действия и вовлечения сущностей в это событие (2.15)		
Организация (organization)	Не определен	3.17 Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений. ***Пример — Компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, предприятие розничной торговли, ассоциация, а также их подразделения или комбинация из них.*** Примечание 1 — Распределение обычно является упорядоченным. Примечание 2 — Организация может быть государственной или частной. [ИСО 9000:2005]	В ИСО/МЭК 20000-1 используются термины «поставщик услуг» и «организация» для разных сущностей, поскольку в любых пояснениях для интегрированной системы менеджмента различие является существенным. См. «поставщик услуг»
Политика (policy)	2.28 Общая концепция и направление деятельности, формально выраженные руководством	Не определен	Слово «политика» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: (политика) план действий, обычно основанный на определенных принципах, выбранных органом или лицом; принцип или совокупность принципов, на которых должны основываться решения; линия поведения, которой нужно придерживаться. Политики в ИСО/МЭК 20000-1 используются для руководящих указаний. Некоторые из них требуются стандартом ИСО/МЭК 20000-1, включая политику менеджмента услуг. Использование их в основном одинаково в обоих стандартах
Предупреждающее действие (preventive action)	2.29 Действие, предпринятое для устранения причин потенциального несоответствия или иной потенциально нежелательной ситуации.	3.18 Действие по избеганию, или устранению причины или уменьшению вероятности возникновения потенциального несоответствия или иной	Определения различаются, так как определение в ИСО/МЭК 20000-1 было расширено, чтобы включить: предупреждающее действие, которое не устраняет причи-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
	[ИСО 9000: 2005]	потенциально нежелательной ситуации. Примечание — Адаптировано из ИСО 9000:2005	ну, но каким-то образом обходит ее, чтобы избежать влияния. В обоих стандартах используется одинаковый термин, но существуют различия в его значении. Не всегда можно или нужно принимать предупреждающие действия в рамках менеджмента услуг. Вместо этого может быть лучше / эффективнее по затратам избежать повторного проявления. Поэтому, чтобы учесть такую возможность, определение из ИСО 9000 было адаптировано в ИСО/МЭК 20000-1. Это связывает корректирующее действие в ИСО/МЭК 20000-1 (определении 3.6) и ИСО/МЭК 27000 (определении 2.12)
Проблема (problem)	Не определен	3.19 Основная причина одного или нескольких инцидентов. Примечание — Во время создания записи о проблеме основная причина обычно неизвестна, и за дальнейшее рассмотрение отвечает процесс менеджмента проблем	См. «инцидент» и «известная ошибка»
Процедура (procedure)	2.30 Установленный способ осуществления деятельности или процесса (2.31). [ИСО 9000:2005]	3.20 Установленный способ осуществления деятельности или процесса. [ИСО 9000:2005] Примечание — Процедуры могут быть документированными или недокументированными	Оба определения основаны на ИСО 9000. В общих чертах они сходны. Отличаются только примечания, т. е. процедуры могут быть недокументированными, однако в ИСО/МЭК 20000-1 все процедуры упоминаются как «документированные процедуры». Те процедуры, которые являются частью плана, документируются как часть этого плана
Процесс (process)	2.31 Совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы. [ИСО 9000:2005]	3.21 Совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы. [ИСО 9000:2005]	Оба определения, основанные на ИСО 9000:2005, одинаковы
Запись (record)	2.32 Документ, содержащий достигнутые результаты или	3.22 Документ, содержащий достигнутые результаты или	Оба определения, основанные на ИСО 9000:2005, одинаковы

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
	свидетельства осуществленной деятельности. [ИСО 9000:2005]	свидетельства осуществленной деятельности. [ИСО 9000:2005] ***Пример — Отчеты о результатах аудита, отчеты об инцидентах, записи об обучении или протоколы совещаний***	
Выпуск (release)	Не определен или не используется	3.23 Совокупность одного или нескольких новых или измененных CI, введенных в рабочую среду в результате одного или более изменений	Нет прямого эквивалента
Достоверность (reliability)	2.33 Свойство непротиворечивого предусмотренного поведения и результатов	Имеет отношение к информационной безопасности в пункте 3.11: «Примечание 1 — Дополнительно данный термин может также включать и другие свойства, такие как, аутентичность, подотчетность, неотказуемость и достоверность»	Слово «достоверность (reliability)» используется в ИСО/МЭК 20000-1 в обычном смысле, присущем английскому языку: надежность (trustworthiness). См. подраздел 9.1 ИСО/МЭК 20000-1: «Должен осуществляться менеджмент CMDB для обеспечения уверенности в ее точности и достоверности, включая управление доступом для обновления»
Запрос об изменении (request for change)	Не определен или не используется	3.24 Предложение об изменении которое должно быть внесено в услугу, компонент услуги или систему менеджмента услуг. Примечание — Изменение услуги включает предоставление новой услуги или отмену услуги, которая больше не нужна	В приложении А ИСО/МЭК 27001 говорится о «менеджменте изменений» как о мере и средстве контроля и управления в А.10.1.2. Многие меры и средства контроля и управления в ИСО/МЭК 27001 касаются управления или контроля изменений. Например, А.8.3, А.10.1, А.10.2.3, А.12.5.1
Риск (risk)	2.34 Сочетание вероятности события (2.15) и его последствий. [ИСО/МЭК Руководство 73:2002]	3.25 Влияние неопределенности на цели. Примечание 1 — Влияние представляет собой отклонение от ожидаемого – позитивное и (или) негативное. Примечание 2 — Цели могут иметь различные аспекты (например, финансовые, аспекты техники безопасности и охраны труда, экологические) и могут при-	В стандартах ИСО/МЭК 20000 явные случаи использования термина «риск» ограничены, хотя многие упреждающие аспекты менеджмента услуг направлены на снижение риска. Следует отметить, что концепция «риска», принятая в перерабатываемом ИСО/МЭК 27001, такая же, как в ИСО/МЭК 20000-1, основана на ИСО 31000. См. «уязвимость»

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
		меняться на разных уровнях (например, стратегическом, в масштабах организации, для проекта, продукта и процесса). Примечание 3 — Риск часто характеризуется ссылкой на потенциальные события и последствия или на их комбинацию. Примечание 4 — Риск часто выражается с точки зрения комбинации последствий события (включая изменения обстоятельств) и соответствующей вероятности их возникновения. [ИСО 31000:2009]	
Принятие риска (risk acceptance)	2.35 Решение о принятии риска (2.34). [ИСО/МЭК Руководство 73:2002]	Не определен	Термин «принятие риска» не определен и не используется в ИСО/МЭК 20000-1. Тем не менее, в ИСО/МЭК 20000-1 имеются требования для определения критериев принятия риска в плане по менеджменту услуг (пункт 4.5.2) и в процессе менеджмента информационной безопасности (пункт 6.6.1). Аналогичные понятия имеются в подразделе 5.4 в требованиях по использованию критериев принятия
Анализ риска (risk analysis)	2.36 Систематическое использование информации для идентификации источников риска и количественной оценки риска (2.34). [ИСО/МЭК Руководство 73:2002] Примечание – Анализ риска обеспечивает основу для оценивания риска (2.41), обработки риска (2.43) и принятия риска (2.35)	Не определен	См. «оценка риска». Следует обращать особое внимание на то, что «анализ риска» – это определенно не то же самое, что «принятие риска» — для справки см. ИСО/МЭК 27005
Оценка риска (risk assessment)	2.37 Общий процесс (2.31) анализа риска (2.36) и оценивания риска (2.41). [ИСО/МЭК Руководство 73:2002]	Не определен	Ссылки на оценку риска в ИСО/МЭК 20000-1 связаны с услугами. Например: - пункт 4.5.3: (Реализация и введение в действие СМУ (Осуществление)) включает «... d) идентификацию, оценку и менеджмент рисков для услуг»; - подраздел 5.2: (Планирова-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			ние новых или измененных услуг) включает «f) идентификацию, оценку и менеджмент рисков»; - пункт 6.6.1: «d) обеспечение уверенности в проведении оценок риска информационной безопасности через запланированные интервалы времени»
Коммуникация риска (risk communication)	2.38 Обмен информацией о риске (2.34) или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами. [ИСО/МЭК Руководство 73:2002]	Не определен	Не используется в ИСО/МЭК 20000-1 ни в одном аспекте, непосредственно связанным с риском
Критерии риска (risk criteria)	2.39 Правила, в соответствии с которыми производят оценивание значимости риска (2.34). [ИСО/МЭК Руководство 73:2002]	Не определен	Используется в ИСО/МЭК 20000-1 подобно его использованию в стандарте ИСО/МЭК 27001: Пункт 4.5.2 ИСО/МЭК 20000-1: «План менеджмента услуг должен включать или содержать ссылку на ... j) подход, который должен быть принят в отношении менеджмента рисков и критериев принятия рисков». Понятие является сходным для обоих стандартов, но имеет большее значение для ИСО/МЭК 27001, чем для ИСО/МЭК 20000-1
Количественная оценка риска (risk estimation)	2.40 Процесс присвоения значений вероятности и последствиям риска (2.34). [ИСО/МЭК Руководство 73:2002]	Не определен	См. «оценка риска»
Оценивание риска (risk evaluation)	2.41 Процесс (2.31) сравнения количественно оцененного риска (2.34) с установленными критериями риска (2.39) для определения значимости риска (2.34). [ИСО/МЭК Руководство 73:2002]	Не определен	См. «оценка риска»
Менеджмент риска (risk man-	2.42 Скоординированные действия по руководству и управ-	Не определен	В общих чертах одинаковое значение в обоих стандартах

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
agement)	лению организацией в отношении риска (2.34). [ИСО/МЭК Руководство 73:2002] Примечание — Обычно менеджмент риска включает оценку риска (2.37), обработку риска (2.43), принятие риска (2.35), коммуникацию риска (2.38), мониторинг риска и проверку риска		
Обработка риска (risk treatment)	2.43 Процесс (2.31) выбора и реализации мер по модификации риска (2.34). [ИСО/МЭК Руководство 73:2002]	Не определен	Термин «обработка риска» не используется в ИСО/МЭК 20000-1; этот термин охвачен термином «менеджмент риска» (см. примеры в «оценке риска»)
Услуга (service)	Не определен	3.26 Средство предоставления ценности клиенту посредством содействия результатам, которых клиент хочет достичь. Примечание 1 — Услуга обычно нематериальна. Примечание 2 — Услуга также может быть передана провайдеру услуг поставщиком, внутренней группой или клиентом, действующим как поставщик	Нет прямого эквивалента
Компонент услуги (service component)	Не определен	3.27 Единичный элемент услуги, который при соединении с другими элементами будет предоставлять полную услугу. ***Пример — аппаратные средства, программное обеспечение, инструментальные средства, приложения, документация, информация, процессы или вспомогательные услуги.*** Примечание — Компонент услуги может состоять из одного или нескольких CI	Нет прямого эквивалента
Обеспечение непрерывности услуг (ser-	Не определен	3.28 Возможность осуществления менеджмента рисков и событий, которые могли бы ока-	См. «уязвимость» и «риск». См. «обеспечение непрерывности бизнеса». Непрерывность услуги обычно понима-

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
vice continuity)		зать серьезное влияние на услугу или услуги для того, чтобы постоянно предоставлять услуги на согласованных уровнях	ется как подсовокупность обеспечения непрерывности бизнеса
Соглашение об уровне услуг (service level agreement – SLA)	Не определен	3.29 Документально оформленное соглашение между поставщиком услуг и клиентом, в котором определены услуги и цели услуг. Примечание 1 — Соглашение об уровне услуг может также устанавливаться между поставщиком услуг и поставщиком, внутренней группой или клиентом, действующими как поставщик. Примечание 2 — Соглашение об уровне услуг может быть включено в договор или иной вид документально оформленного соглашения	Этот термин не используется в ИСО/МЭК 27001. Однако понятие применяется по отношению к цели применения мер и средств контроля и управления А.10.2, когда рассматриваются аспекты безопасности услуги, предоставляемой и поддерживаемой третьей стороной, например, мера и средство контроля и управления А.10.2.1 (согласованные уровни обеспечения непрерывности услуг)
Менеджмент услуг (service management)	Не определен	3.30 Совокупность возможностей и процессов по руководству и контролю деятельности и ресурсов поставщика услуг при проектировании, развитии, предоставлении и совершенствовании услуг для выполнения требований к услугам	Цель применения мер и средств контроля и управления А.10.2 ИСО/МЭК 27001 связана с этим термином
Система менеджмента услуг – СМУ (service management system – SMS)	Не определен	3.31 Система менеджмента для руководства и управления деятельностями, связанными с менеджментом услуг в отношении поставщика услуг. Примечание 1 — Система менеджмента – это совокупность взаимосвязанных или взаимодействующих элементов для установления политики и целей, а также для достижения этих целей. Примечание 2 — СМУ включает все политики, цели, планы, процессы, документацию и ресурсы менеджмента услуг, которые необходимы для проектирования, развития, предоставления и совершенствования услуг и выполнения требова-	См. «система менеджмента информационной безопасности (СМИБ)»

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
		ний в этой части ИСО/МЭК 20000. Примечание 3 — Адаптировано из определения «система менеджмента качества» ИСО 9000:2005	
Поставщик услуг (service provider)	Не определен	3.32 Организация или часть организации, осуществляющая менеджмент и предоставление услуги или услуг клиенту. Примечание — Клиент может быть внутренним или внешним по отношению к организации-поставщику услуг	Поставщик услуг в ИСО/МЭК 20000-1 (определение 3.32) является организацией, стремящейся выполнять требования ИСО/МЭК 20000-1. Этот термин используется, потому что он проводит различие между поставщиком услуг и другими группами, являющимися клиентами, другими частями (поставщики, внутренние группы, клиенты, действующие как поставщики) внешних организаций, заинтересованными сторонами или поставщиками продуктов или инструментальных средств, поддерживающих функционирование СМУ. Поставщик услуг может быть частью более крупной организации или целой организацией.
Запрос услуги (service request)	Не определен или не используется	3.33 Запрос информации, консультации, доступа к услуге или заранее утвержденного изменения	Нет прямого эквивалента
Требование к услуге (service requirement)	Не определен	3.34 Потребности клиента или пользователей в услугах, включающие требования к уровню услуг, а также потребности поставщика услуг	«Требование к услуге» определено в ИСО/МЭК 20000-1 (см. определении 3.34). В ИСО/МЭК 27001 «требование» используется в обычном смысле, присущем английскому языку: необходимо, то, что попросил, необходимо, заказано. «Требование» в ИСО/МЭК 27001 не используется в значении «требования к услуге», хотя в нем существует несколько применений «требований безопасности», законодательных или нормативных требований и т. д.
Поставщик (supplier)	Не определен	3.35 Организация или часть организации, являющаяся внешней по отношению к органи-	ИСО/МЭК 20000-1 содержит ссылки на требования и сами требования к менеджменту относительно:

Продолжение таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
		зации-поставщику услуг, и заключающая договор с поставщиком услуг о содействии проектированию, развитию, предоставлению и совершенствованию услуг или процессов. Примечание — К поставщикам относятся назначенные ведущие поставщики, а не их поставщики-субподрядчики	a) поставщиков; b) ведущих поставщиков (осуществляющих управление субподрядчиками поставщиков); c) внутренних групп (вносящих вклад в услугу); d) клиентов (действующих в качестве поставщиков). Все это способствует услуге в целом и управляется поставщиком услуги. Менеджмент поставщика охватывает поставщиков / ведущих поставщиков (а через ведущих поставщиков – субподрядчиков поставщиков). Менеджмент уровня услуг охватывает менеджмент внутренних групп и клиентов, действующих в качестве поставщиков. В ИСО/МЭК 27001 термин «поставщик» используется только один раз
Положение о применимости (statement of applicability)	2.44 Документ, определяющий цели применения мер и средств контроля и управления (2.11) и меры и средства контроля и управления (2.10), являющиеся адекватными и применимыми для СМИБ (2.23) организации	Не определен или не используется	Подраздел 1.2 «Применение» ИСО/МЭК 20000-1, не является идентичным положению о применимости в ИСО/МЭК 27001
Угроза (threat)	2.45 Потенциальная причина нежелательного инцидента, который может нанести вред системе или организации	Не определен	В ИСО/МЭК 20000-1 термин «создание угрозы» используется единожды в определении 3.12: «Инцидент информационной безопасности – это единичное событие или серия нежелательных или неожиданных событий, связанных с информационной безопасностью, которые обладают значительной вероятностью компрометации деятельности бизнеса и создания угрозы для информационной безопасности»
Развитие (transition)	Не определен	3.37 Деятельность, связанная с внедрением новой или измененной услуги в рабочую среду или из нее	Существует связь между развитием, использованным в разделе 5 ИСО/МЭК 20000-1, и способом управления некоторыми изменениями согласно ИСО/МЭК 27001. Процес-

Окончание таблицы В.1

Термин	ИСО/МЭК 27000:2009	ИСО/МЭК 20000-1:2011	Комментарии по использованию терминов в обоих стандартах
			сы управления, описанные в разделах 5 и 9 ИСО/МЭК 20000-1, тесно связаны с этой концепцией. ISO/IEC 27001 обсуждает менеджмент изменений в следующих пунктах: - А.10.1.2 «Менеджмент изменений операционных процедур и обязанностей»; - А.10.2.3 «Менеджмент изменений сер висов третьей стороны».-
Уязвимость (vulnerability)	2.46 Недостаток актива (2.3) или меры и средства контроля и управления (2.10), который может быть использован угрозой (2.45)	Не определен или не используется	Нет прямого эквивалента

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 20000-1:2011	IDT	ГОСТ Р ИСО/МЭК 20000-1–2013 Информационная технология. Менеджмент услуг. Часть 1. Требования к системе менеджмента услуг
ИСО/МЭК 27000:2009	IDT	ГОСТ Р ИСО/МЭК 27000–2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001–2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

Библиография

[1] ISO 9000, Quality management systems – Fundamentals and vocabulary

[2] ISO 9004, Quality management systems – Guidelines for performance improvements

[3] ISO/IEC TS 15504-8, Information technology – Service management – Part 8: Process assessment mode for service management (under development)

[4] ISO 19011, Quality management systems – Guidelines for quality and/or environmental management systems auditing

[5] ISO/IEC 20000-2, Information technology – Service management – Part 2: Guidance on the application of service management systems

[6] ISO/IEC 20000-3, Information technology – Service management – Part 3: Guidance on scope definition and applicability for ISO/IEC 20000-1

[7] ISO/IEC TR 20000-4, Information technology – Service management – Part 4: Process reference model for service management

[8] ISO/IEC TR 20000-5, Information technology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1

[9] ISO/IEC TR 90006, Information technology – Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011

[10] ISO/IEC 27002, Information technology – Security techniques – Information security management systems – Code of practice for information security controls (under revision)

[11] ISO/IEC 27003, Information technology – Security techniques – Information security management systems – Information security management system implementation guidance

[12] ISO/IEC 27004, Information technology – Security techniques – Information security management systems – Information security management measurements

[13] ISO/IEC 27005, Information technology – Security techniques – Information security management systems – Information security risk management

[14] ISO/IEC 27006, Information technology – Security techniques – Information security management systems – Requirements for bodies providing audit and certification of information security management systems

[15] ISO/IEC 27007, Information technology – Security techniques – Information security management systems – Guidelines for information security management systems auditing

[16] ISO/IEC TR 27008, Information technology – Security techniques – Guidelines for auditors on information security controls

[17] ISO/IEC 27010, Information technology – Security techniques – Information security management systems – Information security management for inter-sector and inter-organizational communications

[18] ISO/IEC 27014, Information technology – Security techniques – Information security management systems – Governance of information security

[19] ISO 31000, Risk management – Principles and Guidelines on Implementation

УДК 006.034: 004.056: 004.057.2

ОКС 03.080.99

35.020;

35.040;

Ключевые слова: информационная технология, информационная безопасность, мера и средство контроля и управления, система менеджмента информационной безопасности, менеджмент услуг, интегрированная система менеджмента

Подписано в печать 02.12.2014. Формат 60x84¼.
Усл. печ. л. 5,58. Тираж 000 экз. Зак. 0000

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»,
123995 Москва, Гранатный пер., 4.

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

gost.e-ecolog.ru