Утвержден и введен в действие
Приказом Федерального
агентства по техническому
регулированию и метрологии
от 17 октября 2014 г. N 1351-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ МЕНЕДЖМЕНТА НЕПРЕРЫВНОСТИ БИЗНЕСА

ОБЩИЕ ТРЕБОВАНИЯ

Business continuity management systems. Requirements

ISO 22301:2012
Societal security - Business continuity management systems - Requirements
(IDT)

ГОСТ Р ИСО 22301-2014

Группа Т59

ОКС 29.020
91.120.40

Дата введения
1 декабря 2015 года

Предисловие

1. Подготовлен Открытым акционерным обществом "Научно-исследовательский центр контроля и диагностики технических систем" (АО "НИЦ КД") на основе собственного аутентичного перевода международного стандарта, указанного в разделе 4.

2. Внесен Техническим комитетом по стандартизации ТК 10 "Менеджмент риска".

3. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2014 г. N 1351-ст.

4. Настоящий стандарт идентичен международному стандарту ИСО 22301:2012 "Социальная безопасность. Системы менеджмента непрерывности бизнеса. Требования" (ISO 22301:2012 "Societal security - Business continuity management systems - Requirements").

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5-2012 (подраздел 3.5).

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

5. Введен впервые.

Правила применения настоящего стандарта установлены в 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).

Введение

0.1. Общие положения

Настоящий стандарт устанавливает требования к созданию и управлению эффективной системой менеджмента непрерывности бизнеса (СМНБ).

СМНБ подчеркивает важность:

- понимания потребностей организации и необходимости установления политики и целей в области непрерывности бизнеса,

- внедрения средств и показателей управления общей способностью организации противостоять разрушительным инцидентам,

- анализа и мониторинга выполнения и результативности СМНБ,

- непрерывного совершенствования, основанного на объективных измерениях.

Ключевыми элементами СМНБ, как и любой другой системы менеджмента, являются:

a) политика;

b) люди с установленными обязанностями;

c) процессы управления, относящиеся к:

1) политике;

2) планированию;

3) внедрению и функционированию;

4) оценке выполнения;

5) анализу со стороны руководства;

6) совершенствованию;

d) документация, обеспечивающая доказательства соответствия;

e) все процессы управления непрерывностью бизнеса в организации.

Непрерывность бизнеса способствует устойчивости общества. В процесс восстановления организации после разрушительных инцидентов может быть вовлечено общество и другие

организации.

0.2. Модель "Планирование-Выполнение-Проверка-Действие" (PDCA)

Настоящий стандарт использует модель PDCA для планирования, установления, внедрения, функционирования, мониторинга, поддержки и непрерывного совершенствования результативности СМНБ организации.

Стандарт обеспечивает определенную степень соответствия другим стандартам в области систем менеджмента, таким как ИСО 9001:2008 "Система менеджмента качества. Требования", ИСО 14001:2004 "Системы экологического менеджмента. Требования и руководство по применению", ИСО/МЭК 27001:2013 "Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования", ИСО/МЭК 20000-1:2011 "Информационные технологии. Менеджмент услуг. Часть 1. Требования к системе менеджмента услуг", и ИСО 28000:2007 "Системы менеджмента безопасности цепи поставок. Технические условия".

На рисунке 1 показано, как СМНБ, используя на входе заинтересованные стороны и требования к управлению непрерывностью бизнеса и посредством необходимых действий и процессов, получает результаты (то есть управляемую непрерывность бизнеса), отвечающие этим требованиям.

Рисунок 1. Модель PDCA, примененная к процессам СМНБ

Таблица 1

Объяснение модели PDCA

Планирование (Установление)	Установление политики в области непрерывности бизнеса, целей, задач, элементов управления, процессов и процедур, важных для совершенствования непрерывности бизнеса. Результаты должны поддерживать общую политику и задачи организации
Выполнение (Внедрение и работа)	Внедрение и работа политики непрерывности бизнеса, средств управления, процессов и процедур
Проверка (Наблюдение и контроль)	Отслеживание и анализ выполнения СМНБ с учетом политики и целей, сообщение результатов руководству, определение и санкционирование действий для исправления и совершенствования
Действие (Поддержка и совершенствование)	Поддержка и совершенствование СМНБ с помощью принятия корректирующих действий, основанных на результатах анализа менеджмента и пересмотре области применения СМНБ, а также политики и целей непрерывности бизнеса

0.3. Компоненты PDCA в настоящем стандарте

Разделы 4 - 10 настоящего стандарта посвящены следующим элементам модели "Планирование-Выполнение-Проверка-Действие".

- В разделе 4 (Планирование) приведены требования, необходимые для установления условий СМНБ в организации, а также к ее потребностям, требованиям и области применения.

- В разделе 5 (Планирование) приведены требования к функциям высшего руководства в СМНБ и описано, как высшее руководство выражает свои ожидания в отношении организации посредством установления политики в области непрерывности бизнеса.

- В разделе 6 (Планирование) приведены требования, относящиеся к установлению стратегических целей и руководящих принципов СМНБ в целом. Содержание раздела 6 отличается от установления возможных вариантов обработки риска, выявляемых при оценке риска, так же как и целей восстановления, выявляемых во время анализа воздействия на бизнес (BIA).

Примечание. Требования к процессу анализа воздействия на бизнес и оценке риска приведены в разделе 8.

- Раздел 7 (Планирование) посвящен функционированию СМНБ в части установления компетентности и обмена информацией с заинтересованными сторонами и включает рекомендации по управлению, поддержке и сохранению требуемой документации.

- В разделе 8 (Выполнение) установлены требования к обеспечению непрерывности бизнеса, порядок разработки процедур управления в условиях инцидента.

- В разделе 9 (Проверка) приведены требования, необходимые для выполнения измерений в области менеджмента непрерывности бизнеса, соответствия СМНБ требованиям настоящего стандарта и ожиданиями руководства, и обратной связи с руководством относительно его ожиданий.

- В разделе 10 (Действие) идентифицированы корректирующие действия по устранению несоответствий СМНБ.

1. Область применения

В настоящем стандарте установлены требования к планированию, созданию, внедрению, функционированию, мониторингу, поддержке в рабочем состоянии и постоянному улучшению документированной системы менеджмента для защиты от инцидентов, снижения вероятности их реализации, подготовки ответных действий и восстановления после инцидентов при их возникновении.

Требования, установленные в настоящем стандарте, являются универсальными и применимы ко всем организациям независимо от типа, размера и других особенностей. Применимость этих требований зависит от производственной среды, структуры и других особенностей организации.

Настоящий стандарт не устанавливает единообразную структуру системы менеджмента непрерывности бизнеса (СМНБ). Стандарт помогает организовать проектирование СМНБ, соответствующей потребностям организации и требованиям заинтересованных сторон. Эти требования формируются в зависимости от юридических, нормативных, организационных и производственных требований, особенностей продукции и услуг, используемых процессов, размера и структуры организации, а также требований заинтересованных сторон.

Настоящий стандарт применим к организациям всех типов и размеров, которые имеют намерения:

a) установить, внедрить, поддерживать и улучшать СМНБ;

b) обеспечить соответствие деятельности организации установленной политике в области непрерывности бизнеса;

c) демонстрировать это соответствие другим сторонам;

d) провести сертификацию/регистрацию своей СМНБ независимым аккредитованным органом по сертификации;

e) самостоятельно проверять и декларировать соответствие СМНБ требованиям настоящего стандарта.

Настоящий стандарт может быть использован для оценки способности организации удовлетворять ее потребностям и обязательствам в области непрерывности бизнеса.

2. Нормативные ссылки <1>

<1> Разделу присвоен номер для сохранения идентичности стандарта.

В настоящем стандарте нет ссылок на нормативные документы.

3. Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

3.1. Деятельность (activity): процесс или система процессов, осуществляемых организацией с целью производства одного или более видов продукции, оказания услуг или их поддержки.

Пример - Примером подобных процессов являются бухгалтерский учет, обеспечение информационных (ИТ) и телекоммуникационных технологий, производство, сбыт.

3.2. Аудит (audit): систематический, независимый и документированный процесс получения свидетельств аудита и их объективной сравнительной оценки с целью установления степени выполнения согласованных критериев аудита.

Примечание 1. Термин "независимый" не обязательно означает "сторонний по отношению к организации". В большинстве случаев, особенно в небольших организациях, независимость может означать, что аудитор не отвечает за выполнение той деятельности, которая является предметом аудита.

Примечание 2. Дополнительные справочные материалы по фактическим данным и критериям аудита см. в ИСО 19011 [3].

3.3. Непрерывность бизнеса (business continuity): стратегическая и тактическая способность организации планировать свою работу в случае инцидента и нарушения ее деятельности, направленная на обеспечение непрерывности деловых операций на установленном приемлемом уровне.

[ИСО 22300]

3.4. Менеджмент непрерывности бизнеса (business continuity management): полный процесс управления, предусматривающий идентификацию потенциальных угроз и их воздействия на деятельность организации, который создает основу для повышения устойчивости организации к инцидентам и направлен на реализацию эффективных ответных мер против, что обеспечивает защиту интересов ключевых причастных сторон, репутации организации, ее бренда и деятельности, добавляющей ценность.

3.5. Система менеджмента непрерывности бизнеса (business continuity management system, BCMS) СМНБ: часть общей системы менеджмента, которая направлена на установление, внедрение, осуществление, управление, мониторинг, анализ, поддержку и постоянное улучшение непрерывности бизнеса.

Примечание. Система менеджмента включает в себя организационную структуру, политики, планирование деятельности, распределение ответственности, процедуры, процессы и ресурсы.

3.6. План непрерывности бизнеса (business continuity plan) ПНБ: набор документированных процедур и информации, которые разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента, и направлены на обеспечение возможности продолжения выполнения организацией критически важных для нее видов деятельности на установленном приемлемом уровне.

3.7. Программа непрерывности бизнеса (business continuity programme): программа действий, направленных на осуществление и поддержку менеджмента непрерывности бизнеса, поддерживаемая и обеспечиваемая высшим руководством и необходимыми ресурсами.

3.8. Анализ воздействия на бизнес (business impact analysis): процесс исследования функционирования бизнеса и последствий воздействия на него разрушающих факторов.

[ИСО 22300]

3.9. Компетентность (competence): способность применять знания и навыки для достижения

намеченных результатов.

3.10. Соответствие (conformity): выполнение требований.

[ИСО 22300]

3.11. Постоянное улучшение (continual improvement): непрерывный процесс совершенствования системы менеджмента с целью повышения ее общей эффективности в соответствии с политикой организации в области менеджмента.

[ИСО 22300]

3.12. Коррекция (correction): действие по устранению обнаруженного несоответствия.

[ИСО 22300]

3.13. Корректирующее действие (corrective action): действие по устранению причины обнаруженного несоответствия и предотвращения его повторного возникновения.

Примечание. В настоящем стандарте действия по минимизации и устранению других нежелательных последствий не подпадают под определение "корректирующее действие".

[ИСО 22300]

3.14. Документ (document): информация и ее носитель.

Примечание 1. В качестве носителя может выступать бумага, магнитные, электронные или оптические компьютерные диски, фотографии или их сочетание.

Примечание 2. Набор документов, например, спецификации и отчеты, часто называют "документацией".

3.15. Документированная информация (documented information): информация, которую организация должна контролировать и хранить.

Примечание 1. Документированная информация может иметь любой формат и любой носитель.

Примечание 2. Документированная информация может относиться к:

- системе менеджмента, включая соответствующие процессы;

- информации, необходимой для работы организации (документация);

- подтверждению достигнутых результатов (отчеты).

3.16. Результативность (effectiveness): степень реализации запланированной деятельности и достижения запланированных результатов.

[ИСО 22300]

3.17. Событие (event): возникновение или изменение специфического набора условий.

Примечание 1. Событие может быть единичным или кратным и может иметь несколько

причин.

Примечание 2. Событие может быть определенным или неопределенным.

Примечание 3. Событие может быть названо терминами "инцидент", "опасное событие" или "несчастный случай".

Примечание 4. Событие без последствий (см. Руководство ИСО 73, 3.6.1.3) может также быть названо терминами "угроза возникновения опасного события", "угроза инцидента", "угроза поражения" или "угроза возникновения аварийной ситуации".

[Руководство ИСО 73]

3.18. Учение (exercise): запланированная репетиция возможного инцидента, разработанная для оценки способности организации справляться с инцидентом, совершенствования ответных мер организации и повышения компетентности вовлеченных сторон.

Примечание 1. Учения могут быть использованы для валидации политики, планов, процедур, подготовки, оснащения и соглашений между организациями; обучения персонала функциям и обязанностям; улучшения координации действий и обмена информацией; повышения производительности и идентификации возможностей улучшения.

Примечание 2. Проверка - это особый тип учения, который направлен на выявление пригодности/непригодности элемента в пределах цели или задач планируемого учения.

[ИСО 22300]

3.19. Инцидент (incident): ситуация, которая может произойти и привести к нарушению деятельности организации, разрушениям, потерям, чрезвычайной ситуации или кризису в бизнесе.

[ИСО 22300]

3.20. Инфраструктура (infrastructure): система средств, оборудования и услуг, необходимая для функционирования организации.

3.21. Заинтересованная сторона, причастная сторона (interested party, stakeholder): лицо или организация, которые могут влиять на решения или деятельность, а также быть затронуты или ощущать себя затронутыми ими.

Примечание. Это может быть человек или группа, которые заинтересованы в определенном решении или виде деятельности организации.

3.22. Внутренний аудит (internal audit): аудит, выполняемый самой организацией или от ее имени для анализа менеджмента и других внутренних целей, который может служить основанием для декларации о соответствии.

Примечание. Во многих случаях, особенно на малых предприятиях, независимость при аудите обеспечивают отсутствием ответственности за деятельность, подвергаемую аудиту.

3.23. Активация плана (invocation): объявление о том, что план обеспечения непрерывности бизнеса организации должен быть введен в действие для продолжения предоставления ключевых услуг или продукции.

3.24. Система менеджмента (management system): система для разработки политики, целей и достижения этих целей.

Примечание 1. Система менеджмента может иметь отношение к единственному или нескольким направлениям деятельности.

Примечание 2. Элементами системы являются структура организации, функции и обязанности персонала, планирование, процедуры и т.д.

Примечание 3. Областью применения системы менеджмента может быть вся организация, установленные и идентифицированные функции организации, установленные и идентифицированные части организации или одна или несколько функций в группе организаций.

3.25. Максимально приемлемый простой (maximum acceptable outage, MAO) МПП: время, по истечении которого неблагоприятные последствия, возникшие в результате необеспечения поставок продукции/услуг или невыполнения деятельности, становятся неприемлемыми.

Примечание. См. также максимально приемлемый период нарушения.

3.26. Максимально приемлемый период нарушения (maximum tolerable period of disruption, MTPD) МППН: время, по истечении которого неблагоприятные последствия, возникшие в результате необеспечения поставок продукции/услуг или невыполнения деятельности, становятся неприемлемыми.

Примечание. См. также максимально приемлемый простой.

3.27. Измерение (measurement): определение значения величины.

3.28. Минимальная цель непрерывности бизнеса (minimum business continuity objective, MBCO) МЦНБ: минимальный уровень услуг и/или поставок продукции, приемлемый для достижения деловых целей организации во время нарушения ее деятельности.

3.29. Мониторинг (monitoring): определение состояния системы, процесса или деятельности.

Примечание. Для определения состояния может возникнуть необходимость проведения проверки, наблюдения или критического отслеживания.

3.30. Соглашение о взаимопомощи (mutual aid agreement): заранее подготовленное обязательство между двумя или более юридическими лицами об оказании помощи друг другу.

[ИСО 22300]

3.31. Несоответствие (nonconformity): невыполнение требования.

[ИСО 22300]

3.32. Цель (objective): результат, который должен быть достигнут.

Примечание 1. Цель может быть стратегической, тактической или операционной.

Примечание 2. Цели могут относиться к различным областям (таким как финансы, здоровье и безопасность, экология) и уровням (например, стратегическому, организации, проекта, продукции и процесса).

Примечание 3. Цель может быть выражена другими способами, например, в виде ожидаемого результата, замысла или критерия, или при помощи других аналогичных понятий (например, выполнения задачи).

Примечание 4. В области систем менеджмента социальной безопасности цели социальной безопасности организация устанавливает в соответствии с политикой социальной безопасности для достижения установленных результатов.

3.33. Организация (organization): группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений.

Примечание 1. Понятие организации охватывает компании, корпорации, фирмы, предприятия, учреждения, благотворительные организации, предприятия розничной торговли, ассоциации, а также их подразделения или комбинации из них.

Примечание 2. Организация может иметь несколько структурных единиц, при этом отдельная структурная единица может быть рассмотрена как организация.

3.34. Аутсорсинг (outsource (verb)): передача организацией определенных бизнес-процессов или производственных функций для выполнения другой организацией.

Примечание. Сторонняя организация находится вне области применения системы менеджмента, хотя произведенная на стороне функция, продукция или процесс находятся в пределах области применения системы менеджмента организации.

3.35. Выполнение (performance): получение измеримого результата.

Примечание 1. Выполнение может относиться как к количественным, так и к качественным результатам.

Примечание 2. Выполнение может относиться к управлению действиями, процессами, продукцией (включая услуги), системами или организациями.

3.36. Оценка выполнения (performance evaluation): процесс определения измеримых результатов.

3.37. Персонал (personnel): люди, работающие в организации и находящиеся под ее управлением.

Примечание. Понятие персонала включает, но не ограничено, постоянный персонал, частично занятый персонал и персонал вспомогательных организаций.

3.38. Политика (policy): намерения и направления деятельности организации, официально сформулированные высшим руководством.

3.39. Процедура (procedure): совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы.

3.40. Процесс (process): набор действий, направленных на достижение результата.

3.41. Продукция и услуги (products and services): результаты деятельности организации, которые она поставляет своим потребителям, получателям и причастным сторонам, например, промышленные товары, автострахование или медицинское обслуживание.

3.42. Приоритетные виды деятельности (prioritized activities): виды деятельности, которым должно быть отдано предпочтение после инцидента в целях смягчения его последствий.

Примечание. Для описания деятельности в пределах этой группы обычно используют следующие термины: критическая, важная, жизненно важная, срочная и ключевая.

[ИСО 22300]

3.43. Запись (record): документ, содержащий достигнутые результаты или свидетельства осуществленной деятельности.

3.44. Целевая точка восстановления данных (recovery point objective; RPO) ЦТВД: состояние, до которого необходимо восстановить данные, используемые в определенной деятельности, для обеспечения возобновления этой деятельности.

Примечание. Иногда употребляют термин "максимальная потеря данных".

3.45. Целевое время восстановления (recovery time objective, RTO) ЦВВ: период времени, установленный для возобновления поставок продукции или услуг, возобновления деятельности или восполнения ресурсов после инцидента.

Примечание. Для продукции, услуг и деятельности целевое время восстановления должно быть меньше времени, в течение которого неблагоприятные воздействия, возникшие в результате необеспечения поставок продукции/услуг или невыполнения деятельности, станут неприемлемыми.

3.46. Требование (requirement): установленные потребность или ожидание, подразумеваемое или обязательное.

Примечание 1. "Подразумеваемое" означает, что это требование является общепринятым или обычным для организации и заинтересованных сторон.

Примечание 2. Установленное требование - это требование, установленное в документации.

3.47. Ресурсы (resources): все активы, персонал, навыки, технологии (включая технологические процессы и оборудование), производственные площади, запасы и информация (на электронном или бумажном носителе), которые должны быть, при необходимости, доступны для использования организацией в текущей деятельности и для достижения поставленных целей.

3.48. Риск (risk): следствие влияния неопределенности на достижение поставленных целей <1>.

Примечание 1. Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (положительного и/или отрицательного).

Примечание 2. Цели могут быть различными по содержанию (в области экономики, здоровья, экологии и т.п.) и назначению (стратегические, общеорганизационные, относящиеся к разработке проекта, конкретной продукции и процессу).

Примечание 3. Риск часто характеризуют с помощью возможных событий (Руководство ИСО 73, 3.5.1.3) и последствий (Руководство ИСО 73, 3.6.1.3) или их сочетания.

Примечание 4. Риск часто выражают в виде сочетания последствий события (включая изменения в обстоятельствах) и вероятности их возникновения (Руководство ИСО 73, 3.6.1.1).

Примечание 5. Неопределенность - это состояние дефицита информации о событии, его последствиях или вероятности возникновения.

Примечание 6. Организация устанавливает цели непрерывности бизнеса в соответствии с политикой непрерывности бизнеса.

<1> В соответствии с ФЗ "О техническом регулировании" от 27.12.2002 N 184-ФЗ "риск - это вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда".

[Руководство ИСО 73]

3.49. Аппетит риска, предпочтительный риск (risk appetite): общая величина риска, который организация готова принять, перенести или действию которого готова подвергнуться в любой момент времени, и тип риска, предпочтительный для организации.

3.50. Оценка риска (risk assessment): процесс, охватывающий идентификацию риска, анализ риска и сравнительную оценку риска.

3.51. Менеджмент риска (risk management): скоординированные действия по руководству и управлению организацией в области риска.

3.52. Тестирование (testing): процедура оценки; способ определения наличия, качества или достоверности чего-либо.

Примечание 1. Тестирование иногда называют "испытанием".

Примечание 2. Тестирование часто применяют в отношении планов поддержки.

[ИСО 22300]

3.53. Высшее руководство (top management): лицо или группа работников, осуществляющих направление деятельности и управление организацией на высшем уровне.

Примечание 1. Высшее руководство может делегировать полномочия и распределять ресурсы в пределах организации.

Примечание 2. Если область применения системы менеджмента охватывает только часть организации, то высшим руководством являются ответственные лица, осуществляющие управление и контроль в этой части организации.

3.54. Верификация (verification): подтверждение посредством предоставления доказательств, что указанные требования были выполнены.

3.55. Производственная среда, рабочая среда (work environment): совокупность условий, в которых выполняют работу.

Примечание. Условия включают физические, социальные, психологические и

экологические факторы (такие как температура, системы поощрения, эргономика и состав атмосферы).

[ИСО 22300]

4. Условия организации

4.1. Понимание организации и ее условий

Организация должна определить внешние и внутренние факторы, влияющие на выполнение организацией поставленных целей и достижение результатов ее СМНБ.

Эти факторы необходимо учитывать при установлении, внедрении и поддержании СМНБ организации.

Организация должна идентифицировать и документировать следующее:

a) виды деятельности, функции, услуги, продукцию, сотрудничество, цепочки поставок, взаимодействия с заинтересованными сторонами, потенциально уязвимые по отношению к разрушительному инциденту;

b) взаимосвязь политики в области непрерывности бизнеса с целями и другими политиками организации, включая стратегию управления совокупным риском;

c) аппетит риска организации.

При установлении условий организация должна:

1) ясно сформулировать свои цели, включая цели, связанные с непрерывностью бизнеса;

2) определить внешние и внутренние факторы, которые создают неопределенность, вызывающую риск;

3) установить критерии риска с учетом аппетита риска;

4) определить цели в области СМНБ.

4.2. Понимание потребностей и ожиданий заинтересованных сторон

4.2.1. Общие положения

Устанавливая СМНБ, организация должна определить:

a) заинтересованные стороны, которые важны для СМНБ;

b) требования этих заинтересованных сторон (т.е. их потребности и ожидания, установленные, подразумеваемые или обязательные).

4.2.2. Законодательные и нормативные требования

Организация должна установить, осуществить и поддерживать процедуру(ы), позволяющие идентифицировать, иметь доступ, оценивать применимые законодательные и нормативные требования, относящиеся к непрерывности ее деятельности, поставок продукции и услуг, а также затрагивающие интересы важных заинтересованных сторон.

Организация должна гарантировать, что применимые юридические, нормативные и другие требования приняты во внимание при установлении, внедрении и поддержании ее СМНБ.

Организация должна зарегистрировать эту информацию и сохранять ее актуальной. Новые требования или изменения правовых, нормативных и других требований должны быть доведены до сведения соответствующих работников и других заинтересованных сторон.

4.3. Определение области применения СМНБ

4.3.1. Общие положения

Для установления области применения СМНБ организация должна определить ее границы и применимость.

При определении области применения организация должна рассмотреть:

- внешние и внутренние факторы, упомянутые в 4.1;

- требования, упомянутые в 4.2.

Должна быть доступна документированная информация по области применения СМНБ.

4.3.2. Область применения СМНБ

Организация должна:

a) установить части организации, включенные в СМНБ;

b) установить требования СМНБ с учетом предназначения организации, ее целей, внутренних и внешних обязательств (включая связанные с заинтересованными сторонами), а также юридических и нормативных обязанностей;

c) идентифицировать продукцию и услуги и все связанные с ними действия в рамках СМНБ;

d) принять во внимание потребности, интересы и ожидания заинтересованных сторон, таких как клиенты, инвесторы, акционеры, участники цепочки поставок, а также ожидания и интересы общественности и/или сообщества;

e) определить область применения СМНБ в соответствии с размером, характером и структурой организации.

При определении области применения организация должна документировать и обосновать все исключения; такие исключения не должны затрагивать способность и обязанность организации обеспечивать непрерывность бизнеса и выполнение операций в соответствии с требованиями СМНБ, определенными с помощью анализа воздействия на бизнес или оценки риска, и применимых юридических и нормативных требований.

4.4. Система менеджмента непрерывности бизнеса

Организация должна установить, внедрить, поддерживать и постоянно улучшать СМНБ, включая необходимые процессы и их взаимодействия, в соответствии с требованиями настоящего стандарта.

5. Лидерство

5.1. Лидерство и заинтересованность

Высшее руководство и руководители на разных уровнях организации должны продемонстрировать свое лидерство по отношению к СМНБ.

Пример - Лидерство и заинтересованность могут быть продемонстрированы с помощью мотивирования людей содействовать результативности СМНБ и предоставления им необходимых полномочий.

5.2. Заинтересованность руководства

Высшее руководство должно продемонстрировать свое лидерство и заинтересованность по отношению к СМНБ посредством:

- установления политики и целей системы менеджмента непрерывности бизнеса и обеспечения их совместимости со стратегическим направлением организации;

- обеспечения интеграции требований системы менеджмента непрерывности бизнеса в бизнес-процессы организации;

- обеспечения доступности ресурсов, необходимых для системы менеджмента непрерывности бизнеса;

- объяснения важности наличия результативной системы менеджмента непрерывности бизнеса и соответствия требованиям СМНБ;

- обеспечения достижения СМНБ ожидаемого результата(ов);

- направления и поддержки людей, способствующих результативности СМНБ;

- содействия непрерывному совершенствованию;

- поддержки других важных руководителей для демонстрации их лидерства и заинтересованности в областях их ответственности.

Примечание 1. Ссылки на "бизнес" в настоящем стандарте следует широко интерпретировать, так как они обозначают виды деятельности, которые являются ключевыми для существования организации.

Высшее руководство должно представить свидетельства своей заинтересованности в создании, внедрении, эксплуатации, мониторинге, анализе, поддержке и совершенствовании СМНБ посредством:

- установления политики в области непрерывности бизнеса;

- обеспечения установления целей и планов СМНБ;

- установления функций, ответственности и полномочий для управления непрерывностью бизнеса;

- назначение одного или большего количества людей с соответствующим авторитетом и компетентностью, ответственных за внедрение и поддержку СМНБ.

Примечание 2. Эти люди могут иметь и другие обязанности в организации.

Высшее руководство должно обеспечить распределение обязанностей и полномочий для выполнения важных функций и осведомленность о них в организации посредством:

- определения критериев принятия риска и допустимых уровней риска;

- активного участия в учениях и тестировании;

- обеспечения проведения внутренних аудитов СМНБ;

- проведения анализа СМНБ;

- демонстрации заинтересованности в постоянном улучшении.

5.3. Политика

Высшее руководство должно установить политику непрерывности бизнеса, которая:

a) соответствует целям организации;

b) обеспечивает основу для установления целей непрерывности бизнеса;

c) включает обязательства по выполнению применимых требований;

d) включает обязательства по постоянному улучшению СМНБ.

Политика СМНБ должна быть:

- доступна в форме документированной информации;

- доведена до сведения персонала организации;

- при необходимости, доведена до сведения заинтересованных сторон;

- актуализирована через установленные промежутки времени и при значительных изменениях в организации.

Организация должна сохранять документированную политику в области непрерывности бизнеса.

5.4. Функции, обязанности и полномочия в организации

Высшее руководство должно обеспечить распределение ответственности и полномочий для выполнения важных функций и довести их до сведения персонала организации.

Высшее руководство должно распределить ответственность и полномочия для:

a) обеспечения соответствия СМНБ требованиям настоящего стандарта;

b) создания отчетов о работе СМНБ для высшего руководства.

6. Планирование

6.1. Анализ риска и благоприятных возможностей

При планировании СМНБ организация должна рассмотреть вопросы, упомянутые в 4.1 и

4.2, и определить риски и благоприятные возможности для:

- обеспечения уверенности в том, что СМНБ может достигнуть ожидаемых результатов;

- предотвращения или уменьшения нежелательных последствий;

- обеспечения постоянного улучшения.

Организация должна запланировать:

a) действия по анализу риска и благоприятных возможностей,

b) действия по

1) их объединению и внедрению в процессы СМНБ (см. 8.1),

2) оценке их результативности (см. 9.1).

6.2. Цели в области непрерывности бизнеса и планы их достижения

Высшее руководство должно обеспечить установление целей в области непрерывности бизнеса и информирование о них на соответствующих уровнях организации.

Цели непрерывности бизнеса должны:

a) быть совместимы с политикой непрерывности бизнеса;

b) учитывать минимальный уровень продукции и услуг, который является приемлемым для достижения целей организации;

c) быть измеримы;

d) соответствовать установленным требованиям;

e) контролироваться и обновляться по необходимости.

Организация должна сохранять документированные цели в области непрерывности бизнеса.

Для достижения целей в области непрерывности бизнеса, организация должна:

- назначить ответственных;

- определить необходимые действия;

- определить необходимые ресурсы;

- назначить сроки выполнения;

- определить метод оценки результатов.

7. Поддержка

7.1. Ресурсы

Организация должна определить и выделить ресурсы, необходимые для создания, внедрения, обслуживания и постоянного улучшения СМНБ.

7.2. Компетентность

Организация должна:

a) определить необходимую компетентность сотрудников, выполняющих работу, которая влияет на функционирование СМНБ;

b) обеспечить компетентность людей посредством обучения, проведения учений и обмена опытом;

c) оценивать результативность предпринятых мер;

d) сохранять документы, подтверждающие компетентность.

Примечание. Применимые меры могут включать, например: предоставление обучения, наставничество или перевод сотрудников по службе; наем или заключение контракта с компетентными людьми.

7.3. Осведомленность

Персонал, осуществляющий работу под контролем организации, должен знать:

a) политику в области непрерывности бизнеса;

b) свой вклад в результативность СМНБ, включая выгоды от постоянного улучшения менеджмента непрерывности бизнеса;

c) последствия, которые могут возникнуть в случае несоответствия требованиям СМНБ;

d) свои функции в случае разрушительных инцидентов.

7.4. Обмен информацией

Организация должна определить потребность во внутреннем и внешнем обмене информацией, относящемся к СМНБ, включая:

a) вопросы для обмена информацией;

b) ситуации, в которых производится обмен информацией;

c) причастные стороны, с которыми производится обмен информацией.

Организация должна установить, внедрить и поддерживать в рабочем состоянии процедуру(ы):

- внутреннего обмена информацией между заинтересованными сторонами и сотрудниками организации;

- внешнего обмена информацией с клиентами, партнерскими организациями, местным сообществом и другими заинтересованными сторонами, включая СМИ;

- приема, документирования и реагирования на сообщения заинтересованных сторон;

- использования национальной и региональной систем предупреждения об угрозах (или аналогичных систем), при необходимости;

- обеспечения доступности средств обмена информацией в условиях разрушительного инцидента;

- связи с властями и обеспечения функциональной совместимости с другими организациями, участвующими в ответных мерах на инцидент, и их персоналом, при необходимости;

- тестирования и обеспечения работы резервных средств связи в случае отказа основных средств связи.

Примечание. Дальнейшие требования для обмена информацией в условиях инцидента установлены в 8.4.3.

7.5. Документированная информация

7.5.1. Общие положения

Документация СМНБ организации должна включать в себя:

- документацию в соответствии с требованиями настоящего стандарта;

- документацию, которую организация определила, как необходимую для оценки результативности СМНБ.

Примечание. Степень документирования информации СМНБ может отличаться в разных организациях и зависит от:

- размера организации, видов ее деятельности, процессов, продукции и услуг;

- сложности процессов и их взаимодействий;

- компетентности сотрудников.

7.5.2. Создание и обновление

При создании и обновлении документации организация должна обеспечить:

a) идентификацию и описание документов (например, наименование, дата, автор или номер ссылки);

b) формат (например, язык, версию программного обеспечения, графику) и носитель информации (например, бумага, электронный формат), а также способ ее проверки и подтверждения пригодности и достаточности.

7.5.3. Управление документацией

Документация, требуемая СМНБ и настоящим стандартом, должна быть управляемой для обеспечения:

a) доступности и пригодности для использования, при необходимости;

b) защищенности (например, от потери конфиденциальности, неправильного использования или потери целостности).

Для управления документацией организация должна определить следующие действия с документацией:

- распределение и доступ;

- обеспечение сохранности;

- управление изменениями (например, контроль версий программного обеспечения);

- хранение и распоряжение;

- поиск и использование;

- обеспечение четкости текста (т.е. обеспечение возможности разборчивости текста при чтении);

- предотвращение непреднамеренного использования устаревшей документации.

Документация внешнего происхождения, определенная организацией как необходимая для планирования и работы СМНБ, должна быть идентифицированной и управляемой.

При установлении управления документацией организация должна обеспечить для нее подходящую защиту (например, защиту от компрометации, несанкционированного изменения или удаления).

Примечание. Доступ подразумевает принятие решений о разрешении на просмотр или разрешение на просмотр и изменение документации и т.д.

8. Деятельность

8.1. Планирование и контроль

Организация должна планировать, внедрять и контролировать процессы, необходимые в соответствии с требованиями СМНБ, и выполнять действия, определенные в 6.1, в том числе:

a) установить необходимые критерии для процессов;

b) осуществлять контроль над процессами в соответствии с критериями;

c) хранить документацию, подтверждающую, что процессы выполнены в соответствии с запланированными действиями.

Организация должна контролировать изменение запланированных действий и анализировать последствия непреднамеренных изменений, принимая меры по смягчению неблагоприятных воздействий.

Организация должна обеспечить контроль процессов аутсорсинга.

8.2. Анализ воздействия на бизнес и оценка риска

8.2.1. Общие положения

Организация должна установить, внедрить и поддерживать в рабочем состоянии формальный документированный процесс анализа воздействий на бизнес и оценки риска, в котором должны быть:

a) установлена область применения оценки риска, определены критерии и способы оценки возможных воздействий инцидента;

b) учтены юридические и другие требования, которые должна соблюдать организация;

c) предусмотрен систематический анализ, установлены приоритетность обработки риска и необходимые для этого затраты;

d) определены выходные данные анализа воздействия на бизнес и оценки риска;

e) установлены требования к актуализации и конфиденциальности этой информации.

Примечание. Существуют различные методологии анализа воздействия на бизнес и оценки риска.

8.2.2. Анализ воздействия на бизнес

Организация должна установить, внедрить и поддерживать в рабочем состоянии формальный и документированный процесс определения приоритетов, целей и задач непрерывности бизнеса. Этот процесс должен включать оценку последствий нарушения видов деятельности, которые поддерживают поставку продукции и услуг.

Анализ воздействия на бизнес должен включать:

a) идентификацию видов деятельности, которые поддерживают поставку продукции и услуг;

b) оценку последствий невыполнения этих видов деятельности;

c) установление приоритетных сроков возобновления деятельности на установленном минимальном приемлемом уровне с учетом времени, в течение которого неблагоприятные воздействия, возникшие в результате необеспечения поставок продукции/услуг или невыполнения деятельности, приводят к неприемлемым результатам;

d) идентификацию зависимостей и ресурсов для поддержания этих видов деятельности, включая поставщиков, партнеров по аутсорсингу и других важных заинтересованных сторон.

8.2.3. Оценка риска

Организация должна установить, внедрить и поддерживать в рабочем состоянии формальный документированный процесс оценки риска для систематической идентификации, анализа и оценки риска разрушительных инцидентов для организации.

Примечание. Этот процесс может быть разработан в соответствии с ИСО 31000.

Организация должна:

a) идентифицировать риск нарушений в приоритетных видах деятельности организации, а также процессах, системах, информации, человеческих активах, аутсорсинге и ресурсах, которые их поддерживают;

b) систематически анализировать риск;

c) оценивать необходимость обработки;

d) определить методы обработки, соответствующие целям в области непрерывности бизнеса и аппетиту риска организации.

Примечание. Организация должна быть осведомлена, что определенные финансовые или установленные государством обязательства требуют предоставления отчета о таких видах риска с разной степенью детализации. Кроме того, некоторые потребности общества также могут служить основанием для предоставления отчета с соответствующей степенью детализации.

8.3. Стратегия непрерывности бизнеса

8.3.1. Определение и выбор

Определение и выбор стратегии должны быть основаны на результатах анализа воздействия на бизнес и оценки риска.

Организация должна определить подходящую стратегию непрерывности бизнеса для:

a) защиты приоритетных видов деятельности;

b) стабилизации, продолжения, возобновления и восстановления приоритетных видов деятельности и их обеспечения ресурсами;

c) смягчения последствий, разработки ответных мер и управления ими.

Определение стратегии должно включать в себя установление приоритетных сроков возобновления действий. Организация должна провести оценку способности к обеспечению непрерывности бизнеса своих поставщиков.

8.3.2. Установление требований к ресурсам

Организация должна определить требования к ресурсам для выполнения выбранных стратегий. Рассматриваемые ресурсы должны включать в себя, но не ограничиваться, следующими:

a) персонал;

b) информация и данные;

c) здания, рабочая среда и связанные с ними коммуникации;

d) оборудование и расходные материалы;

e) системы информационно-коммуникационных технологий (ИКТ);

f) транспорт;

g) финансы;

h) партнеры и поставщики.

8.3.3. Защита и снижение риска

Для идентифицированных рисков, требующих обработки, организация должна разработать меры, обеспечивающие:

a) снижение вероятности разрушений (нарушений);

b) сокращение продолжительности разрушений (нарушений);

c) снижение последствий разрушений (нарушений) для ключевой продукции и услуг организации.

Организация должна выбрать и провести необходимую обработку риска в соответствии с аппетитом риска.

8.4. Установление и внедрение процедур непрерывности бизнеса

8.4.1. Общие положения

Организация должна установить, внедрить и поддерживать в рабочем состоянии процедуры управления и продолжения своей деятельности в условиях действия инцидента на основе целей восстановления, идентифицированных в ходе анализа воздействия на бизнес.

Организация должна документировать процедуры (включая необходимые ответные меры) для обеспечения непрерывности деятельности и управления в условиях инцидента.

Процедуры должны:

a) устанавливать соответствующий порядок внутреннего и внешнего обмена информацией;

b) быть конкретными в отношении неотложных действий, которые должны быть выполнены в условиях разрушения (нарушения) деятельности;

c) быть гибкими для реагирования на непредвиденные угрозы и меняющиеся внутренние и внешние условия;

d) быть сфокусированы на последствиях событий, которые могут нарушить работу;

e) быть разработаны на основе установленных предположений и анализа взаимозависимостей;

f) результативно минимизировать последствия путем осуществления стратегий смягчения последствий инцидента.

8.4.2. Структура ответных мер на инцидент

Организация должна установить, документировать и внедрить процедуры и структуру управления действиями при возникновении разрушительного инцидента с использованием персонала, обладающего необходимой ответственностью, полномочиями и компетентностью.

Структура ответных мер должна

a) определять пороги воздействия, за пределами которых инициируют выполнение ответных мер;

b) оценивать характер и степень разрушительного инцидента и его возможных последствий;

c) приводить в действие соответствующие ответные меры, предусмотренные СМНБ;

d) иметь в наличии процессы и процедуры активации, функционирования, координации ответных мер и информирования о них;

e) иметь в наличии ресурсы для поддержки процессов и процедур управления в условиях разрушительного инцидента для минимизации его последствий;

f) активизировать связь с заинтересованными сторонами и властями, а также средствами массовой информации.

Организация должна определить, руководствуясь безопасностью жизни как важнейшим приоритетом, после консультаций с важными заинтересованными сторонами, необходимость сообщения внешним сторонам о наличии существенного риска и его последствиях для организации и документировать это сообщение. Если принято решение о направлении такого сообщения, то организация должна установить и внедрить процедуры обмена информацией с внешними сторонами, объявления тревоги и предупреждений, включая сообщения в СМИ.

8.4.3. Предупреждение и коммуникации

Организация должна установить, внедрить и поддерживать в рабочем состоянии процедуры для:

a) обнаружения инцидента;

b) мониторинга инцидента;

c) обмена информацией в пределах организации, а также получения, документирования и реагирования на сообщения заинтересованных сторон;

d) получения, документирования и реагирования на информацию национальной или региональной системы предупреждения о рисках;

e) обеспечения доступности средств связи в условиях разрушительного инцидента;

f) упрощенного обмена информацией с аварийно-спасательными службами;

g) записи жизненно важной информации об инциденте, предпринятых действиях и принятых решениях. Кроме того, должно быть рассмотрено следующее:

- оповещение заинтересованных сторон о возможном воздействии на них фактического или возможного инцидента;

- обеспечение взаимодействия нескольких организаций, реагирующих на инцидент, и их персонала;

- работа средств связи.

Процедуры обмена информацией и предупреждения необходимо регулярно проверять.

8.4.4. Планы непрерывности бизнеса

Организация должна установить документированные процедуры реагирования на разрушительный инцидент, а также работы и восстановления деятельности в течение заранее определенного периода времени. Такие процедуры должны устанавливать требования к тем, кто будет их осуществлять.

Планы непрерывности бизнеса должны содержать:

a) определенные функции и ответственность сотрудников и команд, обладающих полномочиями в течение и после инцидента;

b) процесс инициирования ответных мер;

c) информацию о незамедлительных действиях по устранению последствий разрушительного инцидента, в которой уделено особое внимание:

1) благополучию людей,

2) стратегическим, тактическим и оперативным вариантам реагирования на разрушения (нарушения),

3) предотвращению дальнейшей потери или недоступности приоритетных видов деятельности;

d) способы поддержки связи с персоналом, их родственниками, ключевыми заинтересованными сторонами и аварийными службами и условия их применения;

e) способы продолжения или восстановления организацией приоритетных видов деятельности в рамках заранее установленного периода времени;

f) информацию по взаимодействию со СМИ после инцидента, в том числе:

1) стратегию обмена информацией,

2) предпочтительные виды связи со СМИ,

3) руководство или шаблон написания заявлений для СМИ,

4) информацию о представителях организации для связей со СМИ;

g) процесс сворачивания ответных мер после окончания инцидента.

Каждый план непрерывности бизнеса должен определять:

- назначение и область применения;

- цели;

- критерии и процедуры инициирования ответных мер;

- процедуры выполнения ответных мер;

- функции, ответственность и полномочия;

- требования и процедуры обмена информацией;

- внутренние и внешние взаимозависимости и взаимодействия;

- потребности в ресурсах;

- процессы управления информационным потоком и документирования.

8.4.5. Восстановление

Организация должна иметь документированные процедуры по восстановлению и возвращению к нормальному режиму работы после инцидента.

8.5. Учения и проверки

Организация должна проводить учения и проверки своих процедур непрерывности бизнеса для уверенности в том, что они соответствуют целям в области непрерывности бизнеса.

Организация должна проводить учения и тестирование для проверки того, что процедуры:

a) соответствуют области применения и целям СМНБ;

b) основаны на проработанных спланированных сценариях с четко определенными целями и задачами;

c) совместно обеспечивают валидацию мер непрерывности бизнеса с привлечением заинтересованных сторон;

d) обеспечивают риск нарушения деятельности на минимальном уровне;

e) предоставляют информацию для формирования отчетов по результатам учений с приведением данных рекомендаций и мер по постоянному улучшению СМНБ;

f) содействуют постоянному улучшению;

g) проверяются через запланированные интервалы времени и в случае существенных изменений в организации или среде, в которой она осуществляет деятельность.

9. Оценка выполнения

9.1. Мониторинг, измерение, анализ и оценка

9.1.1. Общие положения

Организация должна определить:

a) контролируемые с помощью мониторинга и измерений параметры и объекты;

b) методы мониторинга, измерения, анализа и оценки для обеспечения достоверных результатов;

c) сроки и периодичность проведения мониторинга и измерений;

d) сроки анализа и оценки результатов мониторинга и измерений.

Организация должна сохранить соответствующую документацию в качестве свидетельства результатов функционирования СМНБ.

Организация должна оценить СМНБ и ее результативность.

Дополнительно организация должна:

- принять меры по устранению неблагоприятных тенденций или результатов до возникновения несоответствия;

- сохранять соответствующую документацию в качестве свидетельства результатов СМНБ.

Процедуры мониторинга функционирования СМНБ должны предусматривать:

- установление показателей, соответствующих потребностям организации;

- мониторинг выполнения политики, целей и задач организации в области непрерывности бизнеса;

- мониторинг выполнения процессов, процедур и функций, которые защищают приоритетные виды деятельности;

- мониторинг соответствия требованиям настоящего стандарта и целям в области непрерывности бизнеса;

- мониторинг хронологии свидетельств несовершенства функционирования СМНБ;

- запись данных и результатов мониторинга и измерений для разработки последующих корректирующих действий.

Примечание. Несовершенство выполнения МНБ может включать в себя несоответствие, промахи, ложные тревоги и фактические инциденты.

9.1.2. Оценка процедур непрерывности бизнеса

a) Организация должна периодически проводить оценку процедур и благоприятных возможностей СМНБ для обеспечения их пригодности, адекватности и результативности;

b) Такая оценка может быть осуществлена посредством периодического анализа, учений, проверок, анализа отчетов об инцидентах и оценки функционирования СМНБ. Существенные изменения должны быть своевременно отражены в процедуре(ах);

c) Организация должна периодически оценивать соответствие действующим юридическим и нормативным требованиям, передовому опыту, а также собственной политике и целям в области непрерывности бизнеса;

d) Организация должна проводить оценку через запланированные интервалы времени и при наличии существенных изменений.

При возникновении разрушительного инцидента после инцидента организация должна провести анализ и записать результаты выполненных действий в соответствии с СМНБ.

9.2. Внутренний аудит

Организация должна проводить внутренний аудит через запланированные интервалы времени для предоставления информации о:

a) соответствии СМНБ

1) собственным требованиям организации;

2) требованиям настоящего стандарта;

b) результативности функционирования и поддержания в рабочем состоянии СМНБ.

Организация должна:

- запланировать, установить, внедрить и поддерживать в рабочем состоянии программу(ы) аудита, которая должна включать частоту проведения аудита, его методы, распределение ответственности, требования к планированию и отчетам. Программа(ы) аудита должна учитывать важность проверяемых процессов и результаты предыдущих аудитов;

- для каждого аудита определить критерии и область применения;

- назначить аудиторов и обеспечить объективность и беспристрастность процесса аудита;

- обеспечить информирование руководства о результатах аудита;

- сохранять записи как свидетельство выполнения программы аудита и результаты аудита.

Программа аудита, в том числе все графики работы, должна быть основана на результатах оценки риска для видов деятельности организации, а также результатах предыдущих аудитов. Процедуры аудита должны охватывать область применения, частоту проведения, методологию и компетентность, а также распределение ответственности и требования к проведению аудита и отчетам.

Руководство, ответственное за проверяемые области деятельности, должно обеспечить выполнение всех необходимых исправлений и корректирующих действий без излишней отсрочки для устранения обнаруженных несоответствий и их причин. Последующие действия должны включать верификацию предпринятых мер и отчет о результатах верификации.

9.3. Анализ со стороны руководства

Высшее руководство должно проводить анализ СМНБ организации через запланированные интервалы времени для обеспечения ее постоянной пригодности, адекватности и результативности. Анализ со стороны руководства должен включать рассмотрение:

a) состояния выполнения действий по результатам предыдущих анализов;

b) изменения внешних и внутренних факторов, влияющих на систему менеджмента непрерывности бизнеса;

c) информации о функционировании СМНБ, в том числе о

1) несоответствиях и корректирующих действиях;

2) результатах оценки мониторинга и измерений;

3) результатах аудита;

d) возможностей для постоянного улучшения.

Анализ со стороны руководства должен рассматривать функционирование организации, включая:

- действия, рекомендованные по результатам предыдущих анализов;

- необходимость изменений СМНБ, включая политику и цели;

- возможности для постоянного улучшения;

- результаты аудитов и анализов СМНБ, в том числе ключевых поставщиков и партнеров в соответствующих случаях;

- методы, продукцию или процедуры, которые могут быть использованы в организации для постоянного улучшения функционирования и результативности СМНБ;

- состояние корректирующих действий;

- результаты учений и тестирований;

- риски или проблемы, которые не были должным образом рассмотрены во время предыдущих оценок риска;

- все изменения, которые могут повлиять на СМНБ, как внутренние, так и внешние по отношению к области применения СМНБ;

- адекватность политики;

- рекомендации по постоянному улучшению;

- полученный опыт и действия, связанные с разрушительным инцидентом;

- современные надлежащую практику и рекомендации.

Результаты анализа со стороны руководства должны включать в себя решения, связанные с возможностями постоянного улучшения и необходимостью изменений в СМНБ, в том числе относящиеся к:

a) измененим в области применения СМНБ;

b) постоянному улучшению результативности СМНБ;

c) обновлению оценки риска, анализа воздействия на бизнес, планов непрерывности бизнеса и связанных с ними процедур;

d) изменению процедур, методов и средств управления для реагирования на внутренние и внешние события, которые могут оказать влияние на СМНБ, включая изменения:

1) требований к бизнесу и работе;

2) требований к снижению риска и безопасности;

3) условий работы и процессов;

4) юридических и нормативных требований;

5) договорных обязательств;

6) уровней риска и/или критериев принятия риска;

7) потребностей в ресурсах;

8) финансовых и бюджетных требований;

e) способам измерений результативности методов и средств управления.

Организация должна сохранять документацию в качестве свидетельств результатов анализа со стороны руководства.

Организация должна:

- сообщать результаты анализа со стороны руководства важным заинтересованным сторонам;

- выполнять необходимые действия в соответствии с этими результатами.

10. Постоянное улучшение

10.1. Несоответствие и корректирующие действия

При возникновении несоответствий организация должна:

a) идентифицировать несоответствия;

b) реагировать на несоответствия и, в зависимости от ситуации:

1) применять контроль и исправление несоответствия,

2) устранять последствия несоответствий;

c) оценивать необходимость действий по устранению причин несоответствия, для того, чтобы оно не повторялось и не происходило в другом месте, посредством:

1) анализа несоответствия,

2) определения причин возникновения несоответствий,

3) определения наличия возможности возникновения похожих несоответствий,

4) определения необходимости принятия корректирующих действий для предотвращения возникновения несоответствий в другом месте,

5) определения и осуществления необходимых корректирующих действий,

6) анализа эффективности принятых корректирующих мер,

7) внесения изменений в СМНБ при необходимости;

d) осуществить все необходимые действия;

e) проанализировать результативность принятых корректирующих действий;

f) при необходимости внести изменения в СМНБ.

Корректирующие действия должны соответствовать последствиям выявленных несоответствий.

Организация должна сохранять документацию о:

- характере несоответствий и всех предпринятых действиях,

- результатах корректирующих действий.

10.2. Постоянное улучшение

Организация должна постоянно улучшать пригодность, адекватность и результативность СМНБ.

Примечание. Организация может использовать процессы СМНБ, такие как лидерство, планирование и оценку функционирования в качестве основы для постоянного улучшения.

Приложение ДА
(справочное)

СВЕДЕНИЯ О СООТВЕТСТВИИ ССЫЛОЧНЫХ НАЦИОНАЛЬНЫХ СТАНДАРТОВ ВЕЛИКОБРИТАНИИ, УКАЗАННЫХ В БИБЛИОГРАФИИ НАСТОЯЩЕГО СТАНДАРТА, ССЫЛОЧНЫМ НАЦИОНАЛЬНЫМ СТАНДАРТАМ РОССИЙСКОЙ ФЕДЕРАЦИИ

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 9001:2008	IDT	ГОСТ ISO 9001-2011 Системы менеджмента качества. Требования
ИСО 14001:2004	IDT	ГОСТ Р ИСО 14001-2007 Системы экологического менеджмента. Требования и руководство по применению
ИСО 19011:2011	IDT	ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента
ИСО/МЭК 20000-1:2005	IDT	ГОСТ Р ИСО/МЭК 20000-1-2010 Информационная технология. Менеджмент услуг. Часть 1. Спецификация

ИСО 22300:2012	-	<*>
ISO/PAS 22399:2007	IDT	ГОСТ Р 53647.4-2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности
ИСО/МЭК 24762:2008	-	<*>
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
ИСО/МЭК 27031:2011	IDT	ГОСТ Р ИСО/МЭК 27031-2012 Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса
ИСО 31000:2009	IDT	ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство
ИСО/МЭК 31010:2009	IDT	ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска
Руководство ИСО 73:2009	IDT	ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения
BS 25999-1:2006	IDT	ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство
BS 25999-2:2007	IDT	ГОСТ Р 53647.2-2009 Менеджмент непрерывности бизнеса. Часть 2. Требования

<*> Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание. В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

IDT - идентичные стандарты.

БИБЛИОГРАФИЯ

[1] ISO 9001 Quality management systems - Requirements

[2] ISO 14001 Environmental management systems - Requirements with guidance for use

[3] ISO 19011 Guidelines for auditing management systems

[4] ISO/IEC 20000-1 Information Technology - Service Management

[5] ISO 22300 Societal security - Terminology

[6] ISO/PAS 22399 Societal security - Guideline for incident preparedness and operational continuity management

[7] ISO/IEC 24762 Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services

[8] ISO/IEC 27001 Information Security Management Systems

[9] ISO/IEC 27031 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

[10] ISO 31000 Risk Management - Principles and Guidelines

[11] ISO/IEC 31010 Risk management - Risk assessment techniques

[12] ISO Guide 73 Risk management - Vocabulary

[13] BS 25999-1 Business continuity management - Code of practice, British Standards Institution (BSI)

[14] BS 25999-2 Business continuity management - Specification, British Standards Institution (BSI)

[15] SI 24001 Security and continuity management systems - Requirements and guidance for use, Standards Institution of Israel

[16] NFPA 1600 Standard on disaster/emergency management and business continuity programs, National Fire Protection Association (USA)

[17] Business Continuity Plan Drafting Guideline, Ministry of Economy, Trade and Industry (Japan), 2005

[18] Business Continuity Guideline, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[19] ANSI/ASIS SPC.1, Organizational Resilience: Security, Preparedness, and Continuity Management Systems - Requirements with Guidance for Use

[20] SS 540:2008 Singapore Standard for Business Continuity Management

[21] ANSI/ASIS/BSI BCM.01, Business Continuity Management Systems: Requirements with Guidance for Use.