ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 28002— 2019

СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Устойчивость цепи поставок. Требования и руководство по применению

(ISO 28002:2011, IDT)

Издание официальное

Москва
Стандартинформ
2020

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Международный менеджмент, качество, сертификация» (АНО «ММКС») совместно с Обществом с ограниченной ответственностью «Палекс» (ООО «Палекс»), Ассоциацией по сертификации «Русский Регистр» на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 23 декабря 2019 г. № 1434-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 28002:2011 «Системы менеджмента безопасности для цепи поставок. Развитие устойчивости в цепи поставок. Требования и руководство по применению» (ISO 28002:2011 «Security management systems for the supply chain — Development of resilience in the supply chain — Requirements with guidance for use», IDT).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения его в соответствие с ГОСТ Р 1.5—2012 (пункт 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 статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

0.1 Общие положения

Организации по всему миру стремительно разрабатывают программы управления рисками и устойчивости для устранения неопределенности в достижении своих целей. Существует высокая потребность на стандарты и лучшие практики, так как организации ищут гарантии того, что их поставщики и участники расширенной цепи поставок запланировали и предприняли шаги для предотвращения и снижения угроз и опасностей, которым они подвергаются.

Чтобы обеспечить устойчивость в цепи поставок, организации должны участвовать во всеобъемлющем и систематическом процессе предупреждения, защиты, готовности, минимизации последствий, реагирования, непрерывности и восстановления.

Выживаемость организаций в цепи поставок во многом зависит от устойчивости их поставщиков и потребителей. В результате включение устойчивости и повышение устойчивости организации в цепи поставок должны быть ориентированы как внутри организации, так и извне на ее поставщиков и потребителей. Сохранение неуязвимости организации в цепи поставок в значительной степени зависит от устойчивости ее поставщиков и потребителей. Как результат интеграция менеджмента устойчивости в существующие системы и улучшение устойчивости организации в цепи поставок должны быть сконцентрированы не только на внутренней среде организации, но и на ее поставщиках и потребителях. Точная природа нарушения, вероятно, не будет полностью понятна вначале и может стать полностью понятной только с течением времени. В связи с этим при разработке планов и политик устойчивости необходимо уделять особое внимание адаптации и постоянной оценке новой информации, чтобы гарантировать, что предпринимаются те действия, которые необходимы. Значительные нарушения/сбои цепи поставок, как правило, привлекают средства массовой информации. Неспособность должным образом управлять отношениями со средствами массовой информации может негативно повлиять на способность организации реагировать для обеспечения устойчивости, что приведет к потере доверия заинтересованных сторон.

Эта потеря доверия может привести к потере потребителей, увеличению спроса на информацию со стороны правительства или финансовых организаций и ограничениям, налагаемым внешними организациями. Настоящий стандарт применим для организаций любых форм собственности (частных, некоммерческих, неправительственных и государственных). Это основа управления для планирования действий и принятия решений, необходимых для прогнозирования, предотвращения, если это возможно, подготовки и реагирования на разрушительный инцидент, чрезвычайную ситуацию, кризис или бедствие. При внедрении в существующую систему менеджмента это повышает способность организации управлять и переживать событие, а также предпринимать все необходимые действия, чтобы помочь обеспечить дальнейшую жизнеспособность организации. Независимо от организации ее руководство обязано перед заинтересованными сторонами обеспечивать планирование выживания организации. Основная часть стандарта содержит общие проверяемые критерии для установления, проверки, поддержания и улучшения политики устойчивости при ее интеграции в систему менеджмента для повышения эффективности предупреждения, готовности, минимизации последствий, реагирования, непрерывности и восстановления после разрушительных инцидентов.

Настоящий стандарт разработан в качестве неотъемлемой части ИСО 28000. Он также может быть интегрирован в другие системы менеджмента организации, которые следуют модели «Планируй — Делай — Проверяй — Действуй» (PDCA). Если выбрана независимая сертификация третьей стороной, сертификация будет применяться к общему стандарту системы менеджмента, в который интегрирован настоящий стандарт.

Интеграция адаптивного, преактивного и реактивного подходов к устойчивости может стать рычагом для использования перспектив, знаний и возможностей подразделений и отдельных лиц внутри организации. Из-за относительно низкой вероятности и все же потенциально высокого характера тяжести последствий многих природных, преднамеренных или непреднамеренных угроз и опасностей, с которыми может столкнуться организация, комплексный подход позволяет организации установить приоритеты, которые учитывают индивидуальные потребности в управлении рисками с учетом экономических условий.

0.2 Среда цепи поставок

Управление рисками в цепи поставок требует понимания не только среды организации, но также факторов глобальной среды всей цепи поставок. Каждый узловой пункт цепи поставок имеет набор рисков и процессы управления планированием, снабжением, изготовлением, доставкой и возвратами. Все эти процессы должны быть включены в политику устойчивости организации. Данное понимание позволит организации решить, к какому уровню или звену цепи поставок подключить программу устойчивости.

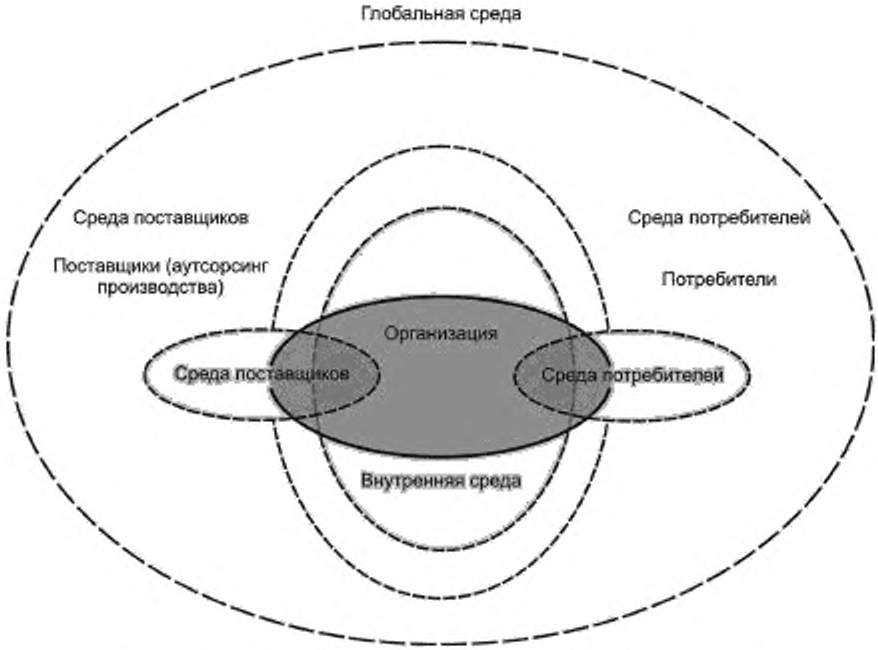

Рисунок 1 — Политика управления устойчивостью в цепи поставок
(Источник: Совет по цепи поставок 2007)

0.3 Процессный подход

Системный подход к управлению требует от организации анализировать требования самой организации и заинтересованных сторон и определять процессы, способствующие эффективности. Система менеджмента может обеспечить основу для постоянного улучшения и повышения вероятности усиления безопасности, готовности, реагирования, непрерывности и устойчивости. Процессный подход обеспечивает уверенность организации и ее потребителей в том, что она способна обеспечить безопасную и надежную среду, которая отвечает требованиям организации и заинтересованных сторон.

Настоящий стандарт применяет процессный подход для установления, реализации, функционирования, мониторинга, проверки, поддержания в рабочем состоянии и улучшения устойчивости организации к нарушениям/сбоям в цепи поставок. Чтобы эффективно работать, организация должна идентифицировать и управлять большим количеством действий. Любой вид деятельности, использующий ресурсы и управляемый для обеспечения возможности преобразования входов в выходы, может рассматриваться как процесс. Часто выходные данные одного процесса непосредственно формируют входные данные для следующего процесса.

Применение системы процессов в организации вместе с идентификацией и взаимодействием этих процессов и управление ими можно назвать «процессным подходом».

На рисунке 2 показан процессный подход к менеджменту устойчивости в цепи поставок, представленный в настоящем стандарте, который позволяет организации учитывать важность:

a) понимания рисков организации, требований по безопасности, готовности, реагированию, непрерывности и способности к восстановлению;

b) разработки политики и целей процесса управления рисками,

c) внедрения и управления системой процесса управления рисками в контексте целей организации;

d) мониторинга и анализа достигнутых результатов, эффективности реализации политики менеджмента устойчивости;

e) постоянного улучшения, основанного на измерении целей.

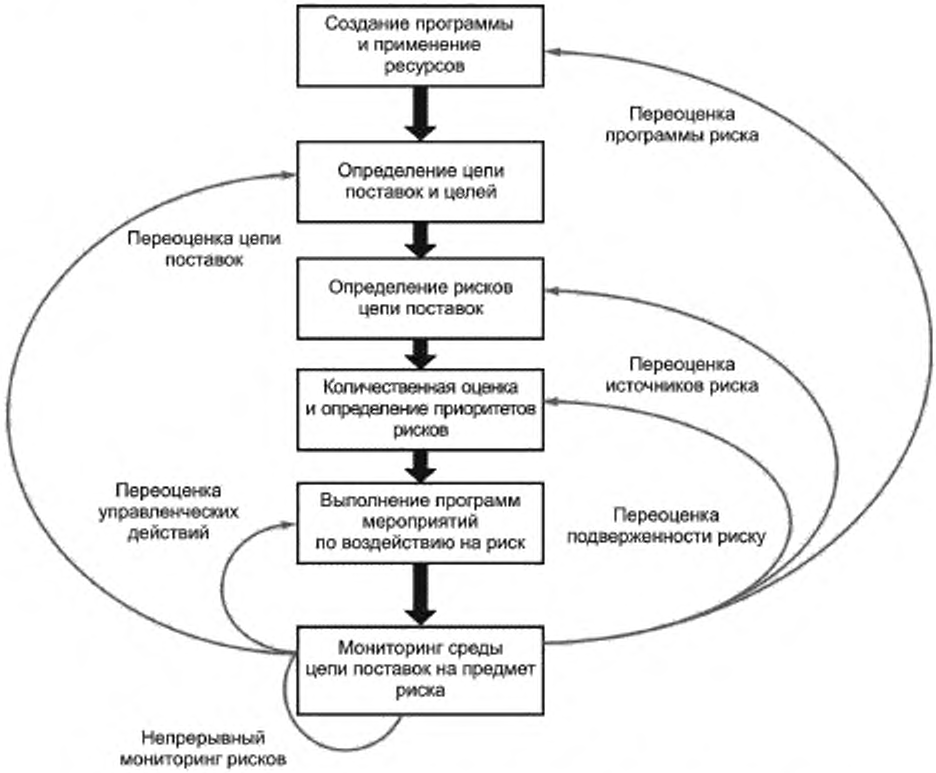

Рисунок 2 — Процессный подход в менеджменте устойчивости цепи поставок

0.3.1 Разработка программ устойчивости цепи поставок и выделение ресурсов

- Признание руководством рисков в цепи поставок приоритетными.
- Поддержка программ высшим руководством.
- Выделение необходимых ресурсов для выполнения программ.

0.3.2 Определение целей цепи поставок и целей устойчивости

- Определение области распространения цепи поставок и отображение цепи поставок.
- Определение цели управления рисками в цепи поставок организации.

0.3.3 Идентификация рисков цепи поставок.

- Всесторонний анализ цепи поставок для определения рисков
- Документирование идентифицированных рисков в максимально возможной степени.

0.3.4 Количественная оценка и определение приоритетных рисков.

- Количественная оценка каждого риска с точки зрения вероятности возникновения и потенциального воздействия.
- Использование количественной оценки риска для определения приоритетных рисков в соответствии с определенными целями.

0.3.5 Программы обработки рисков

- Разработка действий по управлению рисками в соответствии с приоритетом каждого риска.
- Определение ценности каждого действия с точки зрения уменьшения вероятности риска.
- Разработка и выполнение плана реализации указанных действий.

0.3.6 Мониторинг среды цепи поставок

- Непрерывный мониторинг среды цепи поставок на предмет возникновения риска или предвестников риска.
- При срабатывании пороговых значений выполнение соответствующих действий по управлению рисками для минимизации последствий.
- Документирование результатов после анализа действий по управлению рисками и улучшение программы обработки рисков.

0.4 Модель «Планируй — Делай — Проверяй — Действуй» (PDCA)

Настоящий стандарт предназначен для интеграции в любую систему менеджмента, которая основана на модели «Планируй — Делай — Проверяй — Действуй» (PDCA), которая, в свою очередь, будет направлять реализацию и выполнение процессов политики менеджмента устойчивости. На рисунке 3 показано, как система менеджмента может интегрировать в себя политику менеджмента устойчивости, которая фиксирует требования и ожидания заинтересованных сторон и посредством необходимых действий и процессов создает результаты управления рисками, которые соответствуют этим требованиям и ожиданиям.

На рисунке 3 также показана взаимосвязь процессов, представленных в разделе 4 настоящего стандарта.

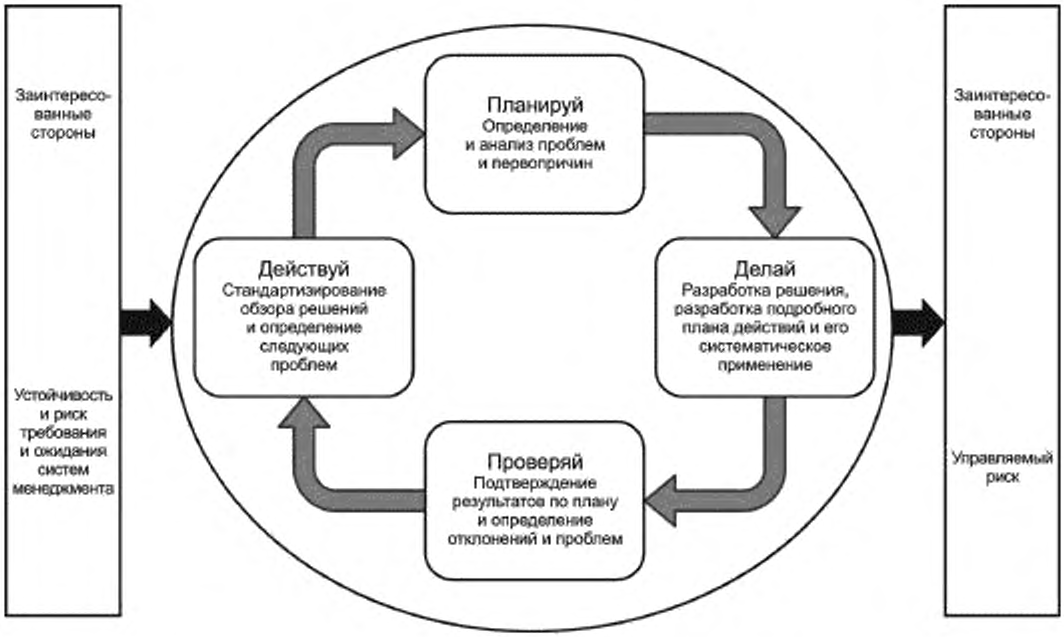

Рисунок 3 — Цикл «Планируй — Делай — Проверяй — Действуй»

Планируй Разработка системы менеджмента	Установление политики, целей, процессов и процедур системы менеджмента, относящихся к управлению рисками и повышению безопасности, готовности, смягчению, реагированию, непрерывности, восстановлению и предоставлению результатов в соответствии с общей политикой и целями организации
Делай Внедрение и использование системы менеджмента	Внедрение и функционирование политики системы менеджмента, элементов управления, процессов и процедур
Проверяй Мониторинг и анализ системы менеджмента	Оценка и измерение результатов деятельности, процессов в соответствии с политикой, целями и практическим опытом системы менеджмента и отчет о результатах анализа со стороны руководства
Действуй Поддерживание в рабочем состоянии системы менеджмента	Осуществление корректирующих и предупреждающих действий, основанных на результатах внутреннего аудита системы менеджмента и анализа со стороны руководства, для достижения постоянного улучшения системы менеджмента

Соответствие системы менеджмента, которая внедрила настоящий стандарт, можно проверить с помощью процесса аудита, который совместим и соответствует методологии ИСО 28000:2007, ИСО 14001:2004 и/или ИСО/МЭК 27001:2005 и модели PDCA.

Дополнительную информацию о критериях применения настоящего стандарта см. в приложении D.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК

Устойчивость цепи поставок. Требования и руководство по применению

Security management systems for the supply chain. Resilience of the supply chain. Requirements with guidance for use

Дата введения — 2020—07—01

1 Область применения

Настоящий стандарт устанавливает требования к политике управления устойчивостью цепи поставок, чтобы дать возможность организации разработать и реализовать политику, цели и программы с учетом:

- нормативно-законодательных требований, относящихся к организации;
- информации о значительных рисках, опасностях и угрозах, которые могут привести к негативным последствиям для организации, ее заинтересованных сторон и цепи поставок;
- защиты активов и процессов организации;
- управления разрушительными инцидентами.

Настоящий стандарт применяется к рискам, которые организация определяет, может контролировать, на которые может влиять или снижать, а также те, которые она не может предвидеть. Настоящий стандарт не устанавливает конкретных критериев выполнения.

Стандарт применяется в тех случаях, когда организация стремится:

a) установить, внедрить, поддерживать и улучшать политику управления устойчивостью для организации и ее цепи поставок;

b) убедиться в соответствии заявленной политики управления устойчивостью;

c) продемонстрировать, что система менеджмента содержит хорошо разработанную политику управления устойчивостью посредством:

1) самопровозглашения и самодекларирования;

2) получения подтверждения соответствия заинтересованными сторонами организации (например, потребителями);

3) подтверждения своего самопровозглашения стороной, внешней по отношению к организации;

4) прохождения сертификации/регистрации этой системы менеджмента внешней организацией.

Все требования стандарта предназначены для интеграции в любую систему менеджмента организации, основанную на модели PCDA. Настоящий стандарт содержит элементы, необходимые для интеграции (включая те, которые касаются технологии, оборудования, процессов и людей). Степень применения стандарта будет зависеть от таких факторов, как допустимый риск, политика организации, характер и масштабы ее деятельности, виды товаров и услуг, место, где и при каких условиях функционирует организация.

Настоящий стандарт предоставляет общие требования, которые в качестве основы применимы ко всем типам организаций (или их подразделениям), независимо от размера и функций в цепи поставок.

Настоящий стандарт предоставляет руководящие указания для организаций по разработке собственных конкретных критериев достижения результатов. Это позволяет организации адаптировать и

Издание официальное

осуществлять политику управления устойчивостью, соответствующую потребностям организации и интересам заинтересованных сторон.

Стандарт сфокусирован на устойчивости, способности организации адаптироваться в комплексной и изменчивой среде, а также защитить цепь поставок, критически важные активы и процессы. Применение настоящего стандарта позволяет организации с большей готовностью предотвращать, по возможности готовиться и реагировать на все виды преднамеренных, непреднамеренных и/или вызванных природой разрушительных событий, которые, если их не контролировать, могут перерасти в чрезвычайную ситуацию, кризис или бедствие. Настоящий стандарт охватывает все фазы управления инцидентами: до, во время и после разрушительного события.

Стандарт позволяет организации:

a) разработать политику предупреждения, защиты, готовности, минимизации последствий, реагирования, непрерывности и восстановления;

b) установить цели, процедуры и процессы для достижения обязательств, изложенных в политике;

c) обеспечить компетентность, осведомленность и обучение;

d) установить измеримые показатели оценки результатов и демонстрации успеха;

e) предпринимать действия, необходимые для улучшения результатов деятельности;

f) демонстрировать соответствие системы требованиям настоящего стандарта;

g) установить и применять процесс постоянного улучшения.

Приложение А содержит информативное руководство по планированию, внедрению, тестированию, поддержанию в рабочем состоянии и улучшению системы.

2 Нормативные ссылки

Для применения настоящего стандарта необходим следующий нормативный документ. Для датированных ссылок применяется только указанное издание. Для недатированных ссылок применяется последнее издание ссылочного документа (включая все изменения).

ISO 28000:2007, Specification for security management systems for the supply chain (Спецификация систем управления безопасностью цепи поставок)

3 Термины, определения и сокращения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **альтернативное рабочее место** (alternate worksite): Рабочее место, кроме основного, для использования, когда основное рабочее место недоступно.

3.2 **активы** (asset): Все, что имеет ценность для организации.

Примечание — Активы включают, но не ограничиваются ими, человеческие, физические, информационные, нематериальные и природные ресурсы.

3.3 **аудит** (audit): Систематический, независимый и документированный процесс получения свидетельств аудита и их объективного оценивания с целью установления степени соответствия согласованным критериям аудита.

Примечания

1 Внутренние аудиты, иногда называемые аудитами, проводимыми первой стороной, проводятся обычно самой организацией или от ее имени для анализа со стороны руководства и других внутренних целей и могут служить основанием для декларации о соответствии. Независимость может быть продемонстрирована отсутствием ответственности за деятельность, подвергаемую аудиту.

2 Внешние аудиты включают в себя аудиты, обычно называемые аудитами, проводимыми второй стороной или третьей стороной. Аудиты, проводимые второй стороной, выполняют стороны, заинтересованные в деятельности организации, например потребители или другие лица от их имени. Аудиты, проводимые третьей стороной, выполняют внешние независимые аудиторские организации, проводящие сертификацию или регистрацию на соответствие ИСО 28000, который является стандартом системы менеджмента безопасности цепи поставок.

3 Аудит, проводимый в одной проверяемой организации для двух и более систем менеджмента одновременно, называется комбинированным или комплексным аудитом.

4 Аудит, проводимый в одной проверяемой организации двумя и более проверяющими организациями одновременно, называется совместным аудитом.

3.4 **аудитор** (auditor): Лицо, обладающее личными качествами и компетенцией для проведения аудита.

3.5 **постоянное улучшение** (continual improvement): Повторяющаяся деятельность для улучшения способности выполнять требования.

Примечание — Процесс разработки целей и поиска возможностей для улучшения является непрерывным процессом с использованием результатов аудита и выводов аудита, анализа данных, анализа со стороны руководства или других средств и, как правило, приводит к корректирующим или предупреждающим действиям.

3.6 **соответствие** (conformity): Выполнение требований.

3.7 **последствие** (consequence): Результат события, влияющий на достижение целей.
[Руководство ИСО 73:2009, определение 3.6.1.3]

Примечания

1 Событие может привести к ряду последствий.

2 Последствие может быть определенным или неопределенным и может оказывать положительное или отрицательное влияние на цели.

3 Последствие может быть выражено качественно или количественно.

4 Первоначальные последствия могут обостряться через побочные эффекты.

3.8 **непрерывность** (continuity): Стратегические и тактические возможности, предварительно одобренные руководством организации, для планирования и реагирования на условия, ситуации и события для продолжения деятельности на приемлемом предварительно определенном уровне.

Примечание — Термин «непрерывность», используемый в настоящем стандарте, является более общим термином для непрерывности операций и деятельности, чтобы гарантировать способность организации продолжать работать за пределами нормальных условий работы. Это относится не только к коммерческим компаниям, но и к организациям любых видов деятельности, например неправительственным, общественным и государственным организациям.

3.9 **корректирующие действия** (corrective action): Действия, предпринятые для устранения причины обнаруженного несоответствия.

Примечания

1 У несоответствия может быть несколько причин.

2 Для предотвращения повторения предпринимают корректирующие действия, а для предотвращения возникновения — предупреждающие действия.

3.10 **кризис** (crisis): Нестабильное состояние, связанное с предстоящим резким или значительным изменением, требующим неотложного внимания и действий для защиты жизни, активов.

3.11 **кризисное управление/кризис менеджмент** (crisis management): Целостный процесс управления, выявляющий потенциальные воздействия, которые угрожают организации, и обеспечивающий основу для повышения устойчивости с возможностью эффективного реагирования. Данный процесс управления защищает интересы ключевых заинтересованных сторон организации, репутацию, бренд и деятельность по созданию ценности, а также эффективное восстановление функциональных возможностей.

Примечание — Кризисное управление также включает в себя управление готовностью, реагированием на изменения и непрерывностью или восстановлением в случае инцидента, а также управление всей программой посредством обучения, учений и проверок, чтобы гарантировать, что планы готовности, реагирования и непрерывности продолжают оставаться актуальными и обновляются.

3.12 **команда (группа) кризисного управления (менеджмента)** (crisis management team): Группа лиц, функционально ответственная за руководство разработкой и выполнением плана реагирования и обеспечения непрерывности деятельности, декларирование сбоя или чрезвычайной/кризисной ситуации, а также обеспечение руководства в процессе восстановления, как до, так и после разрушительного инцидента.

Примечание — Команда кризисного управления может включать непосредственных участников, привлеченных сотрудников организации, представителей заинтересованных сторон и других вовлеченных лиц.

3.13 **критически** (critically): Имеет важное значение в отношении целей и/или результатов.

3.14 **анализ критичности** (criticality analysis): Процесс, предназначенный для систематической идентификации и оценки активов организации на основе важности для ее миссии или функций, группы людей, подверженных риску, или значимости нарушения непрерывности деятельности организации.

3.15 **бедствие** (disaster): Событие, которое наносит большой ущерб или потери.

3.16 **нарушение/срыв** (disruption): Ожидаемое или непредвиденное событие, которое прерывает нормальные функции, операции или процессы (например, суровые погодные условия, политические или трудовые беспорядки, отключение коммунальных услуг, криминальный/террористический акт, технологический сбой или землетрясение).

Примечание — Нарушение может быть вызвано как положительными, так и отрицательными факторами, которые нарушают нормальные функции, операции или процессы.

3.17 **документ** (document): Информация и носитель, который ее содержит.

Примечание — Носитель может быть: бумажный, магнитный, электронный или оптический компьютерный диск, фотография или мастер-копия, или их комбинация.

3.18 **чрезвычайная ситуация** (emergency): Внезапное, срочное, обычно неожиданное, событие или событие, требующее немедленных действий.

Примечание — Чрезвычайная ситуация, как правило, является разрушительным событием или состоянием, которое часто можно предвидеть или подготовить, но которое редко бывает точно предвиденным.

3.19 **учения** (exercises): Периодические мероприятия, предназначенные для оценки эффективности членов команды кризисного управления, команды реагирования и персонала при выполнении политики управления устойчивостью.

Примечания

1 Учения включают действия, выполняемые с целью обучения и подготовки членов команды и персонала к соответствующему реагированию с целью достижения максимальных результатов деятельности.

2 Учения могут включать репетицию процедур предотвращения, реагирования и/или обеспечения непрерывности, но более вероятно, что они будут включать моделирование инцидента, заранее объявленного или без предварительного уведомления, в котором участники разыгрывают ролевую игру, чтобы оценить до момента возникновения фактического инцидента, какие проблемы могут возникнуть.

3.20 **эвакуация** (evacuation): Организованное, поэтапное и контролируемое расселение людей из опасных или потенциально опасных районов в безопасные места.

3.21 **событие** (event): Возникновение или изменение определенного набора обстоятельств.

[Руководство ИСО 73:2009, определение 3.5.1.3]

Примечания

1 Событий может быть одно или несколько, одно событие может иметь несколько причин.

2 В рамках события может не происходить ничего негативного.

3 Иногда событие можно назвать «инцидентом» или «несчастным случаем».

4 Событие без последствий называется «почти ошибка», «инцидент», «ложные срабатывания».

3.22 **средство** (facility): Установки, машины, имущество, здания, транспортные средства, корабли, портовые сооружения и другие объекты инфраструктуры или установки и связанные с ними системы, имеющие четко выраженную и поддающуюся количественной оценке функцию деятельности или услуги.

3.23 **опасность** (hazard): Источник потенциального вреда.

[Руководство ИСО 73:2009, определение 3.5.1.4]

Примечание — Опасность может быть источником риска.

3.24 **воздействие** (impact): Оцениваемое последствие определенного результата.

3.25 **анализ воздействия/анализ последствия** (impact (consequence) analysis): Процесс анализа всех функций деятельности и влияния, которое может оказать на них прерывание работы.

Примечание — Анализ воздействия является частью процесса оценки риска и включает анализ воздействия на деятельность: идентификацию критически важных бизнес-активов, функций, процессов и ресурсов, оценку потенциального ущерба или убытков, которые могут быть причинены организации в результате нарушений/срывов или изменения в деятельности или среде организации. Анализ воздействия определяет:

- как потеря или повреждение проявятся;
- степень потенциального увеличения ущерба или потерь со временем, после инцидента;
- минимальные услуги и ресурсы (человеческие, физические и финансовые), необходимые для того, чтобы бизнес-процессы продолжали функционировать на минимально приемлемом уровне;
- объем и сроки в течение которого деятельность, функции и услуги организации должны быть восстановлены.

3.26 **инцидент** (incident): Событие, которое может привести к человеческим, нематериальным или физическим потерям или нарушению/срыву операций, услуг или функций организации, которые, если не будут выполнены, могут перерасти в чрезвычайную ситуацию, кризис или бедствие.

3.27 **целостность** (integrity): Свойство сохранения точности и полноты активов.

3.28 **вероятность возникновения/правдоподобность появления события** (likelihood): Шанс, что что-то произойдет.

[Руководство ИСО 73:2009, определение 3.6.1.1]

Примечание — В терминологии управления рисками слово «вероятность» используется для обозначения вероятности чего-либо происходящего, определенного, измеренного или определенного объективно или субъективно, качественно или количественно и описанного с использованием общих терминов или математически (например, вероятность или частота за определенный период времени).

3.29 **план управления** (management plan): Четко определенный и документированный план действий, обычно охватывающий ключевой персонал, ресурсы, услуги и действия, необходимые для реализации процесса управления.

3.30 **минимизация последствий** (mitigation): Ограничение любых негативных последствий конкретного инцидента.

3.31 **соглашение о взаимопомощи** (mutual aid agreement): Предварительно согласованное соглашение, разработанное между двумя или более организациями для оказания помощи сторонам соглашения.

3.32 **несоответствие** (nonconformity): Невыполнение требования.

3.33 **цель** (objective): Общая цель в соответствии с политикой, которую организация ставит перед собой.

3.34 **организация** (organization): Группа людей (и средств) с распределением обязанностей, полномочий и отношений.

Пример — Публичная или частная компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, индивидуальный предприниматель, ассоциация или их части и комбинации.

3.35 **политика** (policy): Общие намерения и направления деятельности организации, сформулированные и выраженные высшим руководством.

Примечание — В настоящем стандарте описаны требования для одной такой политики — политики устойчивости цепи поставок.

3.36 **готовность** (preparedness/readiness): Мероприятия, программы и системы, разработанные и реализованные до инцидента, которые могут быть использованы для усиления поддержки и предупреждения, защиты, минимизации последствий, реагирования и восстановления после нарушений/срывов, чрезвычайных ситуаций или бедствий.

3.37 **предупреждение** (prevention): Мероприятия, позволяющие организации избежать, исключить или ограничить вероятность или последствия нарушения/срыва.

3.38 **предупреждающие действия** (preventive action): Действия по устранению причины потенциального несоответствия или другой нежелательной ситуации.

Примечания

1 Может быть несколько причин потенциального несоответствия.

2 Предупреждающие действия предпринимаются для предотвращения возникновения, тогда как корректирующие действия — для предотвращения повторения.

3.39 **предупреждение опасностей и угроз** (prevention of hazards and threat): Процессы, практики, методы, материалы, продукты, услуги или ресурсы, используемые для предотвращения, уменьшения или управления опасностями и угрозами и связанными с ними рисками любого типа с целью уменьшения их потенциальной вероятности или последствий.

3.40 **возможность/вероятность** (probability): Мера возможности появления события, выражаемая действительным числом из интервала от 0 до 1, где 0 соответствует невозможному, а 1 — достоверному событию.

[Руководство ИСО 73:2009, определение 3.6.1.4]

Примечание — См. также 3.28.

3.41 **процедура** (procedure): Установленный порядок выполнения деятельности или процессов.

Примечания

1 Процедура может быть в любой форме и на любом носителе.

2 Если процедура представлена в письменной форме, используется термин «документированная процедура».

3 Документ, содержащий процедуру, может называться процедурой.

3.42 **запись** (record): Документ с указанием достигнутых результатов или с подтверждением выполненных действий.

Примечания

1 Записи могут использоваться, например, для документирования прослеживаемости и предоставления доказательств проверки, предупреждающих и корректирующих действий.

2 Как правило, записям не присваивается номер редакции.

3.43 **остаточный риск** (residual risk): Риск, оставшийся после воздействия на риски.

[Руководство ИСО 73:2009, определение 3.8.1.6]

Примечания

1 Остаточный риск может содержать неопознанный риск.

2 Остаточный риск также может быть известен как «оставшийся риск».

3.44 **устойчивость** (resilience): Способность справиться и адаптироваться к сложной и изменяющейся среде.

[Руководство ИСО 73:2009, определение 3.8.1.7]

Примечания

1 Устойчивость — это способность организации предотвращать или сопротивляться воздействию события или способность возвращаться к приемлемому уровню результатов деятельности и в приемлемый период времени после воздействия события.

2 Устойчивость — это способность системы поддерживать свои функции и структуру перед лицом внутренних и внешних изменений, которая может постепенно ухудшаться.

3.45 **ресурсы** (resources): Любые активы (человеческие, физические, информационные или нематериальные), объекты, оборудование, материалы, продукты или отходы, которые имеют потенциальную ценность и могут быть использованы.

3.46 **план реагирования** (response plan): Документированный сборник процедур и информации, разрабатываемых, комплектуемых, поддерживаемых в состоянии готовности для использования при возникновении инцидента.

3.47 **программа реагирования** (response program): Планирование, процессы и ресурсы для выполнения действий и услуг, необходимых для сохранения и защиты жизни, имущества, операций и критически важных активов.

Примечание — Действия по реагированию обычно включают в себя распознавание инцидента, уведомление, оценку, декларирование, выполнение плана, обмен информацией и управление ресурсами.

3.48 **группа реагирования/команда реагирования** (response team): Группа лиц, ответственных за разработку, выполнение учения и поддержание плана реагирования, включая процессы и процедуры.

3.49 **риск** (risk): Влияние неопределенности на достижение поставленных целей.

[Руководство ИСО 73:2009, определение 1.1]

Примечания

1 Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).

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).

3 Риск часто характеризуют путем описания возможного события и его последствий или их сочетания.

4 Риск часто представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности.

5 Неопределенность — это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей.

3.50 **принятие риска** (risk acceptance): Обоснованное решение о принятии риска.
[Руководство ИСО 73:2009, определение 3.7.1.6]

Примечания

1 Принятие риска может происходить без обработки риска или в процессе обработки риска.

2 Принятые риски подлежат мониторингу и последующему анализу.

3.51 **анализ риска** (risk analysis): Процесс изучения природы и характера риска и определения уровня риска.
[Руководство ИСО 73:2009, определение 3.6.1]

Примечания

1 Анализ риска обеспечивает основу для оценки риска и принятия решений относительно обработки риска.

2 Анализ риска включает оценку риска.

3.52 **оценка риска** (risk assessment): Процесс, охватывающий идентификацию риска, анализ риска и сравнительную оценку риска.
[Руководство ИСО 73:2009, определение 3.4.1]

Примечание — Оценка риска включает процесс выявления внутренних и внешних угроз и уязвимостей, выявления вероятности и последствий события, возникающего из-за таких угроз или уязвимостей, определение критических функций, необходимых для продолжения деятельности организации, определение элементов управления, необходимых для уменьшения подверженности риску, и оценку стоимости таких элементов управления.

3.53 **информирование о риске** (risk communication): Обмен или распространение информации о риске между лицом, принимающим решения, и другими заинтересованными сторонами.

Примечания

1 Руководство ИСО/МЭК 73:2002 (определение 3.2.4), которое было изъято и заменено Руководством ИСО 73:2009.

2 Информация может относиться к существованию, природе, форме, вероятности, серьезности, приемлемости, обработке или другим аспектам риска.

3.54 **критерий риска** (risk criteria): Совокупность факторов, по сопоставлению с которыми оценивают значимость риска (1.1).
[Руководство ИСО 73:2009, определение 3.3.1.3]

Примечания

1 Критерии риска основаны на целях организации, а также на ее внешней и внутренней среде.

2 Критерии риска могут быть рассчитаны.

3.55 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.
[Руководство ИСО 73:2009, определение 2.1]

Примечание — Менеджмент риска обычно включает оценку рисков, обработку рисков, принятие рисков и информирование о рисках.

3.56 **снижение риска** (risk reduction): Действия, предпринятые для уменьшения вероятности, негативных последствий (или того и другого), связанных с риском.

Примечание — Из Руководства ИСО/МЭК 73:2002, определение 3.4.4, которое было изъято и заменено на Руководство ИСО 73:2009.

3.57 **передача риска/разделение риска** (risk sharing (transfer): Форма обработки риска, включающая согласованное распределение риска с другими сторонами.

[Руководство ИСО 73:2009, определение 3.8.1.3]

Примечания

1 Законодательные или обязательные требования могут ограничивать, запрещать или поручать передачу определенного риска.

2 Разделение риска может быть осуществлено посредством страхования или других форм контракта.

3 Степень, в которой риск разделяется, может зависеть от надежности и ясности соглашений о совместном использовании.

4 Передача риска является формой разделения риска.

3.58 **допустимый риск** (risk tolerance): Риск, который организация и причастные стороны готовы сохранять после обработки риска для достижения своих целей.

3.59 **воздействие на риск** (risk treatment): Процесс модификации риска.

[Руководство ИСО 73:2009, определение 3.8.1]

Примечания

1 Обработка рисков может включать:

- избегание риска, принимая решение не начинать или продолжать деятельность, которая порождает риск;
- принятие или увеличение риска, чтобы воспользоваться возможностью;
- устранение источника риска;
- изменение вероятности;
- изменение последствий;
- разделение риска с другой стороной или сторонами (включая контракты и финансирование рисков) и сохранение риска путем осознанного выбора.

2 Обработка рисков, которая имеет дело с негативными последствиями, иногда называется: «смягчение риска», «перенос риска», «ограничение риска», «предотвращение риска» и «снижение риска».

3 Обработка рисков может создать новые риски или изменить существующие риски.

3.60 **защищенность/безопасность** (security): Состояние защиты от опасностей, угроз, рисков или потери.

Примечание — В общем смысле защищенность — это концепция, аналогичная безопасности. Различие между ними заключается в дополнительном акценте на защиту от опасностей, исходящих извне.

3.61 **аспекты безопасности/защищенности** (security aspects): Конкретные характеристики, элементы или свойства, снижающие риск непреднамеренных, преднамеренных и естественных кризисов и катастроф, которые нарушают и оказывают влияние на продукты и услуги, работу, критически важные активы и непрерывность деятельности организации и ее заинтересованных сторон.

3.62 **источник риска** (source): Все, что по отдельности или в сочетании обладает внутренним потенциалом для возникновения риска.

Примечания

1 Адаптировано из Руководства ИСО 73:2009, определение 3.5.1.2.

2 Источник риска может быть материальным или нематериальным.

3.63 **заинтересованная сторона/стейкхолдер** (stakeholder/interested party): Физическое или юридическое лицо, заинтересованное в эффективности, успехе или результативности деятельности организации.

[Руководство ИСО 73:2009, определение 3.2.1.1]

Примечания

1 Например, клиенты, акционеры, финансовые компании, страховые компании, регулирующие органы, государственные органы, сотрудники, подрядчики, поставщики, профсоюзы, общество.

2 Лицо, принимающее решение, может быть заинтересованной стороной.

3.64 **цепь поставок** (supply chain): Взаимосвязанный набор ресурсов и процессов, который начинается с поиска сырья и распространяется через доставку продуктов или услуг конечному потребителю посредством различных видов транспорта.

[ИСО 28000:2007, определение 3.9]

Примечание — Цепь поставок может включать поставщиков, производственные мощности, поставщиков логистических услуг, внутренние распределительные центры, дистрибьюторов, оптовых торговцев и другие организации, ведущие к конечному пользователю (потребителю).

3.65 **целевой показатель** (target): Детализированные требования к результатам деятельности, применимые к организации (или к ее подразделениям), вытекающие из целей. Целевые показатели должны быть установлены и выполнены для достижения этих целей.

Примечание — Адаптировано из ИСО 14001:2004, определение 3.12.

3.66 **тестирование/испытание** (testing): Действия, выполненные для оценки эффективности или возможностей плана относительно определенных целей или критериев измерения.

Примечание — Обычно тестирование включает в себя учения, предназначенные для того, чтобы команды и сотрудники эффективно выполняли свои обязанности и выявляли слабые стороны планов готовности и реагирования/непрерывности/восстановления.

3.67 **угроза** (threat): Потенциальная причина нежелательного инцидента, который может привести к причинению вреда людям, активам, системе или организации, окружающей среде или сообществу.

3.68 **высшее руководство** (top management): Лицо или группа лиц, осуществляющие руководство и управление организацией на самом высоком уровне.

3.69 **уязвимость** (vulnerability): Внутренние свойства чего-либо, что приводит к восприимчивости к источнику риска, который может привести к событию со следствием.

[Руководство ИСО 73:2009, определение 3.6.1.6]

3.70 **оценка уязвимости** (vulnerability assessment): Процесс выявления и количественной оценки уязвимостей.

4 Требования к системе менеджмента, включая политику устойчивости

4.1 Общие требования

Организация должна разработать политику устойчивости цепи поставок в соответствии с требованиями настоящего стандарта. Для того чтобы данная политика была результативной, она должна быть интегрирована в систему менеджмента. Если требования, идентичные требованиям настоящего стандарта, были ранее учтены при внедрении уже существующей системы менеджмента, эти требования не нужно дублировать отдельно.

4.2 Понимание организации и ее среды

4.2.1 Организация должна определить и задокументировать внутренние и внешние факторы среды организации.

Организация должна:

a) идентифицировать факторы внешней среды организации, в том числе:

- культурные, политические, социальные, правовые, нормативные, финансовые, технологические, экономические, природные и конкурентные факторы на международном, национальном, региональном или местном уровнях;
- уровень цепи поставок, обязательства и отношения, ключевые движущие силы и тенденции, воздействующие цели организации;
- восприятие и ценности заинтересованных сторон;

b) идентифицировать факторы внутренней среды организации, в том числе:

- активы, виды деятельности, функции, услуги, продукты, партнерства, цепь поставок и отношения заинтересованных сторон;
- способности, понимаемые с точки зрения ресурсов и знаний (например, капитала, времени, людей, процессов, систем и технологий);
- информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);
- внутренние заинтересованные стороны;
- политики, цели и стратегии для их достижения;
- восприятие, ценности и культура организации;
- стандарты и эталонные модели, принятые организацией;
- структуры (например, управление, обязанности и ответственность).

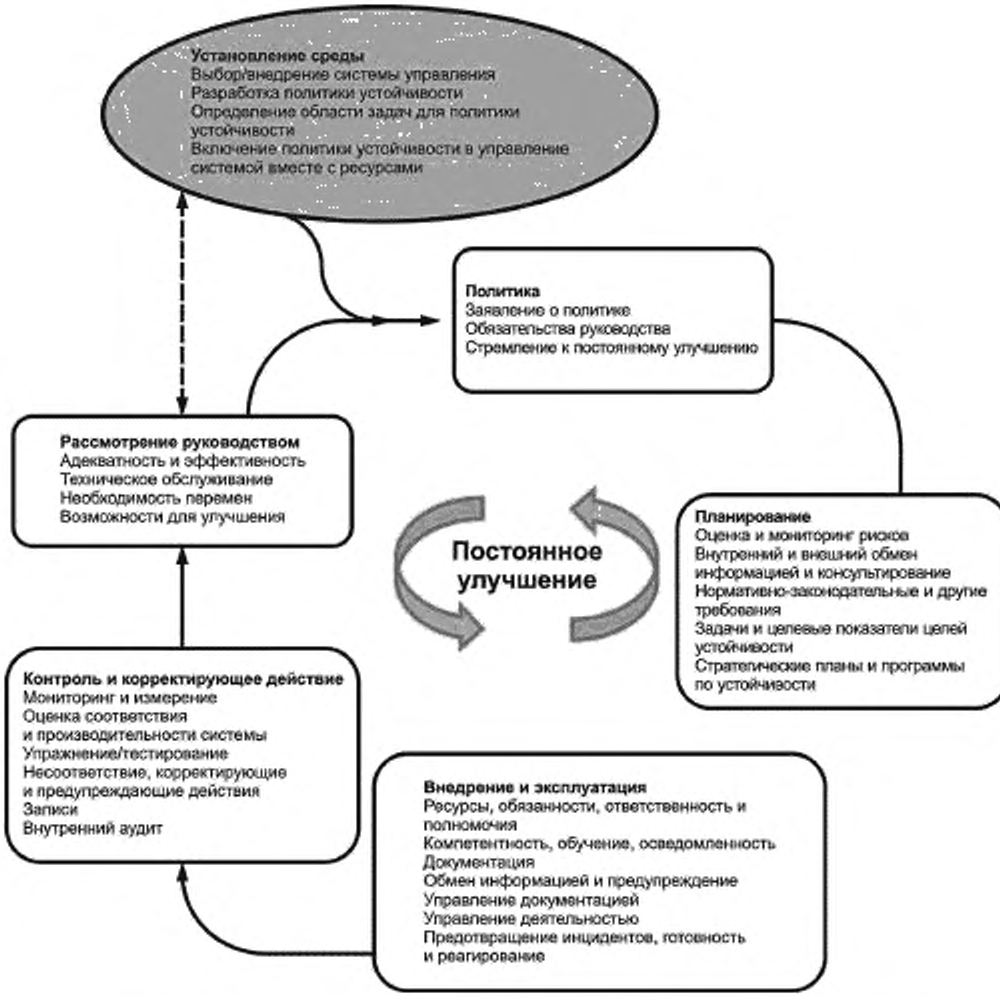

Рисунок 4 — Диаграмма потоков системы менеджмента, включая политику устойчивости

4.2.2 С целью демонстрации своей приверженности процессу управления рисками и устойчивости при анализе своей среды организация должна определить и задокументировать следующие специфические внутренние и внешние факторы:

a) критические действия организации, функции, услуги, продукты, партнерства, отношения цепи поставок, заинтересованные стороны и потенциальное воздействие, связанное с разрушительным инцидентом в пределах одной или более цепей поставок;

b) компоненты сквозной цепи поставок товаров или услуг, показывающие, как они настроены или связаны для доставки критических товаров и/или услуг;

c) связь между политикой управления устойчивостью, целями организации и другими политиками;

d) обоснование необходимости процесса управления рисками и управления устойчивостью;

e) полномочия и ответственность по процессу управления рисками и устойчивости;

f) предпочтительный риск организации или неприятие риска;

g) ресурсы, доступные для помощи тем, кто обладает полномочиями и ответственностью в области процесса управления рисками и устойчивости;

h) приверженность периодическому анализу и пересмотру политики менеджмента устойчивости;

i) постоянное улучшение.

4.3 Область применения политики менеджмента устойчивости

Организация должна определить и задокументировать цели и область применения политики менеджмента устойчивости с указанием специфичных внутренних и внешних факторов среды организации.

При определении области применения организация должна:

a) определить границы организации, которые должны быть включены в сферу политики устойчивости. Это может быть вся организация, одно или несколько подразделений, или компоненты одного или нескольких потоков сквозной цепи поставок товаров и услуг;

b) установить требования к менеджменту устойчивости с учетом целей организации, задач, внутренних и внешних обязательств (в том числе связанных с заинтересованными сторонами и юридическими обязанностями);

c) рассмотреть критические цели деятельности, активы, виды деятельности, функции, товары и услуги;

d) определить риски, основанные как на внутренних, так и на внешних потенциальных нарушениях/срывах, которые могут негативно повлиять на деятельность и функции организации в контексте их потенциальной вероятности воздействия;

e) определить область применения политики менеджмента устойчивости в соответствии с размерами, характером и сложностью деятельности организации с позиции постоянного улучшения.

Организация должна определить область применения, которая позволит защитить и сохранить целостность организации и ее цепи поставок, включая отношения с заинтересованными сторонами, взаимодействие с ключевыми поставщиками, партнерами по аутсорсингу и др., заинтересованные стороны (например, партнеры по цепи поставок, поставщики, потребители, акционеры, сообщество, в котором функционирует организация, и т. д.).

На основе оценки риска организация также должна присвоить стратегические весовые коэффициенты менеджменту безопасности, обеспечению готовности, минимизации последствий, кризисному управлению, управлению чрезвычайными ситуациями, управлению непрерывностью деятельности, управлению и восстановлению управления при возникновении бедствий (см. 4.4).

4.4 Обеспечение ресурсами для реализации политики менеджмента устойчивости

Руководство должно обеспечить наличие ресурсов, необходимых для реализации и управления политикой менеджмента устойчивости. Ресурсы включают человеческие ресурсы и специализированные навыки, оборудование, внутреннюю инфраструктуру, технологии, информацию, интеллектуальные и финансовые ресурсы.

4.5 Политика менеджмента устойчивости

Высшее руководство должно разработать, задокументировать и обеспечить ресурсами систему менеджмента организации, в которую интегрируется политика менеджмента устойчивости, подтверждая приверженность защите человеческих, природных и физических активов, осуществлению прогнозирования и подготовки к возможным неблагоприятным событиям; устойчивости производственной деятельности и бизнеса.

4.6 Заявление о политике

Для интеграции в существующую систему менеджмента при применении настоящего стандарта должно быть разработано заявление о политике. Заявление о политике устойчивости должно соответствовать характеру и масштабу потенциальных угроз, опасностей, рисков и последствий их воздействия на деятельность, функции организации, товары, услуги и цепь поставок.

Политика должна.

a) в качестве первоочередной задачи включать обязательство по обеспечению безопасности жизни сотрудников и общества;

b) включать обязательство постоянного улучшения;

c) включать обязательство по улучшению организационной структуры, устойчивости и непрерывности цепи поставок;

d) включать обязательство по адаптивной и проактивной минимизации риска;

e) включать обязательство соблюдать применимые нормативно-законодательные и другие требования, относящиеся к организации;

f) включать определение и документальное отражение допустимого риска, связанного с областью применения политики, с четким адресным отнесением, где в системе менеджмента, внедренной в организации, рассматриваются аспекты, относящиеся к устойчивости;

g) включать рамки для установления и анализа целей и целевых показателей политики устойчивости;

h) включать ссылки на исключения и ограничения.

Политика должна содержать:

- ответственное лицо за разработку политики с контактными данными,
- описание, как документируется, внедряется и поддерживается в рабочем состоянии политика устойчивости;
- доведение до сведения персонала и лиц, работающих от имени организации;
- обеспечение доступности для заинтересованных сторон.

Примечание — Организация может принять решение обнародовать неконфиденциальную версию своей политики, исключив из нее конфиденциальную информацию, связанную:

a) с проведением анализа через запланированные интервалы времени и действиями в условиях значительных изменений;

b) с официальным одобрением высшим руководством.

Приложение А
(справочное)

Информационное руководство по интеграции настоящего стандарта в существующую систему менеджмента организации

А.1 Общие положения

Организации, внедряющие настоящий стандарт, обязаны интегрировать политику менеджмента устойчивости в систему менеджмента, основанную на цикле PDCA. Политика менеджмента устойчивости может быть одной из многих политик, принятых организацией при определении общей политики управления организацией. Политика менеджмента устойчивости становится вкладом в систему менеджмента организации. Разработку, внедрение, потребности в ресурсах и управление выполнением каждой корпоративной политики следует документировать в рамках систем менеджмента. В этом приложении содержится информационное руководство по включению элементов политики устойчивости в политику системы менеджмента на основе цикла PDCA. Если в систему менеджмента также включают другие политики, следует обратиться за соответствующим руководством.

А.2 Политика менеджмента устойчивости

Политика менеджмента устойчивости должна быть разработана и документирована в соответствии с требованиями настоящего стандарта. Политика должна быть добавлена к другим, уже существующим политикам по системам менеджмента.

А.3 Ответственность руководства

Руководство должно предоставить свидетельства вовлеченности в разработку, внедрение, реализацию, мониторинг, анализ, поддержание в рабочем состоянии и улучшение политики устойчивости посредством:

a) разработки политики менеджмента устойчивости;

b) обеспечения разработки целей и планов реализации политики менеджмента устойчивости;

c) установления ролей, компетенций, ответственности за выполнение функций менеджмента устойчивости;

d) назначения одного (или более) ответственного компетентного специалиста за политику менеджмента устойчивости с определением конкретных полномочий и ответственности за внедрение и поддержание системы менеджмента устойчивости;

e) информирования организации о важности выполнения целей менеджмента устойчивости и соответствия политике менеджмента устойчивости, ответственности за соблюдение нормативно-законодательных требований и необходимости постоянного улучшения;

f) выделения достаточных ресурсов для разработки, внедрения, реализации, мониторинга, анализа, поддержания в рабочем состоянии и улучшения менеджмента устойчивости;

g) определения критериев допустимого риска и допустимых уровней риска;

h) обеспечения проведения внутренних аудитов по политике менеджмента устойчивости;

i) проведения анализа со стороны руководства политики менеджмента устойчивости;

j) демонстрации вовлеченности в постоянное улучшение.

А.4 Планирование

А.4.1 Оценка рисков и мониторинг

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процесс оценки риска:

a) для идентификации рисков преднамеренных, непреднамеренных и естественных опасностей и угроз, которые могут иметь прямое или косвенное воздействие на деятельность, операции, функции и цепь поставок организации, человеческие, нематериальные и физические активы, природную среду и заинтересованные стороны;

b) для систематического анализа рисков (включая вероятность, уязвимость, критичность воздействия и последствия);

c) для идентификации рисков, имеющих значительные последствия для деятельности, функций, товаров и услуг, цепи поставок организации, отношений с заинтересованными сторонами, природной среды;

d) для систематической оценки и расстановки приоритетов управления рисками и обработки рисков и соответствующих затрат.

Организация должна:

a) документировать и сохранять эту информацию актуальной и конфиденциальной, если применимо;

b) с установленной периодичностью анализировать и пересматривать область распространения и политику менеджмента устойчивости, оценку рисков, оценку продолжающейся пригодности внешних и внутренних факторов среды организации;

c) гарантировать, что приоритетные риски учитывают при разработке, внедрении и функционировании системы менеджмента устойчивости;

d) проводить повторную оценку риска при изменении факторов среды организации, производственной среды, процедур, функций, услуг, сервисов, в партнерских соглашениях и цепи поставок;

e) разрабатывать критерии для оценки степени риска. Критерии должны отражать внутренние и внешние факторы среды организации, включая ценности, цели и ресурсы;

f) установить критерии для максимально допустимого времени простоя, целевого показателя времени восстановления, а также приемлемых уровней потерь, связанных с товарами, услугами и функциями организации и ее цепи поставок;

g) установить приоритетные сроки восстановления деятельности и функций внутри организации и по всей цепи поставок;

h) оценивать прямые и косвенные преимущества и затраты от вариантов снижения риска и повышения устойчивости и непрерывности.

А.4.2 Внутреннее и внешнее информирование и консультирование

В процессе оценки риска организация должна разработать, внедрить и поддерживать в рабочем состоянии документированный процесс обмена информацией и консультирования с заинтересованными сторонами и партнерами по цепи поставок, чтобы гарантировать, что:

a) риск адекватно идентифицирован;

b) понятны интересы заинтересованных сторон, зависимости и связи в цепи поставок;

c) оценку устойчивости и оценку риска проводят во взаимодействии с другими аспектами управления; а также

d) оценку риска проводят в рамках соответствующих факторов внутренней и внешней среды и параметров, относящихся к организации и ее цепи поставок.

А.4.3 Мониторинг и анализ процесса оценки риска

Организация должна разработать, внедрить, поддерживать в рабочем состоянии и документировать процесс мониторинга и анализа оценки рисков для:

a) актуализации оценки риска (при необходимости);

b) определения и оценивания влияния среды, внешних и внутренних факторов, предположений и других обстоятельств, которые могут меняться со временем, на оценку рисков;

c) оценки эффективности управления рисками и обработки рисков;

d) оценки фактической эффективности после инцидента.

А.4.4 Нормативно-законодательные и иные требования

Организация должна установить и поддерживать в рабочем состоянии процедуры для:

a) идентификации нормативно-законодательных и иных требований, которые относятся к организации и соотносятся с опасностями, угрозами и рисками, связанными с ее объектами, средствами, деятельностью, функциями, товарами, услугами, цепью поставок, средой и заинтересованными сторонами;

b) определения, насколько эти требования применимы к опасностям, угрозам, риску и их потенциальному воздействию и насколько эти требования выполняются.

Организация должна документировать данную информацию и поддерживать ее в актуальном состоянии.

Организация должна обеспечить, чтобы применимые нормативно-законодательные требования, которыми она руководствуется, учитывались при разработке, внедрении и поддержании в рабочем состоянии ее системы менеджмента устойчивости.

А.4.5 Цели и целевые показатели в области устойчивости

Организация должна разработать, внедрить и поддерживать в рабочем состоянии документированные цели и целевые показатели для управления рисками с целью предотвращения, избегания, сдерживания, смягчения, реагирования и восстановления после разрушительных инцидентов. Документированные цели и целевые показатели должны устанавливать внутренние и внешние ожидания для организации и ее цепи поставок, которые имеют решающее значение для выполнения миссии, доставки продуктов и услуг и функциональных операций.

Цели должны быть разработаны и согласованы с политикой менеджмента устойчивости и оценкой риска, включая обязательства по:

a) минимизации риска путем снижения вероятности его возникновения и тяжести последствий;

b) увеличению устойчивости посредством адаптивного, проактивного и ретроспективного подходов с учетом финансовых, функциональных (производственных) требований и требований бизнеса, включая цепь поставок;

c) соблюдению нормативно-законодательных и иных требований;

d) постоянному улучшению.

При разработке и пересмотре целей и целевых показателей организация должна учитывать нормативно-законодательные и иные требования, значительные риски, технологические возможности организации, финансовые, функциональные требования и требования бизнеса, мнения заинтересованных сторон и участников.

Целевой показатель должен быть измерен качественно и/или количественно. Целевые показатели должны соответствовать целям политики устойчивости и должны быть получены из целей политики устойчивости. Целевые показатели должны:

a) иметь соответствующий уровень детализации;

b) быть соразмерны оценке риска и установленным организацией срокам для восстановления;

c) быть конкретными, измеримыми, достижимыми, актуальными и основанными на времени (где это практически осуществимо);

d) быть доведены до сведения персонала и третьих сторон, включая подрядчиков и партнеров по цепи поставок, с намерением, чтобы эти лица были осведомлены о своих индивидуальных обязательствах;

e) периодически пересматриваться, чтобы гарантировать, что они остаются актуальными и соответствующими целям политики менеджмента устойчивости и своевременно корректируются.

A.4.6 Стратегические планы и программы для обеспечения устойчивости

Организация должна разработать, внедрить и поддерживать в рабочем состоянии одну и более стратегических программ для достижения целей и целевых показателей. Программы должны быть оптимизированы и расставлены по приоритетам для управления и снижения риска на основе вероятности его возникновения и тяжести последствий в виде нарушения/сбоя цепи поставок организации. Программа(ы) должна(ы) включать:

a) определение ответственности и ресурсов для достижения целей и целевых показателей в соответствии с функциями и уровнем в организации;

b) рассмотрение деятельности и функций организации, нормативно-законодательных требований, обязательств по договорам/контрактам и цепи поставок, потребностей заинтересованных сторон, соглашений о взаимопомощи и среды организации;

c) средства, временны́е рамки и распределение ресурсов, с помощью которых должны быть достигнуты цели менеджмента устойчивости, цели и целевые показатели устойчивости.

Организация должна разработать и поддерживать в рабочем состоянии один или более стратегических планов и программ для:

a) предупреждения и защиты — избегать, устранять, сдерживать, защищать или предотвращать вероятность разрушительных инцидентов и их последствий, включая удаление человеческих и физических активов из зоны риска;

b) минимизации последствий — минимизация воздействия разрушительного инцидента;

c) реагирования — первоначальная реакция на разрушительный инцидент, связанный с защитой людей и имущества от немедленного вреда. Первоначальная реакция руководства может быть частью первой реакции организации;

d) непрерывности — доступность процессов, средств управления и ресурсов для обеспечения того, чтобы организация продолжала выполнять свои критически важные бизнес-задачи и цели;

e) восстановления — возобновление процессов, ресурсов и возможностей организации для удовлетворения текущих операционных требований в течение периода времени, указанного в целях.

Организация должна оценивать свою стратегическую(ие) программу(ы), чтобы определить, создают ли эти мероприятия новые риски. Программы менеджмента устойчивости следует периодически пересматривать, чтобы обеспечить их эффективность и соответствие целям и целевым показателям. При необходимости в программы должны быть соответствующим образом внесены изменения.

A.5 Внедрение и функционирование

A.5.1 Ресурсы, обязанности, ответственность и полномочия в области менеджмента устойчивости

Обязанности, ответственность и полномочия должны быть определены, задокументированы и доведены до сведения, чтобы способствовать эффективному управлению устойчивостью в соответствии с политикой менеджмента устойчивости, целями, целевыми показателями и программами. Высшее руководство организации должно назначить конкретного представителя руководства, который, независимо от других обязанностей, должен выполнять определенные обязанности, иметь ответственность и полномочия для:

a) обеспечения, того, чтобы политика менеджмента устойчивости была разработана, внедрена, доведена до персонала и поддерживалась в рабочем состоянии в соответствии с требованиями настоящего стандарта;

b) идентификации и мониторинга требований и ожиданий партнеров и заинтересованных сторон цепи поставок организации и принятия соответствующих мер для управления этими ожиданиями;

c) обеспечения доступности необходимых ресурсов;

d) представления отчетов о выполнении политики менеджмента устойчивости высшему руководству для рассмотрения и в качестве основы для улучшений.

Организация должна создать:

a) систему менеджмента устойчивости, кризисное управление, группу(ы) реагирования с определенными ролями, конкретными полномочиями и необходимыми ресурсами для контроля возникновения инцидентов, предупреждения, обеспечения готовности, реагирования и восстановления;

b) логистические возможности и процедуры для поиска, приобретения, хранения, распространения, обслуживания, тестирования и учета услуг, персонала, ресурсов, материалов и средств, произведенных или переданных для поддержки системы менеджмента;

c) цели управления ресурсами персонала, оборудования, обучения, средств финансирования, страхования, контроля ответственности, экспертных знаний, материалов и временны́х рамок, в которых они будут необходимы из ресурсов организации и от любого партнера для соблюдения времени реагирования;

d) процедуры поддержки и информирования заинтересованных сторон, стратегических альянсов и взаимопомощи.

Организация должна разработать финансовую(ые) и административную(ые) процедуру(ы) для поддержания политики менеджмента устойчивости до момента возникновения инцидента, в ходе и после его возникновения.

Процедуры должны:

a) обеспечивать гарантию быстрого выполнения решений о выделении средств;

b) соответствовать установленным уровням полномочий и принципам бухгалтерского учета.

А.5.2 Компетентность, подготовка и осведомленность

Организация должна гарантировать, что любое лицо, выполняющее задачи, которое потенциально может предотвратить, вызвать, реагировать, снизить или влиять на значительные опасности, угрозы и риски, является компетентным (на основании соответствующего образования, обучения или опыта), с сохранением подтверждающих записей.

Организация должна определить компетенции и потребности в обучении, связанные с управлением опасностями, угрозами и рисками, характерными для организации, политикой менеджмента устойчивости, как внутри организации, так и по всей ее цепи поставок. Организация должна обеспечивать обучение и подготовку или предпринимать другие действия для удовлетворения этих потребностей с сохранением соответствующих записей.

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуру(ы), чтобы гарантировать, что все лица, работающие в организации или от ее имени, осведомлены:

a) о значительных опасностях, угрозах и рисках, которые связаны с их работой, потенциальных воздействиях, преимуществах лучшего выполнения работы;

b) о процедурах предупреждения инцидента, сдерживания, минимизации последствий, индивидуальной защиты, эвакуации, реагирования, поддержания непрерывности и восстановления;

c) о важности выполнения требований политики и процедур менеджмента устойчивости и требований системы менеджмента безопасности цепи поставок;

d) о своей обязанности и ответственности в достижении соответствия требованиям политики менеджмента устойчивости;

e) о потенциальных последствиях отклонений от указанных процедур; а также

f) о преимуществах улучшения персональных результатов работы.

Организация должна создать, продвигать и внедрить культуру менеджмента устойчивости в рамках организации и цепи поставок, которая:

a) обеспечивает, чтобы культура менеджмента устойчивости стала частью основных ценностей организации, цепи поставок и управления организацией в целом;

b) обеспечивает осведомленность партнеров по цепи поставок и заинтересованных сторон о политике менеджмента устойчивости и их обязанностей в любых планах по обеспечению устойчивости.

А.5.3 Информирование и оповещение

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры в отношении опасностей, угроз, рисков и политики менеджмента устойчивости для:

a) документирования, ведения записей, информирования об изменениях в документации, планах и процедурах, системе менеджмента, результатах оценки и анализа;

b) внутреннего обмена информацией между различными уровнями и функциями организации;

c) внешнего обмена информацией в рамках цепи поставок с другими партнерами и заинтересованными сторонами;

d) приема, документирования и ответа на информацию от внешних заинтересованных сторон;

e) адаптации и интеграции национальной или региональной консультативной системы по рискам и угрозам или ее эквивалента в планирование и оперативное использование в работе;

f) переноса обмена важной информацией и знаниями в цепи поставок между партнерами и заинтересованными сторонами;

g) предупреждения об опасности потенциального воздействия фактического или надвигающегося разрушительного инцидента заинтересованных сторон и партнеров в цепи поставок;

h) обеспечения доступности средств связи для информирования в кризисной ситуации нарушения/сбоя;

i) облегчения структурированного обмена информацией между респондентами, непосредственно находящимися в чрезвычайной ситуации;

j) обеспечения взаимодействия нескольких организаций-респондентов и персонала;

k) ведения записи значимой информации об инциденте, предпринятых действиях и принятых решениях;

l) работы средств коммуникаций.

Организация должна решить, исходя из целей безопасности жизнедеятельности, какие первоочередные задачи осуществлять по обеспечению устойчивости. Организация должна проконсультироваться с партнерами по цепи поставок и заинтересованными сторонами, чтобы решить, какую информацию предоставлять внешним заинтересованным сторонам о значительном риске. Данное решение организация должна документировать. Если решение состоит в том, чтобы сообщить информацию, организация должна разработать и внедрить метод(ы) для этого внешнего обмена информацией, передачи оповещений и сигналов тревоги (в том числе с помощью средств массовой информации).

Информирование о политике менеджмента устойчивости должно регулярно тестироваться.

А.5.4 Документирование

Документация политики менеджмента устойчивости должна включать:

a) политику менеджмента устойчивости, цели и целевые показатели;

b) описание области применения политики менеджмента устойчивости;

c) описание основных элементов политики менеджмента устойчивости и их интеграцию в соответствующие документы;

d) документацию, включая записи, требуемые настоящим стандартом;

e) документацию, включая записи, определенные организацией как необходимые для обеспечения эффективного планирования и управления процессами, относящимися к значительным рискам.

Организация должна оценить конфиденциальность информации и принять соответствующие меры для предотвращения несанкционированного доступа.

А.5.5 Управление документацией

Необходимо управление документацией, регламентируемой политикой менеджмента устойчивости. Записи представляют собой особый тип документа и должны управляться в соответствии с требованиями, приведенными в А.5.4.

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры с целью:

a) соблюдения нормативно-законодательных требований;

b) утверждения документов на предмет адекватности до момента их выдачи;

c) пересмотра, актуализации и повторного утверждения документов, при необходимости;

d) гарантии идентификации внесенных изменений и текущего статуса документов;

e) обеспечения наличия действующих версий в местах их применения;

f) установления параметров хранения, архивирования и утилизации;

g) уверенности в том, что документы остаются разборчивыми и легко идентифицируемыми;

h) гарантии того, что документы внешнего происхождения, определенные организацией как необходимые для планирования и осуществления политики менеджмента устойчивости, идентифицированы и их распределение контролируется;

i) определения способа хранения устаревших и неактуальных документов, которые организация должна хранить;

j) обеспечения целостности документов, гарантии их защищенности от несанкционированного доступа, надежного резервного копирования, доступа только для уполномоченного персонала и защиты от повреждения, порчи или потери.

А.5.6 Управление деятельностью

Организация должна определить те операции и действия, которые необходимы для достижения:

a) политики менеджмента устойчивости;

b) управления действиями, определенными как имеющие значительный риск;

c) соблюдения нормативно-законодательных требований;

d) целей политики менеджмента устойчивости;

e) выполнения программ политики менеджмента устойчивости; и

f) требуемого уровня устойчивости цепи поставок.

Организация должна разработать, внедрить и поддерживать в рабочем состоянии адаптивные и проактивные планы и процедуры для тех операций, которые связаны с выявленными значительными рисками, включая политику менеджмента устойчивости, оценку риска, требования к цепи поставок, цели и целевые показатели, чтобы обеспечить их выполнение в указанных условиях, сводящих риск к минимуму, посредством:

a) разработки, внедрения и поддержания в рабочем состоянии процедур, относящихся к идентифицированным опасностям, угрозам и рискам в деятельности, функциях, товарах и услугах организации, обмене информацией о применимых процедурах и требованиях к цепи поставок и подрядчикам;

b) разработки, внедрения и поддержания в рабочем состоянии документированных процедур для управления ситуацией, при которой их отсутствие может привести к отклонению от политики менеджмента устойчивости, целей и целевых показателей;

c) проведения оценки любого риска на фазе предконтроля и фазе постконтроля деятельности в цепи поставок, внедрения и поддержания в рабочем состоянии документированной процедуры для минимизации вероятности и снижения тяжести последствий разрушительного инцидента;

d) разработки и поддержания в рабочем состоянии требований к товарам и услугам, которые оказывают воздействие на устойчивость, доведение информации до поставщиков;

e) обоснования критериев деятельности организации в документированных процедурах.

Эти процедуры должны включать средства управления для проектирования, установки, эксплуатации, восстановления элементов оборудования, связанных с устойчивостью, логистических потоков, контрольно-измерительных приборов и т. д., когда это применимо. В тех случаях, когда существующие договоренности пересматриваются и вводятся новые договоренности, которые могут воздействовать на устойчивость управления деятельностью/операциями и видами деятельности, организация должна рассмотреть сопутствующие риски до реализации новых договоренностей.

Новые или пересмотренные соглашения должны включать:

a) актуализированную организационную структуру, обязанности или ответственность;

b) пересмотренную политику устойчивости, цели, целевые показатели и программы;

c) пересмотренные процессы и процедуры;

d) внедрение новой инфраструктуры, оборудования или технологий, которые могут включать аппаратное или программное обеспечение;

e) включение новых подрядчиков, поставщиков, партнеров по цепи поставок или персонала, если это применимо.

Процедуры управления деятельностью/операциями должны:

a) обратить внимание на надежность, устойчивость, безопасность и здоровье людей, на защиту имущества и окружающей среды, потенциально подверженных разрушительному инциденту;

b) установить владельцев риска, обработки риска и мероприятий по управлению (как внутренних, так и внешних);

c) обеспечить, чтобы сигналы запроса были учтены при планировании мощностей;

d) гарантировать наличие процессов для проверки ответов поставщиков (например, проверить время восстановления предприятия / процесса / продукта);

e) быть соразмерными целям устойчивости цепи поставок и соответствовать их назначению;

f) обеспечить обратную связь, чтобы узнать, меняются ли стратегии управления рисками в рамках обычной разработки, или изменений процесса, или решений поставщика.

A.5.7 Предупреждение инцидента, готовность и реагирование

A.5.7.1 Общие положения

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры управления разрушительными инцидентами, которые могут оказать воздействие на организацию, ее деятельность, функции, услуги, цепь поставок, заинтересованные стороны и среду организации. Процедуры должны содержать документированную информацию, как организация будет предотвращать, защищать, готовиться, снижать, реагировать и восстанавливаться после разрушительных инцидентов. Организация должна подготовиться к фактическим разрушительным инцидентам и реагировать на них, чтобы предотвратить инцидент, минимизировать вероятность его возникновения или смягчить связанные с ним неблагоприятные последствия.

При разработке, внедрении и поддержании в рабочем состоянии процедуры для предотвращения, подготовки и реагирования на разрушительный инцидент организация оперативно должна рассмотреть каждое из следующих действий:

a) сохранение безопасности жизнедеятельности;

b) защита активов;

c) предотвращение дальнейшей эскалации разрушительного инцидента;

d) сокращение продолжительности нарушения/срыва в работе/операциях;

e) восстановление критической непрерывности работы;

f) восстановление нормальной деятельности/операций, включая оценку улучшений;

g) защита имиджа и репутации, включая освещение в СМИ и отношения с заинтересованными сторонами.

Организация должна периодически анализировать и, при необходимости, пересматривать свои процедуры по предупреждению инцидента, готовности, реагированию и восстановлению. В частности, после учений или возникновения аварий или инцидентов, которые могут перерасти в чрезвычайную ситуацию, кризис или бедствие.

Организация должна обеспечить, чтобы любое(ые) лицо(а), выполняющее(ие) мероприятия по предупреждению инцидента, защите, готовности и минимизации последствий, а также мероприятия реагирования и восстановления от своего имени, было(и) компетентным(и) на основе соответствующего образования, обучения и/или опыта. Соответствующие записи должны быть сохранены.

Организация должна документировать эту информацию и обновлять ее через регулярные промежутки времени или по мере изменения.

A.5.7.2 Предупреждение инцидента, готовность и структура реагирования

Организация должна разработать, задокументировать и внедрить процедуры и структуру управления для предотвращения, подготовки, смягчения и реагирования на разрушительное событие с использованием персонала, обладающего необходимыми полномочиями, опытом и компетенцией.

Структура предупреждения, готовности и реагирования для персонала должна предусматривать:

a) подтверждение характера и масштабов разрушительного события или потенциального воздействия, которое событие может оказать на организацию, ее цепь поставок, заинтересованные стороны;

b) инициирование соответствующих проактивных и реактивных мероприятий;

c) наличие планов, процессов и процедур для активации, эксплуатации, координации и обмена информацией, предупреждения, готовности и ответных мер;

d) наличие ресурсов, доступных для реализации планов, процессов и процедур для управления разрушительным событием или работой для минимизации воздействия до того, как оно возникает;

e) обмен информацией в цепи поставок с партнерами, заинтересованными сторонами и местными органами власти, а также со средствами массовой информации.

А.5.7.3 Предупреждение инцидента, защита и минимизация последствий

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры для предотвращения и защиты от разрушительного события, минимизации его последствий и продолжения своей деятельности на основе целей устойчивости, разработанных в процессе оценки риска.

Цели устойчивости разрабатываются посредством процесса оценки риска. Процедуры должны основываться на иерархии мероприятий по управлению, расположенных в приоритетном порядке, определенном на основе вероятности возникновения кризисной ситуации. Процедуры следует разрабатывать для:

a) недопущения риска путем полного устранения воздействия риска;

b) снижения риска путем изменения видов деятельности, процессов, оборудования или материалов;

c) изолирования или удаления активов от риска;

d) работы технических средств контроля для обнаружения, сдерживания и задержки источника потенциальной опасности или угрозы;

e) административного контроля, который включает методы работы или процедуры, которые снижают риск;

f) защиты активов, если риск не может быть устранен или уменьшен.

А.5.7.4 Реагирование на инцидент

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры для управления разрушительным событием и продолжения деятельности, основываясь на целях восстановления, разработанных в процессе оценки риска. Организация должна документировать процедуры, включая механизм цепи поставок для обеспечения непрерывности деятельности и управления разрушительным событием.

Процедура(ы) должна(ы):

a) содержать конкретную информацию о первичных шагах, которые следует предпринять во время нарушения/срыва;

b) гибко реагировать на непредвиденные инциденты и изменение внутренних и внешних условий;

c) быть сосредоточена на воздействии различных опасностей и угроз, которые могут потенциально нарушать работу/операции, а не на конкретных событиях;

d) быть разработана на основе обоснованных предположений и анализа взаимозависимостей;

e) быть эффективна в минимизации негативных воздействий посредством реализации соответствующих планов минимизации последствий;

f) рассматривать управление процессом преобразования после инцидента, которое способствует возобновлению и восстановлению работы/операций.

Организация должна разработать документированные процедуры, в которых подробно описывается, как организация будет управлять разрушительным событием и как она будет восстанавливать или поддерживать свою деятельность на заранее определенном уровне, основываясь на утвержденных руководством целях восстановления.

Каждый план должен определять:

a) цель и область применения;

b) цели и критерии успеха;

c) порядок реализации процедуры с распределением ролей, обязанностей и полномочий;

d) требования и процедуры по обмену информацией;

e) внутренние и внешние взаимозависимости и взаимодействия;

f) потребности в ресурсах;

g) информационные потоки и процессы документирования.

Организация должна периодически тестировать/проверять, анализировать и, при необходимости, пересматривать планы обеспечения непрерывности и восстановления. В частности, это следует проводить после возникновения разрушительного события и связанного с ним анализа после события.

А.6 Контроль и корректирующие действия

А.6.1 Общие положения

Организация должна анализировать планы менеджмента устойчивости, процедуры и возможности посредством периодической оценки, тестирования/испытания, отчетов об инцидентах, извлеченных уроках, эффективности оценки и учений. Значительные изменения в этих факторах должны быть немедленно отражены в процедуре. Организация должна вести запись результатов периодических оценок.

А.6.2 Мониторинг и измерения

Организация должна разработать, внедрить и поддерживать в рабочем состоянии показатели результативности (KPI) и процедуры мониторинга и измерений для регулярного мониторинга и измерения тех характеристик своей деятельности, которые оказывают существенное воздействие на ее эффективность, включая партнерство и отношения в рамках цепи поставок.

Процедура(ы) должна(ы) включать документирование информации по мониторингу результатов деятельности (KPI), применимого оперативного контроля и соответствия целям и целевым показателям менеджмента устойчивости организации.

Организация должна оценивать и документировать результаты деятельности систем, которые защищают ее активы, также системы обмена информацией и информационные системы.

А.6.3 Оценка соблюдения и результатов деятельности системы

А.6.3.1 Оценка соблюдения

В соответствии со своим обязательством соблюдения организация должна установить, внедрить и поддерживать процедуру(ы) периодической оценки соответствия применимым нормативно-законодательным требованиям.

Организация должна оценить соответствие другим требованиям, которые относятся к ней, включая лучшие отраслевые практики. Организация может пожелать объединить эту оценку с оценкой соблюдения законодательства, упомянутой выше, или разработать отдельную процедуру.

Организация должна вести записи результатов периодических оценок.

А.6.3.2 Учения и тестирование/испытание

Организация должна испытывать и оценивать уместность и эффективность политики менеджмента устойчивости, программ, процессов и процедур, включая партнерство и отношения в рамках цепи поставок.

Организация должна провести валидацию политики менеджмента устойчивости с использованием учений и тестирований/испытаний, которые:

a) соответствуют области распространения системы менеджмента устойчивости и целям организации;

b) основаны на оценке риска и хорошо спланированы, с четко определенными целями и задачами;

c) минимизируют риск нарушений/срывов работы/операций и возможность возникновения риска для деятельности и активов;

d) завершаются по итогам оформлением официального отчета, содержащего результаты, рекомендации и меры для своевременного внедрения улучшений;

e) рассматриваются в контексте содействия постоянному улучшению;

f) проводятся с запланированными интервалами, определяемыми руководством организации, и, время от времени, без предварительного уведомления, а также в тех случаях, когда происходят существенные изменения в организации и среде, в которой она работает.

А.6.4 Несоответствия, корректирующие и предупреждающие действия

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры для устранения фактических и потенциальных несоответствий для принятия корректирующих и предупреждающих действий. Процедура(ы) должна(ы) определять требования для:

a) выявления и исправления несоответствия(ий) и принятия мер для смягчения их воздействия;

b) расследования несоответствий, определения их причин(ы), принятия мер во избежание их повторения;

c) оценки необходимости действий для предотвращения несоответствий и реализации соответствующих действий, направленных на предотвращение их возникновения;

d) выполнения корректирующих и предупреждающих действий;

e) записи результатов, предпринятых корректирующих и предупреждающих действий;

f) проверки результативности предпринятых корректирующих и предупреждающих действий.

Предпринимаемые действия должны соответствовать воздействию потенциальных проблем и проводиться в ускоренном порядке.

Организация должна идентифицировать измененные риски и определить требования к предупреждающим действиям, акцентируя внимание на значительно изменившихся рисках.

Приоритет предупреждающих действий следует определять на основании результатов оценки риска.

Организация должна вносить любые необходимые изменения в документацию политики менеджмента устойчивости.

А.6.5 Управление записями

Организация должна разработать и поддерживать в рабочем состоянии записи для демонстрации соответствия требованиям политики менеджмента устойчивости и достигнутых результатов.

Организация должна разработать, внедрить и поддерживать в рабочем состоянии процедуры защиты целостности записей, включая доступ, идентификацию, хранение, защиту, поиск и утилизацию записей.

Записи должны быть и оставаться разборчивыми, узнаваемыми и отслеживаемыми.

А.6.6 Внутренний аудит

Организация должна проводить внутренние аудиты политики менеджмента устойчивости через запланированные интервалы времени и на непериодической основе (по решению руководства), чтобы определить, соответствуют ли цели управления, элементы управления, процессы и процедуры политике менеджмента устойчивости. Это необходимо, чтобы определить:

a) соответствие требованиям данного стандарта и применимым нормативно-законодательным требованиям;

b) соответствие требованиям менеджмента рисков организации;

c) эффективное внедрение и поддерживание в рабочем состоянии;

d) ожидаемые результаты.

Программу аудита следует составлять с учетом статуса и важности процессов и областей, подлежащих аудиту, а также результатов предыдущих аудитов. Должны быть установлены критерии аудита, объем, периодичность и методы аудита. Выбор аудиторов и проведение аудитов должны обеспечивать объективность и беспристрастность процесса аудита. Аудиторы не должны проводить аудит своей собственной работы.

Ответственность и требования к планированию и проведению аудитов, а также к отчетности о результатах и ведению записей (см. А.6.5) должны быть определены в документированной процедуре.

Руководство, ответственное за проверяемую область, должно гарантировать, что действия для устранения обнаруженных несоответствий и их причин предпринимаются без неоправданной задержки. Последующие действия должны включать верификацию предпринятых действий и отчет о результатах проверки.

А.7 Анализ со стороны руководства

А.7.1 Общие требования

Руководство должно проводить анализ системы менеджмента безопасности через запланированные интервалы времени, чтобы обеспечить продолжающуюся пригодность, адекватность и результативность. Этот анализ должен включать оценку возможностей для улучшения, оценку необходимости изменений в системе менеджмента, включая политику и цели системы устойчивости. Результаты анализа должны быть четко задокументированы, должны вестись записи (см. А.6.5).

А.7.2 Входные данные для анализа со стороны руководства

Входные данные для анализа со стороны руководства должны включать:

a) результаты анализа отчетов аудитов и анализа политики менеджмента устойчивости;

b) обратную связь от заинтересованных сторон;

c) технологии, продукты или процедуры, которые можно использовать в организации для повышения результатов деятельности и эффективности системы менеджмента устойчивости;

d) статус корректирующих и предупреждающих действий;

e) результаты учений и тестирования/испытания;

f) уязвимость к угрозам, которые были неадекватно оценены в предыдущей оценке риска;

g) результаты измерений эффективности;

h) действия по результатам предыдущих анализов со стороны руководства;

i) любые изменения, которые могут повлиять на политику менеджмента устойчивости;

j) адекватность политики и целей;

k) рекомендации по улучшению.

А.7.3 Выходные данные анализа со стороны руководства

Выходные данные анализа со стороны руководства должны включать любые решения и действия, связанные:

a) с улучшением результативности политики менеджмента устойчивости;

b) с актуализацией оценки риска, готовности к инцидентам и планом реагирования;

c) с модификацией, при необходимости, процедур и элементов управления, которые влияют на риск, для реагирования на внутренние или внешние события, которые могут повлиять на политику менеджмента устойчивости, включая изменения в:

1) требованиях организации и деятельности;

2) требованиях по безопасности и снижению риска;

3) условиях функционирования процессов, влияющих на существующие требования к работе/деятельности;

4) нормативно-законодательных требованиях;

5) контрактных обязательствах;

6) уровне риска и критериях допустимого риска;

d) с потребностями в ресурсах;

e) с улучшением измерения эффективности управления.

А.7.4 Поддержание в рабочем состоянии

Высшее руководство должно установить определенную документированную программу поддержания системы менеджмента в рабочем состоянии, чтобы гарантировать, что любые внутренние или внешние изменения, которые воздействуют на организацию, рассматриваются в контексте политики менеджмента устойчивости. Должны быть идентифицированы любые новые критические действия, которые необходимо включить в программу поддержания системы менеджмента устойчивости в рабочем состоянии.

А.7.5 Постоянное улучшение

Организация должна постоянно повышать результативность системы менеджмента посредством использования политики менеджмента устойчивости, целей, результатов аудита, анализа наблюдаемых событий, корректирующих и предупреждающих действий и анализа со стороны руководства.

Приложение В
(справочное)

Информационное руководство по использованию настоящего стандарта

В.1 Введение

Примечание — Дополнительный текст, приведенный в этом приложении, носит исключительно информационный характер и предназначен для понимания определенных разделов настоящего стандарта. Хотя эта информация касается и согласуется с требованиями указанных разделов настоящего стандарта, она не предназначена для добавления, исключения или каким-либо образом изменения этих требований.

Стихийные бедствия, экологические, технологические аварии, техногенные кризисы исторически демонстрировали, что имеют место разрушительные инциденты, оказывающие воздействие, как на государственный, так и на частный секторы. Задача учета данных видов воздействия выходит за рамки большинства ранее развернутых планов реагирования или действий по ликвидации последствий бедствий. В настоящее время организации должны участвовать во всеобъемлющем и систематическом процессе предупреждения, защиты, подготовки и готовности, минимизации последствий, реагирования, непрерывности и восстановления. Уже недостаточно просто составить план реагирования, который предполагает сценарии бедствий или чрезвычайных ситуаций. Современные угрозы требуют создания непрерывного, динамичного и интерактивного процесса, который служит для обеспечения непрерывности основной деятельности организации до, во время и после возникновения крупного кризиса.

Настоящий стандарт предоставляет организациям всех размеров политику менеджмента устойчивости, необходимую для достижения и демонстрации адаптивного и упреждающего снижения риска и повышения эффективности организационной устойчивости, связанной с их физическими возможностями, услугами, деятельностью, товарами, цепью поставок и непрерывностью функционирования организации.

Они делают это в контексте:

a) повышения безопасности в отношении рисков и угроз;

b) более строгого выполнения нормативно-законодательных требований;

c) повышения конкурентоспособности бизнеса;

d) увеличения взаимозависимости в обществе (на организационном, функциональном или юрисдикционном уровне);

e) повышения осведомленности о необходимости адекватного реагирования на чрезвычайные ситуации и планирования восстановления;

f) учета проблем заинтересованных и затронутых сторон;

g) потребности в обеспечении непрерывности и устойчивости деятельности.

Инцидент с разрушительными последствиями, который должным образом не управляется, может быстро перерасти в чрезвычайную ситуацию, кризис или даже бедствие. Подготовка к инциденту до его возникновения может свести к минимуму вероятность его возникновения и воздействие. Неуправляемый разрушительный инцидент может испортить имидж, репутацию или бренд организации в дополнение к значительному физическому или экологическому ущербу, травмам или гибели людей.

Адаптивное и проактивное планирование и подготовка к потенциальным инцидентам и срывам уменьшат вероятность возникновения, воздействие и продолжительность срыва. Целостный процесс управления может помочь избежать и свести к минимуму приостановку работы критически важных служб и операций, что позволит максимально быстро вернуться к обычной работе служб и стандартным операциям.

Настоящий стандарт содержит руководство, или рекомендации, для любой организации по выявлению и разработке наилучшей практики для содействия и стимулирования действий:

a) по снижению риска по всей цепи поставок;

b) по обеспечению высшего руководства руководством, видением и лидерством в отношении стратегий защиты активов и обеспечения устойчивости организации;

c) по идентификации и оценке активов, услуг и функций для определения видов деятельности, которые имеют решающее значение для краткосрочного и долгосрочного успеха организации;

d) по выявлению потенциальных опасностей и угроз и оценке риска от их воздействия;

e) по предотвращению и/или минимизации воздействия широкого спектра опасностей и угроз, включая стихийные бедствия, технологические и экологические катастрофы, а также техногенные катастрофы, терроризм и преступность;

f) по пониманию ролей и ответственности, необходимых для защиты активов и дальнейшей устойчивости;

g) по необходимости управления и готовности к инцидентам/чрезвычайным ситуациям и обеспечения ресурсами для реагирования;

h) по разработке стратегических альянсов и соглашений о взаимопомощи;

i) по разработке и ведению планов готовности к инцидентам /чрезвычайным ситуациям, плана реагирования и соответствующих оперативных процедур;

j) по разработке и проведению тренингов и учений для поддержания планов реагирования и оперативных процедур и оценки готовности организации к предупреждению, защите от инцидента/чрезвычайной ситуации;

k) по разработке и проведению обучения по планам реагирования и оперативным процедурам для обеспечения готовности организации к предупреждению, защите от инцидента/чрезвычайной ситуации;

l) по обеспечению того, чтобы соответствующие сотрудники, потребители, поставщики и другие заинтересованные стороны знали о предупреждении, готовности к инциденту/чрезвычайной ситуации и мерах реагирования и (при необходимости) доверяли их применению;

m) по разработке процедур внутреннего и внешнего обмена информацией, включая реагирование на запросы о получении информации от средств массовой информации;

n) по установлению измеримых показателей для измерения и демонстрации успеха;

o) по документированию ключевых ресурсов, инфраструктуры, задач и обязанностей, необходимых для поддержания важнейших производственных функций;

p) по созданию процессов, обеспечивающих актуальность информации и ее соответствие меняющимся рискам и изменениям в среде организации.

Для организации это актуально — защитить свои физические, виртуальные и человеческие активы. Успех ее системы менеджмента зависит от приверженности руководителей всех уровней управления и подразделений в организации, особенно высшего руководства организации. Лица, принимающие решения, должны быть готовы составить бюджет и обеспечить необходимые ресурсы для функционирования системы.

Необходимо создать соответствующую административную структуру для эффективной борьбы с рисками, для предупреждения, минимизации последствий и управления разрушительными событиями.

Это обеспечит понимание всеми заинтересованными сторонами того, кто принимает решения, как эти решения выполняются, каковы обязанности и ответственность участников. Персонал, участвующий в управлении инцидентами, должен назначаться для выполнения этих ролей в рамках своих обычных служебных обязанностей, и не следует ожидать, что он будет выполнять их на добровольной основе. Независимо от организации ее руководство имеет обязательства перед заинтересованными сторонами и обязано планировать выживание организации.

B.2 Общее руководство

Система менеджмента — это динамичный и многогранный процесс, элементы которого взаимодействуют как структурированный набор функциональных единиц. Он обеспечивает структуру, основанную на предпосылке, что составные части системы могут быть лучше поняты при рассмотрении в контексте отношений друг с другом и с другими системами, а не изолированно. Единственный способ полностью понять и реализовать элементы системы менеджмента — это понять каждую часть по отношению к целому. Поэтому следует отметить, что система менеджмента представляет собой не простую совокупность элементов, а скорее сложный набор взаимосвязанных частей, взаимодействующих друг с другом.

Это приводит к повторяющемуся процессу, в котором понимание среды организации, политика, оценка риска, внедрение и функционирование, оценка и анализ со стороны руководства — это не просто логичная последовательность шагов, а скорее сеть взаимодействующих функций.

Системный подход к менеджменту включает в себя:

- понимание среды и факторов среды, в которой работает система;
- определение основных элементов системы, а также границ системы;
- понимание обязанностей или функции каждого элемента в системе;
- понимание динамического взаимодействия между элементами системы.

Системный подход обеспечивает разработку целостных стратегий и политики. Это обеспечивает надежную аналитическую основу для разработки стратегий и политик, которые должны быть реализованы в сложной и изменяющейся среде, в которой работает организация.

Создание основы для оценки риска и эффективности стратегий и политик до и во время реализации обеспечивает обратную связь для принятия решений на протяжении всего процесса.

Реализация политики менеджмента устойчивости, регламентированной настоящим стандартом, направлена на повышение безопасности, готовности, улучшение реагирования, обеспечение непрерывности и восстановление работоспособности.

Таким образом, настоящий стандарт основан на предпосылке, что организация будет периодически анализировать и оценивать свою систему менеджмента и политику устойчивости для определения возможностей для улучшения и их реализации.

Скорость, степень и сроки процесса постоянного улучшения определяются организацией в свете экономических и других обстоятельств.

Усовершенствования в системе менеджмента призваны привести к дальнейшим улучшениям безопасности, готовности, реагирования, непрерывности и эффективности восстановления, а также устойчивости организации.

Настоящий стандарт требует от организации:

a) установить соответствующую политику менеджмента устойчивости;

b) определить опасности и угрозы, связанные с прошлой, существующей или планируемой деятельностью, функциями, продуктами и услугами организации, чтобы определить значимость риска;

c) определить применимые нормативно-законодательные требования и другие требования, относящиеся к организации;

d) определить приоритеты и установить соответствующие цели и целевые показатели менеджмента устойчивости;

e) создать структуру и программу(ы) для реализации политики и достижения целей и целевых показателей;

f) содействовать планированию, контролю, мониторингу, предупреждающим и корректирующим действиям, аудиту. Анализировать действия, чтобы гарантировать, что политика соблюдается и система менеджмента устойчивости продолжает соответствовать требованиям;

g) адаптироваться к меняющимся обстоятельствам.

B.3 Понимание организации и ее среды

Чтобы организация спроектировала и внедрила систему менеджмента и политику устойчивости для управления своими рисками и цепью поставок, она должна сначала оценить и понять внутренние и внешние факторы среды, в которой она функционирует. При разработке политики устойчивости организация должна учитывать внутренние и внешние параметры среды, относящиеся к ее цепи поставок (см. рисунок B.1). Среда организации определит необходимую область распространения и критерии для управления рисками организации и ее цепи поставок, а также послужит основой для постановки целей оценки риска, самого риска и критериев восстановления, а также параметров для оценки риска и процессов обработки риска.

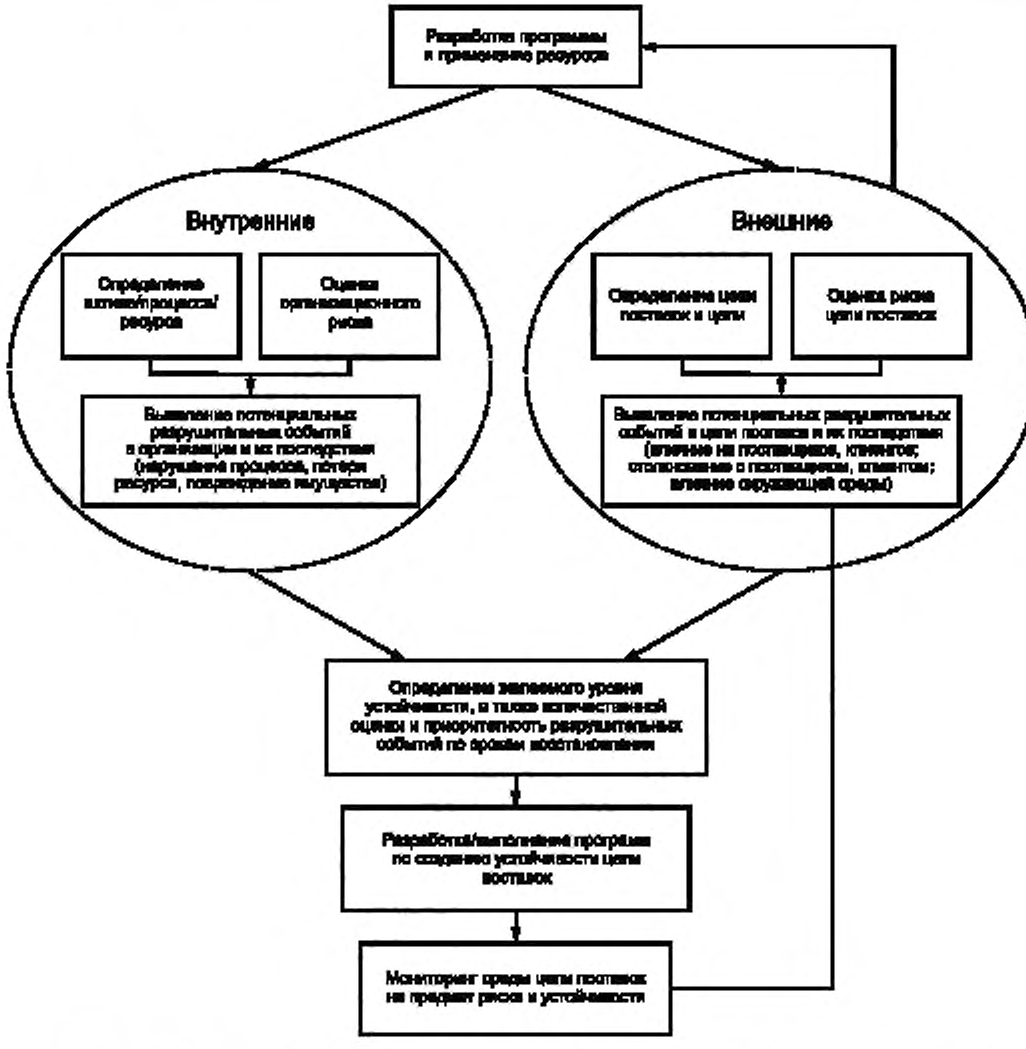

Рисунок B.1 — Понимание факторов среды организации для управления устойчивостью цепи поставок

B.4 Область применения политики менеджмента устойчивости

Организация имеет свободу и гибкость в определении области применения и может принять решение о внедрении стандарта в отношении всей организации, конкретных операционных подразделений организации или компонентов одного/нескольких комплексных продуктов/услуг в потоках своей цепи поставок. Организация должна определить и задокументировать область применения своей политики менеджмента устойчивости. Область применения предназначена для уточнения границ организации и узлов цепи поставок, к которым будет применяться политика управления устойчивостью, особенно если организация является частью более крупной организации. После определения области применения все виды деятельности, продукты и услуги организации, входящие в эту область, должны быть включены в политику менеджмента устойчивости. При определении области применения доверие к политике менеджмента устойчивости будет зависеть от выбора организационных границ. Если часть организации исключена из сферы действия ее политики менеджмента устойчивости, такое исключение должно быть обосновано.

Если стандарт внедряется для конкретного операционного подразделения, политики и процедуры, разработанные другими подразделениями организации, могут использоваться для удовлетворения требований настоящего стандарта при условии, что они применимы к конкретному операционному подразделению, в котором система внедряется.

Управление устойчивостью включает в себя проблемы и действия до, во время и после разрушительного инцидента. Следовательно, настоящий стандарт охватывает предупреждение, предотвращение, сдерживание, готовность, минимизацию последствий, реагирование, обеспечение непрерывности и восстановление. Среда риска, а также реалии деятельности организации отражают разные стратегические весовые коэффициенты на каждом из этих компонентов, однако ни один компонент не должен иметь нулевой вес. Заявление о применимости должно разъяснять расстановку стратегических весовых коэффициентов управления безопасностью, управления готовностью, управления чрезвычайными ситуациями, управления бедствиями, управления кризисами и управления непрерывностью деятельности в разработке системы менеджмента, основанной на оценке риска (см. А.4.1).

B.5 Обеспечение ресурсами политики менеджмента устойчивости

Должны быть определены ресурсы, необходимые для реализации политики менеджмента устойчивости. К ним относятся человеческие ресурсы и специальные навыки, оборудование, внутренняя инфраструктура, технологии, информация, знания и финансовые ресурсы. Высшее руководство должно обеспечивать доступность ресурсов, необходимых для создания, внедрения, контроля и поддержания системы менеджмента устойчивости.

B.6 Политика

Политика менеджмента устойчивости является движущей силой для внедрения и совершенствования системы менеджмента устойчивости для поддержания непрерывности и устойчивости деятельности организации. Следовательно, политика должна отражать ответственность высшего руководства:

a) по соблюдению всех применимых нормативно-законодательных и иных требований;

b) по предупреждению, готовности, минимизации последствий разрушительных инцидентов;

c) по постоянному улучшению.

Политика менеджмента устойчивости является основой, на которой организация устанавливает свои цели и целевые показатели. Политику менеджмента устойчивости следует сформулировать понятным языком, доступным для понимания внутренним и внешним заинтересованным сторонам (особенно партнерам организации по цепи поставок), периодически анализировать и пересматривать с учетом меняющихся условий и информации. Область применения системы менеджмента устойчивости должна быть четко определена и отражать уникальный характер, масштаб и воздействия риска на деятельность, функции, товары и услуги организации.

Политика менеджмента устойчивости должна быть доведена до сведения всех лиц, которые работают в организации (или от ее имени), включая цепь поставок, подрядчиков, работающих с использованием средств организации. Информирование контрагентов может осуществляться в формах, альтернативных самому заявлению о политике, таких как правила, директивы и процедуры, и поэтому может включать только соответствующие разделы политики. Политика менеджмента устойчивости организации должна быть разработана и документирована высшим руководством в контексте политики менеджмента устойчивости любого более широкого корпоративного органа, частью которого она является, и с одобрения этого органа.

Важно, чтобы высшее руководство организации выделяло необходимые ресурсы и отвечало за создание, сопровождение, испытание и внедрение комплексной системы менеджмента устойчивости. Это обеспечит понимание руководством и персоналом на всех уровнях внутри организации того, что система менеджмента устойчивости является важнейшим приоритетом высшего руководства. Не менее важно, чтобы высшее руководство использовало подход «сверху вниз» к системе менеджмента устойчивости, чтобы руководство на всех уровнях понимало ответственность за эффективное и результативное ведение плана как приоритетной части общего управления организацией.

Для обеспечения широкого принятия системы менеджмента устойчивости следует создать группу планирования менеджмента устойчивости и группы поддержки, включающие старших руководителей всех основных организационных структур.

В.7 Планирование

В.7.1 Оценка риска и мониторинг

Процесс оценки риска предоставляет инструментарий лицам, принимающим решения, для лучшего понимания рисков, которые могут повлиять на достижение целей в текущей работе, в целом в деятельности организации, а также в цепи поставок. Процесс оценки риска предназначен для создания систематической деятельности организации по выявлению критических активов, опасностей, угроз, уязвимостей, рисков и воздействий для определения тех аспектов, которые являются значимыми для организации и ее цепи поставок. Оценка риска обеспечивает основу для оценки адекватности и эффективности существующих средств контроля, а также решений о наиболее подходящих подходах, которые будут использоваться при управлении рисками. При оценке риска идентифицируются те риски, которые следует рассматривать в качестве приоритетов в политике менеджмента устойчивости организации. Оценка риска обеспечивает основу для постановки целей, целевых показателей и программ в рамках системы менеджмента безопасности, а также для измерения того, насколько результативно работает система менеджмента устойчивости.

Организация должна применять ИСО 31000:2009 (рисунок В.2).

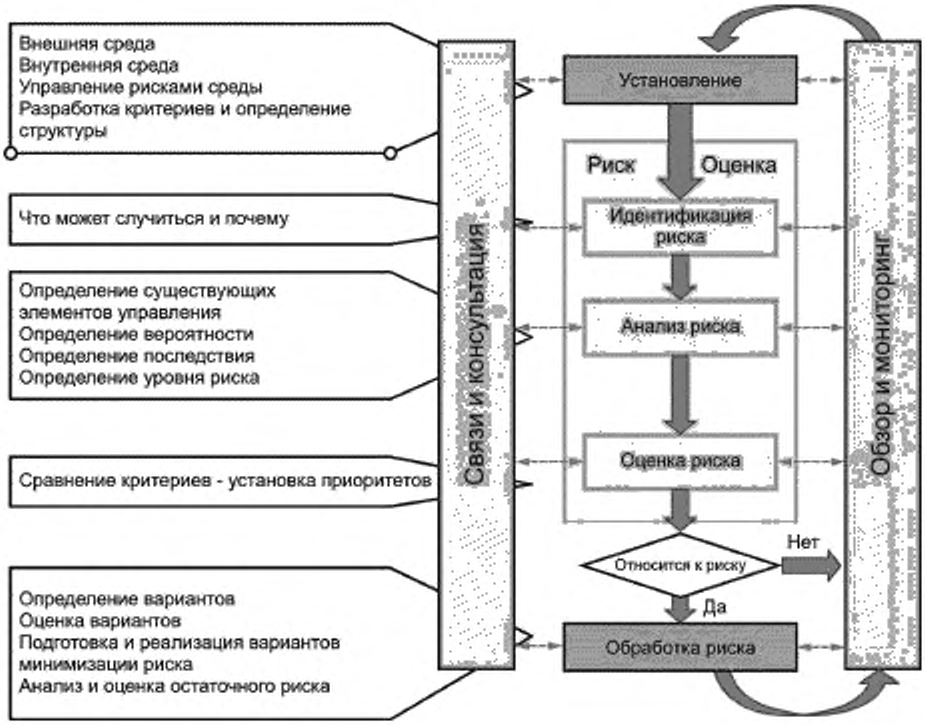

Рисунок В.2 — Процесс управления риском

Понимание среды организации позволяет определить, что именно необходимо защищать, определяет систему ранжирования элементов оценки риска для обеспечения согласованности.

Внешняя среда включает в себя:

- культурную, политическую, правовую, нормативную, финансовую, природную, рыночную среду (на международном, национальном и местном уровнях);
- ключевые движущие силы и тенденции, оказывающие влияние на цели;
- восприятие и ценности внешних заинтересованных сторон.

Внутренняя среда включает в себя:

- возможности, с точки зрения наличия ресурсов и знаний (люди, процессы, системы, технологии, время, финансовые ресурсы);
- информацию: системы, потоки и процессы принятия решений;
- заинтересованные стороны;
- цели и стратегии организации;

- восприятие, ценности и культуру;
- политику и процессы;
- стандарты, эталонные модели, структуры (управление, обязанности и ответственность);
- согласованные процессы оценки риска, цели, критерии риска, уязвимости, опасности, угрозы, вероятность возникновения и тяжесть последствий, программы оценки рисков и сроки.

В процессе определения внутренней и внешней среды организация должна всесторонне идентифицировать все значимые активы организации. Это включает в себя выявление относительной важности различных видов активов для жизнеспособности и успеха организации. Активы должны включать в себя людей, имущество, информацию, процессы, виды деятельности и нематериальные активы (например, долю на рынке или положение, репутацию, доверие и т. д.). Имущество может включать в себя существующие конструкции и/или оборудование, имеющие критическое значение для деятельности организации. Организации могут выбирать категории видов деятельности, товаров и услуг для определения их критичности, риска и воздействия. Процесс оценки проводится по внутренним и внешним факторам среды организации.

Оценка риска — это общий процесс идентификации риска, анализа риска и оценки риска:

a) Идентификация риска: процесс обнаружения, распознавания и регистрации рисков. Он включает оценку угроз, критичности и уязвимости в качестве входных данных в процессе идентификации. В процессе рассматриваются причины и источники риска, а также события, ситуации и обстоятельства, которые могут повлиять на воздействие риска на организацию и ее цепь поставок.

Идентификация вероятных угроз/опасностей включает в себя проактивный сбор информации о потенциальных источниках вреда. Угрозы/опасности могут включать, помимо прочего, опасных лиц, финансовые факторы, влияния конкурентов или поставщиков, деловую активность или другие внутренние или внешние ситуации для организации. Оценка уязвимости выявляет те слабые стороны, которые существуют в физической, процедурной и оперативной деятельности. Оценка уязвимости позволяет улучшить возможности для снижения реализации угроз.

b) Анализ риска — это процесс обработки и понимания риска. Он обеспечивает основу для принятия решения о том, какой риск следует обрабатывать и какой наиболее подходящий метод обработки следует использовать. Он рассматривает причины и источники риска, их последствия и вероятность того, что инцидент и связанные с ним последствия могут произойти.

Организация должна определить, какие последствия или воздействие инцидента на объект или средства могут представлять угрозу. Последствия могут быть классифицированы на основании смерти или угрозы жизни человека, финансового или операционного воздействия, прерывания бизнеса, структурного ущерба и ущерба нематериальным активам (репутации, торговой марке, доверию, отраслевому и публичному позиционированию).

Процесс определения последствий также может быть известен как анализ воздействия.

c) Оценка риска — это процесс сравнения оцененных уровней риска с критериями риска, определенными при установлении контекста. Оценка риска определяет значимость уровня и типа риска. Оценка риска использует понимание риска, полученного в анализе риска, для принятия решений о стратегиях, необходимых для контроля риска и его минимизации.

Оценка риска обеспечивает понимание рисков, их причин, последствий, вероятностей их возникновения. Следовательно, организация должна провести комплексную оценку риска в рамках своей системы менеджмента устойчивости с учетом входных и выходных данных (как предполагаемых, так и непреднамеренных), связанных со следующим:

a) действия, продукты и услуги, осуществляемые как в настоящее время, так и в прошлом (внутри организации и в рамках цепи поставок);

b) запланированные или новые разработки, новые или измененные виды деятельности, функции, продукты и услуги;

c) отношения с партнерами и заинтересованными сторонами по цепи поставок;

d) взаимодействие со средой и обществом;

e) критическая инфраструктура.

Оценка риска необходима, чтобы устанавливать цели и целевые показатели времени восстановления. Этот процесс должен учитывать нормальные и ненормальные рабочие условия, условия остановки и запуска, а также разумно предсказуемые разрушительные и чрезвычайные ситуации и отвечать требованиям времени восстановления. Однако следует помнить, что невозможно предвидеть все разрушительные и чрезвычайные ситуации. Поэтому для того, чтобы установить цели времени восстановления, организация должна также учитывать воздействие нарушений на свои критические активы, деятельность и функции, вне зависимости от характера нарушений, с тем чтобы установить цели по срокам восстановления и отреагировать на потребности во времени восстановления внутри и в рамках своей цепи поставок

Существует множество подходов и методик оценки рисков, которые определяют порядок шагов проведения анализа. Независимо от методики у организации должен быть формализованный и документированный процесс идентификации, анализа и оценки риска, который включает в себя идентификацию угроз и опасностей, а также рисков, уязвимости, критичности, вероятности возникновения, тяжести последствий и анализ воздействия.

Оценка риска должна:

a) рассматривать возможные риски (включая их критичность), связанные с деятельностью, функциями, товарами, услугами организации и ее цепью поставок. Также нужно рассматривать потенциал рисков для прямого

или косвенного воздействия на деятельность организации, людей, имущество, активы, возмещение, имидж и репутацию, прибыль, кредитование и /или среду организации;

b) использовать документированную количественную или качественную методику для оценки вероятности возникновения потенциальных рисков и тяжести их воздействия, если они возникнут;

c) основываться на разумных критериях, с фокусировкой внимания на всех потенциальных рисках, которые организация признает в своей деятельности;

d) рассматривать зависимость организации от других организаций в цепи поставок и насколько другие участники цепи зависят от нее, включая критические инфраструктуры и обязательства;

e) рассматривать целостность данных, телекоммуникаций и технологий информационной безопасности;

f) оценивать последствия юридических и других обязательств, которые регулируют деятельность организации;

g) рассматривать риски, связанные с заинтересованными сторонами, подрядчиками, поставщиками и другими вовлеченными сторонами;

h) анализировать информацию о риске и выбирать те риски, которые могут вызвать значительные последствия, и/или те риски, последствия которых трудно определить с точки зрения значимости;

i) анализировать и оценивать уровень устойчивости организации и каждого критического актива к каждой опасности или угрозе;

j) оценивать риск и воздействия, на которые организация может повлиять. Однако при любых обстоятельствах именно организация определяет степень контроля и свои стратегии для принятия риска, избегания, управления, минимизации, определения допустимого риска, переноса и/или обработки риска.

В некоторых местах критическая инфраструктура, общественные активы и культурное наследие могут быть важным элементом среды, в которой работает организация, поэтому их следует учитывать при понимании риска и воздействия на окружающую среду.

Поскольку организация может иметь много рисков, она должна установить и задокументировать критерии и методику для определения тех рисков, которые она сочтет значительными. Не существует единого метода определения значительного риска. Однако используемый метод должен обеспечивать согласованные результаты и включать в себя установление и применение критериев оценки, таких как критерии, относящиеся к критичности каждой организационной деятельности и функции, правовые вопросы и проблемы внутренних и внешних заинтересованных сторон. Организация должна анализировать вероятность возникновения, тяжесть последствий и воздействия нарушений на свои операции и выявлять критические операции, которым уделяется первоочередное внимание для восстановления, чтобы установить целевые показатели времени восстановления.

При оценке воздействий организации должны учитывать:

a) затраты на персонал: физический и психологический вред, который может быть нанесен работникам, потребителям, поставщикам и другим заинтересованным сторонам;

b) финансовые затраты: замена оборудования, имущества, простои, плата за сверхурочную работу, девальвация запасов, потерянные продажи/бизнес, судебные процессы, штрафные санкции и т. д;

c) издержки корпоративного имиджа: репутация на рынке, репутация в обществе, негативная информация в прессе, потеря клиентов и т. д;

d) экономические потери для сообщества, в котором действует организация: косвенные воздействия на региональную экономику, снижение благосостояния населения, потери для налоговой базы местных юрисдикций и т. д;

e) воздействие на окружающую среду: ухудшение качества окружающей среды.

При оценке максимально допустимого времени простоя, приемлемого уровня потерь и приоритетных сроков восстановления цели организации должны основываться на следующем:

a) обязательства по цепи поставок с учетом последствий до и после;

b) как долго процессы могут не функционировать, прежде чем воздействия станут неприемлемыми;

c) как скоро должны быть восстановлены процессы (сначала следует установить кратчайшее допустимое отключение);

d) различные цели времени восстановления в зависимости от времени года (конец года, подача налоговой декларации и т. д.);

e) определение и документирование альтернативных процедур для стратегического альянса, взаимопомощи, режима «ручного управления», уведомления/предупреждения и т. д;

f) оценка стоимости альтернативной процедуры в сравнении с ожиданием восстановления системы.

При разработке информации, относящейся к значительному риску, организации следует учитывать необходимость сохранения информации в исторических целях, а также способы ее использования при разработке и реализации политики менеджмента устойчивости.

Процесс идентификации и оценки риска должен учитывать место осуществления деятельности, стоимость и время проведения анализа, а также наличие надежных данных. В этом процессе может использоваться информация, уже разработанная для бизнес-планирования, регулирования или других целей.

Процесс выявления и оценки рисков не предназначен для изменения или увеличения юридических обязательств организации.

B.7.2 Нормативно-законодательные и иные требования

Организация должна идентифицировать нормативно-законодательные требования, применимые к ее деятельности и функциям. Требования могут включать в себя:

a) национальные и международные законодательные требования;

b) законодательные требования округа/области/района;

c) местные нормативно-законодательные требования.

Примеры других требований, которые могут относиться к организации, включают, если применимо:

a) соглашения с государственными органами;

b) соглашения с покупателями;

c) нормативные руководящие принципы;

d) добровольные принципы или кодексы наилучшей практики;

e) добровольные обязательства по маркировке или управлению товаром;

f) требования торговых ассоциаций;

g) соглашения с общественными группами или неправительственными организациями;

h) публичные обязательства организации или ее головной организации;

i) корпоративные требования.

Определение того, как нормативно-законодательные и другие требования применяют к оценке рисков организации, обычно осуществляется в процессе определения этих требований. Следовательно, не обязательно иметь отдельную или дополнительную процедуру для того, чтобы установить эти требования.

B.7.3 Цели и целевые показатели устойчивости

Цели и целевые показатели должны быть четко сформулированными и измеримыми, где это практически осуществимо. Цель — это общее направление в соответствии с политикой, которую организация ставит перед собой. Целевой показатель — это подробное требование к результатам деятельности, применимое к организации (или ее частям), которое вытекает из целей и которое необходимо установить и выполнить для достижения этих целей. Целевые показатели должны охватывать краткосрочные и долгосрочные аспекты. Программы должны определять стратегические средства для достижения целей и целевых показателей.

Цели, целевые показатели и программы должны базироваться на оценке риска.

При рассмотрении технологических вариантов организация должна учитывать возможность использования наилучших доступных технологий, если это экономически целесообразно, рентабельно и уместно.

Ссылка на финансовые требования организации не подразумевает, что организации обязаны использовать методологии учета затрат, однако организация может принять решение учитывать прямые, косвенные и скрытые издержки.

B.7.4 Стратегические планы и программы для обеспечения устойчивости

Создание и использование одной или нескольких программ имеет важное значение для успешной реализации политики менеджмента устойчивости. В каждой программе должно быть описано, как будут достигнуты цели и целевые показатели организации, включая сроки, необходимые ресурсы и персонал, ответственный за реализацию программ(ы). Данные программы могут подразделяться в соответствии с элементами деятельности/операций организации.

Программа должна включать, где это уместно и практически реализуемо, рассмотрение всех этапов деятельности и функций организации, связанных с обязательствами по цепи поставок, планированием, проектированием, строительством, вводом в эксплуатацию, эксплуатацией, модернизацией, производством, маркетингом, удалением отходов и выводом из эксплуатации. Разработка программы может быть предпринята для текущих и новых видов деятельности, товаров и/или услуг.

Программы предупреждения, готовности и минимизации последствий должны учитывать возможность изолирования людей и имущества, находящихся в опасности/подверженных риску, перемещение, переоснащение и предоставление защитных систем или оборудования, информирование, сбор данных, документов, кибербезопасность, процедуры управления угрозами или опасностями, процедуры обмена информацией, дублирование или запасные варианты необходимого персонала, критических систем, оборудования, информации, операций или материалов, в том числе от партнеров.

Организация должна планировать реагирование на инциденты и восстановление, принимая во внимание основные виды деятельности, цепь поставок и договорные обязательства, потребности сотрудников и сообщества, непрерывность работы и восстановление окружающей среды. Организации имеют разные подходы к управлению кризисами. Независимо от подхода существует три общих и взаимосвязанных шага реагирования руководства, которые требуют упреждающего планирования и реализации в случае разрушительного инцидента:

a) реагирование на чрезвычайную ситуацию. Первоначальное реагирование на разрушительный инцидент обычно включает в себя защиту людей и собственности от непосредственного вреда. Первоначальная реакция руководства может быть первой частью реагирования организации;

b) непрерывность. Процессы, средства управления и ресурсы доступны для обеспечения того, чтобы организация продолжала достигать своих критических целей деятельности/функционирования;

c) восстановление. Процессы, ресурсы и потенциал деятельности организации восстанавливаются для удовлетворения текущих требований к функционированию. Этот этап часто включает в себя внесение значительных организационных улучшений, даже до степени переориентации стратегических или операционных целей.

B.8 Внедрение и функционирование (оперативная реализация)

B.8.1 Ресурсы, обязанности, ответственность и полномочия

Успешная реализация политики менеджмента устойчивости требует приверженности от всех лиц, работающих в организации или от ее имени. Следовательно, обязанности не должны рассматриваться как ограниченные функцией управления рисками, а могут также охватывать другие области организации — оперативное управление или функции персонала, отличные от управления рисками, безопасностью, готовностью, непрерывностью и реагированием.

Принятие обязательств должно начинаться на самом высоком уровне управления. Соответственно, высшее руководство должно разработать политику менеджмента устойчивости организации и обеспечить реализацию данной политики. В рамках этого обязательства высшее руководство должно назначить уполномоченного представителя из состава руководства с определенной ответственностью и полномочиями для реализации политики менеджмента устойчивости. В крупных или сложно устроенных организациях может быть несколько назначенных представителей. На малых или средних предприятиях эти обязанности может выполнять один человек.

Необходимо создать соответствующую административную структуру для эффективного кризисного управления во время разрушительного инцидента. Должны существовать четкие определения для структуры управления, должны быть распределены полномочия для принятия решений и ответственности за реализацию. Организация должна иметь группу кризисного управления, чтобы управлять инцидентом/реагированием на событие.

Группа должна быть в состоянии выполнить следующие функции: управление человеческими ресурсами, информационными технологиями, инфраструктурой, безопасностью, юридическими функциями, обменом информацией, отношениями со СМИ, производством, складированием, другими важными поддерживающими процессами и функциями. Всю эту деятельность следует проводить под четким управлением высшего руководства или его представителя.

Группе кризисного управления должны оказывать поддержку столько групп реагирования, сколько необходимо, с учетом таких факторов, как размер и тип организации, количество сотрудников, местоположение и т. д.

Группа реагирования должна разработать планы реагирования для решения различных аспектов потенциальных кризисов, таких как оценка ущерба, восстановление предприятия, начисление заработной платы, управление человеческими ресурсами, функционирование информационных технологий и административная поддержка. Планы реагирования должны соответствовать общей системе менеджмента устойчивости и быть в нее включены. Отдельные лица должны быть привлечены для участия в группах реагирования с учетом их навыков, уровня приверженности и заинтересованности.

Руководство должно предоставлять ресурсы для обеспечения того, чтобы система менеджмента устойчивости была разработана, внедрена и поддерживалась в рабочем состоянии. Также важно, чтобы ключевые обязанности системы менеджмента устойчивости были четко определены и доведены до сведения всех лиц, работающих в организации или от ее имени.

Обязанности, полномочия и ответственность также должны быть определены, задокументированы и сообщены для координации с внешними заинтересованными сторонами. Данное взаимодействие осуществляется с подрядчиками, партнерами, другими организациями в цепи поставок, государственными органами и финансовыми учреждениями.

B.8.2 Компетентность, подготовка и осведомленность

Организация должна определить, какие знания и навыки необходимы соответствующим лицам, которые несут ответственность и имеют полномочия для выполнения задач, и какой уровень понимания и осведомленности должен быть ими достигнут. Настоящий стандарт в плане компетентности, подготовки и осведомленности персонала регламентирует следующее:

a) понимание важности соответствия политике менеджмента устойчивости, процедурам устойчивости и требованиям общей системы менеджмента;

b) знание значительных опасностей, угроз и рисков, фактических или потенциальных воздействий, которые связаны с их работой, а также знание преимущества улучшения персональной деятельности;

c) знание обязанностей и ответственности, необходимых для достижения соответствия требованиям политики менеджмента устойчивости;

d) знание процедур для предупреждения инцидентов, сдерживания, минимизации последствий, самозащиты, эвакуации, реагирования и восстановления;

e) знание потенциальных последствий отклонений от указанных процедур.

Должны быть разработаны программы осведомленности (и обучения) о воздействии разрушительных инцидентов для внутренних и внешних заинтересованных сторон, партнеров в цепи поставок.

Осведомленность, знания, понимание и компетентность могут быть достигнуты или улучшены посредством обучения, подготовки и проведения учений.

Организация должна требовать, чтобы подрядчики, работающие от ее имени, имели возможность продемонстрировать, что их сотрудники обладают необходимой компетентностью и/или соответствующей подготовкой.

Руководство должно определить уровень компетентности, подготовки и опыта, требуемого для обеспечения необходимой квалификации персонала, особенно того, который исполняет специализированные функции по управлению устойчивостью.

Весь персонал должен быть обучен выполнять свои индивидуальные обязанности в случае инцидента или кризиса. Они также должны быть проинформированы о ключевых компонентах системы менеджмента устойчивости, о планах реагирования, которые непосредственно влияют на них. Такое обучение может включать процедуры проведения мероприятий по предупреждению, защите, минимизации последствий, эвакуации, укрытию на месте, процессам регистрации для учета сотрудников, мероприятиям на альтернативных рабочих местах, а также по обработке запросов от СМИ.

Группы кризисного управления и реагирования должны быть осведомлены об их обязанностях и ответственности, в том числе о взаимодействии с непосредственными участниками инцидента, партнерами по цепи поставок и заинтересованными сторонами.

Чек-листы критических действий и информации, которую нужно собрать, являются ценными инструментами в образовательных процессах и процессах реагирования. Группы должны проходить обучение через регулярные промежутки времени, не реже одного раза в год. Новых членов групп следует обучать, как только они присоединятся к составу группы. Эти группы также должны быть обучены предупреждению инцидентов, которые могут перерасти в кризисы. Рекомендуется, чтобы любые внешние ресурсы, которые могут быть задействованы в реагировании, такие как пожарная охрана, полиция, службы здравоохранения и сторонние поставщики, были знакомы с соответствующими частями планов реагирования.

В.8.3 Информирование и оповещение

Внутренний обмен информацией важен для обеспечения эффективного внедрения системы менеджмента устойчивости. Методы внутреннего обмена информацией могут включать в себя регулярные встречи рабочих групп, информационные бюллетени, доски объявлений и интернет-сайты.

Организация должна определять и устанавливать отношения с учреждениями государственного сектора, организациями и должностными лицами, отвечающими за сбор оперативных данных, оповещение, предупреждение, реагирование и восстановление, связанные с потенциальными нарушениями, выявленными в ходе оценки риска. Должны быть приняты меры внутреннего и внешнего обмена информацией и оповещения для нормальных и ненормальных условий.

Организации должны внедрить процедуру для получения, документирования и реагирования на соответствующие сообщения из своей цепи поставок, от заинтересованных и вовлеченных сторон. Эта процедура может включать в себя диалог с заинтересованными сторонами и рассмотрение их соответствующих проблем. В некоторых случаях ответы на вопросы заинтересованных сторон могут включать соответствующую информацию о риске и воздействиях, связанных с функциями и операциями организации. Эти процедуры также должны касаться необходимого обмена информацией с государственными органами в отношении прогнозирования чрезвычайных ситуаций и других соответствующих вопросов.

Организация может запланировать разделение своих сообщений по содержанию и средствам коммуникации с учетом решений, принятых по соответствующим целевым группам. При рассмотрении внешних сообщений об опасностях, угрозах, рисках, воздействиях и процедурах контроля организация должна учитывать мнения и информационные потребности всех заинтересованных сторон. Если организация решает сообщать внешним заинтересованным сторонам о своих опасностях, угрозах, риске, воздействиях, процедуре управления, то организация должна установить процедуру для выполнения таких действий. Эта процедура может меняться в зависимости от нескольких факторов, включая тип передаваемой информации, целевую группу и индивидуальные обстоятельства организации. Методы внешнего обмена информацией могут включать годовые отчеты, информационные бюллетени, веб-сайты, оповещения и общественные собрания.

Эффективность обмена информацией — один из наиболее важных компонентов в управлении срывами или кризисами. Внутренние и внешние заинтересованные стороны должны быть идентифицированы для передачи сигналов тревоги, оповещений, предупреждений, сообщения о кризисе и информации об ответных действиях организации. Чтобы обеспечить лучший обмен информацией и подходящие сообщения для различных групп, может быть целесообразно сегментировать аудиторию. Таким образом, будут отправляться сообщения, предназначенные специально для конкретной группы.

Предварительное планирование обмена информацией крайне важно. Шаблоны сообщений и заявлений могут быть созданы заранее для тех угроз и рисков, которые были идентифицированы в ходе оценки риска. Процедуры, обеспечивающие возможность распространения сообщений в короткие сроки, также должны быть установлены, особенно при использовании таких ресурсов, как интернет, интернет-сайты и бесплатные горячие линии.

Организация должна назначить единственного основного представителя (с указанием исполняющих обязанности в случае отсутствия), который будет управлять / распространять информацию о кризисах в СМИ и других медиа. Этот человек должен быть обучен работе со СМИ до момента возникновения кризиса. Вся информация должна передаваться из одного источника, чтобы обеспечить согласованность предоставляемых сообщений. Следует подчеркнуть, что персонал должен быть быстро проинформирован о том, куда направлять звонки из СМИ, и только уполномоченные представители компании могут разговаривать со СМИ. В некоторых ситуациях может быть также необходим специально обученный пресс-секретарь предприятия.

В.8.4 Документирование

Уровень детализации документации должен быть достаточным для описания политики менеджмента устойчивости и того, как ее элементы работают вместе, со ссылками для получения более подробной информации о работе отдельных элементов политики менеджмента устойчивости. Эта документация может быть интегрирована

с документацией других систем, внедренных организацией. Документирование не предполагает форму руководства.

Документация политики менеджмента устойчивости может отличаться в различных организациях и зависит:

a) от размера и типа организации и ее деятельности, товаров или услуг;

b) от сложности процессов и их взаимодействия;

c) от компетенции персонала.

Пример документации:

a) заявление о политике, цели и целевые показатели;

b) информация о значительных рисках;

c) процедуры;

d) информация о процессе;

e) организационная структура;

f) внутренние и внешние стандарты;

g) планы реагирования, минимизации последствий, действия в условиях чрезвычайной ситуации и кризиса;

h) записи.

Решение по документированию процедуры должно основываться на следующем:

a) последствия невыполнения, в том числе последствия для человеческих и материальных активов и окружающей среды;

b) необходимость продемонстрировать соответствие нормативно-законодательным требованиям и иным применимым требованиям, которые относятся к организации;

c) необходимость обеспечения того, чтобы деятельность осуществлялась последовательно;

d) наличие преимуществ, которые могут включать следующее:

1) упрощенная реализация при информировании и обучении,

2) более легкое выполнение и пересмотр,

3) меньший риск двусмысленности и отклонений,

4) демонстрация и визуализация;

e) выполнение требований настоящего стандарта.

Документы, изначально созданные для целей, отличных от политики менеджмента устойчивости, могут использоваться как часть этой политики. В случае необходимости на эти документы следует сделать ссылки в политике.

В.8.5 Управление документацией

Цель данного подраздела состоит в том, чтобы обеспечить создание и поддержание документации в рабочем состоянии таким образом, который достаточен для внедрения системы менеджмента устойчивости. Однако основное внимание организации должно быть сосредоточено на эффективном внедрении системы менеджмента устойчивости и безопасности, готовности, реагировании, непрерывности и результатах деятельности по восстановлению, а не на сложной системе управления документацией.

Организация должна обеспечивать целостность документов, гарантируя их защищенность от несанкционированного доступа, надежное резервное копирование, доступность только для уполномоченного персонала и защиту от повреждения, порчи или потери.

В.8.6 Управление деятельностью

Организация должна провести оценку тех операций/видов деятельности, которые связаны с выявленным значительным риском, и убедиться, что они осуществляются таким образом, чтобы контролировать или уменьшать вероятность возникновения связанных с ними неблагоприятных последствий с целью выполнения требований политики устойчивости, целей и целевых показателей.

Оценка должна включать все части операций внутри организации, включая цепь поставок и деятельность по техническому обслуживанию.

Поскольку эта часть политики менеджмента устойчивости содержит указания о том, как учитывать системные требования в повседневных операциях, она требует использования документированных процедур для управления ситуациями, в которых отсутствие документированных процедур может привести к отклонениям от политики, целей и целевых показателей менеджмента устойчивости.

Чтобы минимизировать вероятность возникновения разрушительного инцидента, эти процедуры должны включать элементы управления для проектирования, установки, эксплуатации, восстановления и модификации элементов оборудования, приборов, связанных с риском, и т. д., в зависимости от обстоятельств. В тех случаях, когда существующие договоренности пересматриваются и вводятся новые договоренности, которые могут воздействовать на устойчивость управления видами деятельности/операциями, организация должна рассмотреть минимизацию сопутствующих рисков и угроз до реализации новых договоренностей.

В.8.7 Предупреждение инцидента, готовность и реагирование

В.8.7.1 Общие положения

Каждая организация несет ответственность за разработку мероприятий по предотвращению инцидентов, готовности к ним, минимизации последствий, процедур восстановления, которые соответствуют ее собственным конкретным потребностям. При разработке своих процедур организация должна учитывать следующее:

a) потенциальный разрушительный инцидент, который необходимо идентифицировать, понимать и устранять/избегать/предотвращать. Оценка риска может быть использована для выявления особенностей возможных разрушительных инцидентов, включая любые предвестники и предупреждающие знаки;

b) процесс управления рисками должен быть систематическим и целостным процессом, основанным на формализованной оценке рисков для идентификации, измерения, количественной и качественной оценке рисков для обеспечения оптимального решения;

c) варианты обработки риска могут включать стратегии избегания, предотвращения, распространения, снижения, разделения и принятия. Снижение минимизирует риск или тяжесть последствий. Распространение распределяет активы и/или потенциальную потерю мощности. Разделение предполагает деление риска с другой стороной или сторонами. Принятие — это обоснованное решение пойти на определенный риск.

B.8.7.2 Предупреждение инцидента, готовность и структура реагирования

Организация должна установить процедуру для распознавания появления определенных опасностей, которые требуют конкретного уровня реагирования, чтобы избежать, предотвратить, смягчить или отреагировать на потенциальное нарушение. Сильная программа политик и процедур обнаружения и предоставления будет поддерживать этот процесс.

Некоторые отделы или функции организации имеют уникальное расположение для наблюдения за предвестниками надвигающегося кризиса. Персонал, назначенный в эти отделы или функции, должен пройти соответствующую подготовку. Следует информировать всех сотрудников об ответственности за сообщение о потенциальном кризисе (включая механизм оповещения). Общая численность сотрудников также может быть отличным источником прогнозирующей информации, когда существует документированная структура отчетности и когда внимание уделяется тому, что сообщает сотрудник. Как только будет установлена возможность возникновения разрушительного инцидента, следует немедленно сообщить руководителю, представителю руководства или другому лицу, на которое возложена ответственность за оповещение о кризисе и управление им внутри организации и по всей цепи поставок.

- Должны быть установлены, задокументированы и соблюдаться всеми сотрудниками критерии оповещения с четко документированными сроками и последовательностью уведомлений. Фактическая активация процесса реагирования должна требовать четко определенной квалификации.

- Квалифицированный персонал должен иметь свободный доступ к обновленным конфиденциальным спискам лиц и организаций, с которыми можно связаться, когда будут выполнены определенные условия или параметры потенциального кризиса.

- Оповещения о разрушительной или кризисной ситуации должны быть своевременными и четкими, должны использовать различные процедуры и технологии с учетом того, что используемые устройства имеют свои преимущества и ограничения.

При некоторых видах сбоев/нарушений и кризисов, системы оповещения сами подвергаются воздействию бедствия либо из-за проблем с пропускной способностью, либо из-за повреждения инфраструктуры. Таким образом, важно иметь запасную подсистему, встроенную в систему оповещений, и несколько различных способов связаться с перечисленными лицами и организациями.

Как только возникает нарушение/срыв деятельности, должна быть проведена оценка проблемы (оценочный процесс принятия решения, который определит характер решаемой проблемы) и оценка тяжести последствий (процесс определения серьезности нарушения/срыва, а также оценка возможных расходов при развитии событий). Факторы, которые следует учитывать, включают в себя размер проблемы, тяжесть последствий и возможное воздействие на организацию и ее цепь поставок.

Точка, в которой ситуация объявляется чрезвычайной или кризисной, должна быть четко определена, задокументирована и соответствовать конкретным и контролируемым параметрам. Ответственность за объявление кризиса также должна быть четко определена и распределена. Необходимо назначить первого и второго заместителей ответственного лица.

Деятельность, которая должна осуществляться в чрезвычайной ситуации (или в кризисе), включает (но не ограничивается):

a) оповещение партнеров по цепи поставок и других задействованных сторон;

b) дополнительное уведомление персонала (обзвон);

c) эвакуацию, укрытие или переселение;

d) выполнение протокола безопасности;

e) реагирование или перемещение на альтернативное предприятие;

f) развертывание группы кризисного управления;

g) кадровые назначения и обеспечение доступности соответствующего персонала;

h) активацию договора о чрезвычайной ситуации;

i) изменения в работе/деятельности.

B.8.7.3 Предупреждение инцидента, защита и минимизация последствий

Предупреждение может включать активные шаги по координации со спецслужбами, правоохранительными органами и государственными учреждениями, заключение соглашения об обмене информацией, физическую защиту ключевых активов, контроль доступа, учебные программы готовности и осведомленности, системы оповещения и сигнализации, практики по снижению угрозы.

Организационная культура, оперативные планы и цели управления должны мотивировать людей чувствовать личную ответственность за предупреждение, предотвращение, сдерживание и обнаружение.

Сдерживание и обнаружение могут усложнить осуществление подрывного действия или действия против организации или существенно ограничить его. Стратегии предупреждения, обнаружения и сдерживания могут быть следующими:

a) архитектурные — природные или искусственные барьеры, перепроектированная или перемещенная инфраструктура;

b) оперативные — административные процедуры, удаление опасных материалов, переработанные системы и операции, найм сотрудников службы безопасности, программы информирования сотрудников, контрнадзор и контрразведка как способ избежать проблему, перемещение систем, операций, инфраструктуры и персонала;

c) технологические — альтернативные материалы и процессы коммуникации, призванные обеспечить возможность взаимодействия, информационные сети, обнаружение вторжений, контроль доступа, запись наблюдения, проверка посылок и багажа, системы контроля.

Планирование физической безопасности включает защиту периметра территории, периметра здания, защиту внутреннего пространства, а также защиту активов и их контента. Защита начинается по внешнему периметру:

a) планирование физической безопасности включает функции обнаружения, сдерживания, задержки и реагирования;

b) мероприятия по физической безопасности должны быть разработаны таким образом, чтобы обнаружение находилось как можно дальше от цели. Задержки планируются ближе к цели;

c) проект системы безопасности должен связывать внешнее или внутреннее обнаружение с оценкой и реагированием;

d) меры физической безопасности могут включать в себя предупреждение преступности посредством проектирования среды, физических барьеров и упрочнения площадки, ограничений и контроля доступа на входе, охранного освещения, систем обнаружения вторжений и сигнализации, внутреннего видеонаблюдения, охраны персонала, политики и процедур безопасности.

Экономически эффективные стратегии минимизации последствий должны применяться для предотвращения или уменьшения воздействия потенциальных кризисов:

a) стратегии минимизации последствий должны рассматривать немедленные, временные и долгосрочные действия;

b) должны быть определены различные ресурсы, которые будут способствовать процессу минимизации последствий. Эти ресурсы, в том числе необходимый персонал, его обязанности и ответственность, средства, технологии и оборудование, должны быть отражены в плане и стать частью «обычной работы»;

c) системы и ресурсы должны постоянно подвергаться мониторингу как части стратегии минимизации последствий. Такой мониторинг можно сравнить с инвентаризацией запасов;

d) должен проводиться постоянный мониторинг ресурсов, необходимых организации для смягчения последствий кризиса, чтобы гарантировать, что они будут доступны и способны работать в соответствии с планом во время нарушения/срыва и кризиса. Примеры таких систем и ресурсов включают, но не ограничиваются этим: аварийное оборудование, системы пожарной сигнализации и пожаротушения, местные ресурсы и поставщиков, альтернативные рабочие места, карты и планы этажей, системы резервного копирования и внешнее хранилище.

B.8.7.4 Реагирование на инцидент

Планы готовности и реагирования следует разрабатывать на основе реалистичного «сценария наихудшего случая» с пониманием того, что реагирование может быть соответствующим образом масштабировано в соответствии с реальным кризисом.

Люди являются наиболее важным аспектом любой готовности и плана реагирования. То, как человеческие ресурсы организации управления будут влиять на успех или неудачу управления инцидентами.

a) Должна быть разработана система, с помощью которой весь персонал может быть быстро учтен после наступления кризиса. Эта система может варьироваться от простого телефонного справочника до тщательно продуманного сайта оповещения. Актуальная и точная контактная информация должна поддерживаться для всего персонала. Следует рассмотреть возможность привлечения услуг туристических компаний для оказания помощи в поиске сотрудников в командировках.

b) Должны быть приняты меры для уведомления о любых ближайших родственниках в случае травм или гибели людей. Если это возможно, уведомление должно осуществляться лично высшим руководством. Должно быть обеспечено соответствующее обучение.

c) Организация должна внедрить программу «Представитель семьи» в случае тяжелой травмы или смерти. Представителем семьи должен быть кто-то, кроме лица, выполняющего уведомление. Этот представитель должен выступать в качестве основной точки контакта между семьей и организацией. Комплексное обучение для представителя является необходимостью.

d) Кризисное консультирование должно быть организовано по мере необходимости. Во многих случаях такое консультирование выходит за рамки квалификации и опыта сотрудников организации. Другие надежные источники консультирования должны быть определены до кризисной ситуации.

e) Кризис может иметь далеко идущие финансовые последствия для организации, ее сотрудников и их семей, а также других заинтересованных сторон. Эти последствия следует считать важной частью плана готовности и реагирования. Последствия могут включать финансовую поддержку семей жертв. Кроме того, могут иметь место налоговые последствия, на которые следует ссылаться и уточнять заранее.

f) Система заработной платы должна оставаться в рабочем состоянии в течение всего кризиса.

Логистические решения, принятые заранее, будут влиять на успех или неудачу хорошей готовности и плана реагирования. Среди них есть следующие:

a) первичный кризисный центр должен быть заранее определен. Это должно быть определенное установленное помещение, используемое группой кризисного управления и группой реагирования для руководства и контроля действий по управлению кризисами. Данное помещение должно иметь источник бесперебойного питания; необходимые компьютерные, телекоммуникационные, отопительные, вентиляционные системы, системы кондиционирования воздуха и другие системы поддержки. Кроме того, предметы первой необходимости для чрезвычайных ситуаций должны быть идентифицированы и храниться в данном центре;

b) в тех случаях, когда выделенный центр невозможен, должно быть гарантировано назначенное место, где команды могут направлять и контролировать деятельность по кризисному управлению. Должны быть приняты меры контроля доступа, чтобы члены всех команд были в доступе 24/7;

c) должен быть определен вторичный кризисный центр на случай, если первичный центр подвергся воздействию кризиса;

d) организация должна рассмотреть вопрос о создании виртуальных командных центров для распределенного доступа к информации, а также для охвата рассредоточенных или удаленных заинтересованных сторон.

После того как команда/группа кризисного управления активирована, должен быть оценен ущерб. Оценка ущерба может проводиться самой группой кризисного управления или назначенной командой по оценке ущерба. Ответственность за документирование всех фактов, связанных с инцидентом, и ответные действия, включая финансовые расходы, должна быть возложена на уполномоченных лиц.

a) В ситуациях, связанных с физическим ущербом имуществу компании, на предприятии следует мобилизовать группу кризисного управления или назначенную им группу оценки ущерба. Группа получит доступ, если будет получено разрешение от органов общественной безопасности, и проведет предварительную оценку степени ущерба и вероятного периода времени, в течение которого объект будет непригодным для использования.

b) Некоторые виды нарушений/срывов не связаны с немедленным физическим повреждением рабочего места или объекта/средств организации. К ним относятся кризисы в бизнесе, с людьми, информационными технологиями и в обществе. В этих кризисах группа кризисного управления, скорее всего, оценит ущерб или воздействие по мере развертывания нарушения/срыва.

При необходимости следует изучить существующие финансовые и страховые полисы, а также определить и получить дополнительное финансирование и страховое покрытие.

a) Параметры полиса должны быть установлены заранее, включая предварительное одобрение страховой компанией любых поставщиков, связанных с реагированием. Там, где возможно, объем средств, помогающих обеспечить непрерывность операций, должен определяться в процессе планирования.

b) Любые денежные средства должны храниться в легкодоступном месте, чтобы обеспечить их доступность во время кризиса, а некоторые денежные средства и кредит должны быть доступны в выходные и в нерабочее время.

c) Все расходы, связанные с нарушением/срывом и кризисом, должны регистрироваться в форме записей в течение периодов реагирования и восстановления.

d) С поставщиками страховых услуг следует связаться как можно раньше в период реагирования, особенно в случаях широкомасштабного кризиса, когда конкуренция за такие ресурсы может быть жесткой. Все страховые полисы и контактная информация должны быть легко доступны группе кризисного управления и должны находиться в сохранности или вне офиса, в зависимости от обстоятельств.

Транспортирование во время нарушения/срыва или кризиса может быть проблемой. Условия транспортировки должны быть организованы заранее, если это возможно. Области, где транспортирование имеет решающее значение, включают, но не ограничиваются следующим:

a) эвакуация персонала — это может быть со снесенной старой площадки или с обособленного подразделения (в другом регионе или стране);

b) транспортировка на альтернативное рабочее место;

c) поставки на предприятие или на альтернативное предприятие;

d) транспортирование критически важных данных на рабочее место;

e) транспорт для персонала с особыми потребностями.

B.8.7.5 Планы обеспечения непрерывности и восстановления после инцидента

Организация должна разработать и документировать процедуры, подробно описывающие, как организация будет управлять разрушительным событием и как она будет восстанавливать или поддерживать свою деятельность на заранее определенном уровне, основываясь на утвержденных руководством целях восстановления:

a) соглашения о цепи поставок, критических поставщиках или поставщиках услуг должны быть установлены соответствующим образом, а их контактная информация должна храниться как часть планов реагирования, непрерывности и восстановления. Такая информация может включать номера телефонов, имена контактов, номера

счетов, пароли (надлежащим образом защищенные) и другую информацию в случае, если кому-то, кто не знаком с процессом, потребуется установить контакт;

b) во избежание нарушения цепи поставок может быть целесообразным запросить и проанализировать планы реагирования, непрерывности и восстановления у партнеров цепи поставок и критически важных поставщиков, чтобы оценить их способность продолжать предоставлять необходимые материалы и услуги в случае далеко идущего кризиса. Как минимум, обязанности продавца или поставщика услуг и соглашения об уровне обслуживания в цепи поставок должны быть согласованы до кризиса;

c) организация должна иметь альтернативное рабочее место, которое предназначено для возобновления и восстановления бизнеса. При отсутствии других и доступных объектов компании доступ к альтернативным рабочим местам может быть организован через соответствующих поставщиков. Планирование, касающееся идентификации и наличия альтернативных рабочих мест, должно осуществляться на ранней стадии процесса планирования готовности и плана реагирования. Альтернативные рабочие места должны обеспечивать адекватный доступ к ресурсам, необходимым для возобновления бизнеса, определенного как критичный с позиции последствий при анализе воздействия;

d) хранение данных и активов за пределами предприятия является ценной стратегией минимизации последствий, позволяющей быстро реагировать на кризис и возобновлять/восстанавливать бизнес. Внешнее хранилище должно находиться на достаточном расстоянии от основного объекта, чтобы такое же событие аналогичным образом не затронуло внешнее хранилище. Элементы, подлежащие рассмотрению для хранения за пределами площадки, включают в себя записи (на бумаге и других носителях), критически важные для деятельности предприятия. Процедура должна быть включена в план, чтобы обеспечить своевременную доставку любых необходимых предметов из внешнего хранилища в центр кризисного управления или на альтернативные рабочие места;

e) соглашение о взаимопомощи определяет ресурсы, которые могут быть использованы совместно или заимствованы у других организаций во время нарушений/ срывов, а также взаимную поддержку с другими организациями. Такие соглашения должны быть юридически обоснованы и надлежащим образом документированы, четко понятны всем вовлеченным сторонам и должны представлять надежные ресурсы, а также обязательство сотрудничать;

f) стратегические альянсы определяют партнеров по поставке, с которыми существуют взаимозависимые отношения для производства и поставки продуктов и услуг и распределения рисков;

g) как только степень ущерба становится известна, необходимо определить приоритеты процесса восстановления, а график восстановления должен быть разработан и задокументирован. Расстановка приоритетов должна учитывать фундаментальную критичность процесса и другие факторы, включая отношения к обязательствам в цепи поставок, другие процессы, критические графики и нормативные требования в формулировках критичности, тяжести последствий и анализа воздействия. Решения относительно определения приоритетов процессов должны быть задокументированы, и по ним должны вестись записи, включая дату, время и обоснование решений;

h) как только процессы, подлежащие восстановлению, будут расставлены по приоритетам, возобновление работы может начаться с процессов, восстановленных в соответствии с графиком расстановки приоритетов. Возобновление этих процессов может происходить либо на текущем рабочем месте, либо на альтернативном рабочем месте (в зависимости от обстоятельств кризиса). Документированное подтверждение, когда процессы были возобновлены, должно сохраняться;

i) после того как критические процессы возобновлены, приступают к возобновлению остальных процессов. Там, где это применимо, решения о приоритетности этих процессов должны быть тщательно задокументированы заранее. Время фактического возобновления процессов должно быть задокументировано;

j) организация должна стремиться вернуться к нормальной жизни. Если невозможно вернуться к докризисному «нормальному» уровню, следует установить «новый нормальный уровень». Этот «новый стандарт» создает ожидание того, что, хотя на рабочем месте могут произойти изменения и реструктуризация, организация вернется к продуктивной работе. Каждый шаг процесса и все решения должны быть тщательно задокументированы;

k) как правило, именно в этот момент кризис может быть официально объявлен «оконченным». Важно задокументировать это решение. Для повышения доверия сотрудников и клиентов могут проводиться пресс-конференции и общение в СМИ.

B.9 Контроль и корректирующие действия

B.9.1 Мониторинг и измерения

Данные, собранные в результате мониторинга и измерений, могут быть проанализированы для выявления закономерностей и получения информации. Знания, полученные из этой информации, могут быть использованы для осуществления корректирующих и предупреждающих действий. Должны быть установлены измеримые показатели, чтобы оценить успех политики менеджмента устойчивости.

Ключевыми характеристиками являются те, которые необходимо учитывать организации, чтобы определить, как она управляет своим значительным риском, достигает целей и целевых показателей, а также улучшает безопасность, готовность, реагирование, непрерывность и восстановление деятельности.

Для обеспечения достоверных результатов, когда это необходимо, измерительное оборудование следует калибровать или проверять через определенные промежутки времени или перед использованием в соответствии со

стандартами измерений, сопоставимыми с международными или национальными стандартами измерений. Если таких стандартов не существует, должны вестись записи по базе, используемой для калибровки.

В.9.2 Оценка соответствия и результатов деятельности системы

В.9.2.1 Оценка соответствия

Организация должна продемонстрировать оценку соответствия установленным нормативно-законодательным требованиям, включая применимые разрешения или лицензии. Организация должна иметь возможность продемонстрировать, что она оценила соответствие другим требованиям, относящимся к ее деятельности.

В.9.2.2 Учения и тестирования/испытания

Сценарии тестирований/испытаний должны разрабатываться с использованием событий, выявленных в оценке риска.

Тестирование может помочь группам реагирования и сотрудникам эффективно выполнять свои обязанности и выявлять недостатки в системе менеджмента устойчивости, которые необходимо исправить. Тестирование повышает доверие и авторитет к политике менеджмента устойчивости.

Первым шагом в тестировании/испытании должна стать постановка целей и ожиданий. Критическая цель состоит в том, чтобы определить, работает ли определенный процесс реагирования на нарушение и как его можно улучшить. Другие примеры целей включают в себя:

a) тестирование пропускной способности (например, пропускная способность телефонной системы для вызова или ответа);

b) сокращение времени, необходимого для выполнения процесса (например, использование повторных упражнений для сокращения времени реагирования);

c) обеспечение осведомленности и знаний всего персонала о системе менеджмента устойчивости.

Уроки, извлеченные из предыдущих тестирований/испытаний, а также фактических инцидентов, должны быть включены в цикл тестирования политики менеджмента устойчивости.

Должна быть установлена ответственность за тестирование политики менеджмента устойчивости. Более крупные организации могут рассмотреть возможность создания группы тестирования.

Где это применимо, можно использовать опыт внешних ресурсов (консультанты, местные аварийные службы и т. д.).

Необходимо установить расписание и график, как часто следует проводить тестирование плана и его компонентов.

Объем тестирования/испытания должен планироваться по времени. Тестирования должны начинаться с относительно простых вещей и становиться все более сложными по мере развития процесса тестирования. Первые тесты могут включать чек-листы учения и небольшие компоненты политики менеджмента устойчивости. По мере развития графиков тестирования тестирования должны становиться все более сложными, вплоть до полномасштабной активации всей политики менеджмента устойчивости, включая внешнее участие сотрудников служб безопасности и чрезвычайных ситуаций.

Некоторые участники могут выполнять несколько ролей в ходе тестирования. Все участники должны понимать свои обязанности в процессе обучения. В обучении должны участвовать все участники. В тестах могут участвовать различные группы из самой организации, а также из государственного сектора. В рамках учений участникам должно быть разрешено взаимодействовать и обсуждать вопросы и полученные уроки.

После завершения учений и тестирований результаты должны быть подвергнуты критической оценке. Оценка должна включать, среди прочего, оценку того, насколько хорошо были достигнуты цели и задачи теста, эффективность участия и будет ли сама система менеджмента устойчивости функционировать, как ожидается в случае реального кризиса. Будущее тестирование/испытание, а также сама система менеджмента устойчивости должны, при необходимости, модифицироваться на основе результатов тестирований.

План тестирования должен быть оценен и изменен по мере необходимости. Тестирования должны быть динамичными, принимая во внимание изменения в системе менеджмента устойчивости, текучесть кадров, фактические инциденты и результаты предыдущих учений.

Результаты учений и тестирования должны быть задокументированы.

В.9.3 Несоответствие, корректирующие действия и предупреждающие действия

В зависимости от характера несоответствия при установлении процедуры для удовлетворения этих требований организации могут выполнить их с минимальным формальным планированием, или это может быть более сложная и долгосрочная деятельность. Любая документация должна соответствовать уровню действий.

В.9.4 Управление записями

Система управления записями может включать среди прочего:

a) записи соответствия;

b) записи об обучении;

c) записи мониторинга процесса;

d) записи о поверке, техническом обслуживании и калибровке;

e) соответствующие записи подрядчиков и поставщиков;

f) отчеты об инцидентах;

g) записи о тестировании предварительной готовности к инцидентам и чрезвычайным ситуациям;

h) результаты аудита;

i) результаты анализа со стороны руководства;

j) решение по внешнему обмену информацией;

k) записи применимых нормативно-законодательных требований;

l) записи о значительном риске;

m) записи собраний по политике в области устойчивости;

n) записи по безопасности, готовности, реагированию, непрерывности и информированию о результатах деятельности по восстановлению;

o) записи о соответствии нормативным требованиям;

p) записи об обмене информацией с заинтересованными и вовлеченными сторонами.

Надлежащим образом следует учитывать конфиденциальную информацию.

Организация должна обеспечить целостность записей, сделав их защищенными от несанкционированного доступа, надежно зарезервированными, доступными только для уполномоченного персонала и защищенными от повреждения, порчи или потери.

Организация должна проконсультироваться с соответствующим юридическим органом в своей организации, чтобы определить соответствующий период времени, в течение которого документы должны храниться, установить, внедрить и поддерживать процессы для эффективного выполнения этих требований.

Примечание — Записи не являются единственным источником доказательств, подтверждающих соответствие настоящему стандарту.

B.9.5 Внутренний аудит

Внутренний аудит политики менеджмента устойчивости может проводиться персоналом организации или внешними лицами, выбранными организацией, работающими от ее имени. В любом случае лица, проводящие аудит, должны быть компетентными и иметь возможность делать это беспристрастно и объективно. В небольших организациях аудит должен проводиться персоналом, независимым от тех, кто несет прямую ответственность за проверяемую деятельность.

Примечание — Если организация желает объединить аудит своей политики менеджмента устойчивости с аудитом безопасности, охраны труда или окружающей среды, цель и область каждого из них должны быть четко определены.

B.10 Анализ со стороны руководства

Анализ со стороны руководства должен охватывать область распространения политики менеджмента устойчивости, хотя не все элементы политики необходимо пересматривать сразу, и процесс проверки может происходить в течение определенного периода времени.

Политику менеджмента устойчивости следует регулярно пересматривать и оценивать. Проверки следует проводить в соответствии с заранее установленным графиком, а документация по проверке должна поддерживаться в рабочем состоянии. Следующие факторы могут инициировать анализ, в противном случае его следует проводить после планирования:

- оценка риска. Политика менеджмента устойчивости должна пересматриваться каждый раз, когда оценка риска для организации завершена. Результаты оценки риска можно использовать для определения того, продолжает ли политика менеджмента устойчивости адекватно реагировать на риск, с которым сталкивается организация;

- отраслевые тенденции и изменения в секторе экономики. Основные отраслевые тенденции или изменения должны инициировать пересмотр политики менеджмента устойчивости. Общие тенденции в секторе/отрасли и в методах планирования непрерывности бизнеса могут использоваться для целей бенчмаркинга;

- нормативные требования. Новые нормативные требования могут потребовать пересмотра политики менеджмента устойчивости;

- опыт проведения мероприятия. Анализ политики менеджмента устойчивости следует проводить после инцидента, вызывающего разрушение;

- результаты тестирования и учений. На основе результатов тестирования и учений следует, при необходимости, изменить политику менеджмента устойчивости.

Постоянное улучшение и управление политикой менеджмента устойчивости должно отражать изменения в риске, действиях, функциях и деятельности организации, которые будут влиять на систему менеджмента устойчивости. Ниже приведены примеры процедур, систем или процессов, которые могут повлиять на планирование:

a) изменения в политике;

b) изменения опасностей и угроз;

c) изменения в организации и ее бизнес-процессах;

d) изменения в цепи поставок, потоках, узлах цепи поставок и обязательствах;

e) изменения в допущениях при оценке риска;

f) кадровые изменения (сотрудники и подрядчики);

g) изменения в поставщиках в цепи поставок;

h) технологические и технические изменения;

i) изменения в системах и прикладном программном обеспечении;

j) критические уроки, извлеченные из тестирования/испытания;

k) проблемы, обнаруженные при фактической реализации плана в условиях кризиса;

l) изменения внешней среды (новые предприятия в этом районе, новые дороги или изменения в существующих схемах движения и т. д.);

m) другие элементы, отмеченные при рассмотрении плана и выявленные в ходе оценки риска.

Приложение С
(справочное)

Соглашения по терминологии

Соглашения по терминологии в таблице С.1 соответствуют Директивам ИСО/МЭК, Часть 2, 2004, Приложение Н, Глагольные формы для выражения обязательств.

Таблица С.1 — Глагольная форма выражения обязательств

Глагольная форма	Значение	Использование (ИСО/ МЭК, Директивы. Часть 2. Правила для структуры и составления международных стандартов)	Эквивалентные выражения для использования в исключительных случаях
shall	Должен	Проверяемые требования к документу — «используется для указания требований, которым необходимо строго следовать для соответствия документу и отклонения от которых не допускаются»	Надо; требуется; требуется, чтобы; необходимо; необходимо, чтобы
should	Следует	Рекомендации — «используется для обозначения того, что из нескольких возможностей одна рекомендуется как особенно подходящая, без упоминания или исключения других, или что определенный курс действий предпочтителен, но не обязателен, или что (в отрицательной форме) определенная возможность или курс действий не рекомендуется, но не запрещается»	Рекомендуется, чтобы; желательно; надо; допустимо
may	Может	Разрешение — «используется для обозначения действий, допустимых в рамках документа»	Разрешается; допускается
can	Может	Возможности и способности — «используется для заявлений о возможностях и возможностях, материальных, физических или причинных»	Способен; есть возможность; возможно

Элементы, представленные в списках, не следует рассматривать как исчерпывающие, если не указано иное. Порядок списка также не следует рассматривать как определяющий последовательность или приоритет, если это не указано. Общий характер данного международного документа позволяет организации включать дополнительные элементы, а также обозначать последовательность или приоритет, основанный на конкретных условиях работы и обстоятельствах организации.

Приложение D
(справочное)

Выбор критериев для применения

Адаптация и внедрение ряда методов менеджмента устойчивости на систематической основе могут способствовать достижению оптимальных результатов для всех заинтересованных и вовлеченных сторон. Однако адаптация настоящего стандарта сама по себе не гарантирует оптимальных результатов устойчивости. Чтобы достичь целей, политика менеджмента устойчивости должна быть интегрирована в систему менеджмента и включать в себя лучшие имеющиеся практики, методы и технологии, где это уместно и где экономически целесообразно. Экономическая эффективность таких практик, методов и технологий должна быть полностью учтена.

Настоящий стандарт не устанавливает абсолютных требований к устойчивости за пределами обязательств в политике организации:

a) соблюдение применимых нормативно-законодательных требований и других требований, применимых к деятельности организации;

b) поддержка предупреждения критического риска и его минимизация;

c) приверженность постоянному улучшению.

Основная часть настоящего стандарта содержит только те общие критерии, которые могут быть объективно проверены в ходе аудита. Руководство по поддержке методов менеджмента устойчивости содержится в других приложениях к настоящему стандарту.

Настоящий стандарт, как и другие стандарты, не предназначен для использования в целях создания нетарифных торговых барьеров или для увеличения, или изменения юридических обязательств организации. Действительно, соблюдение стандарта само по себе не дает иммунитета от юридических обязательств. Организации могут проводить внешний или внутренний аудит на соответствие политики менеджмента устойчивости настоящему стандарту. Аудит может быть осуществлен первой, второй или третьей стороной. Проверка не требует сертификации. Сертификация применяется только к стандарту систем менеджмента, в которые интегрирован стандарт политики менеджмента устойчивости.

Настоящий стандарт не включает требования, относящиеся к другим политикам управления, таким как требования к качеству, охране труда и технике безопасности или управлению финансовыми рисками.

Уровень детализации и сложности политики менеджмента устойчивости, объем документации и ресурсы, предназначенные для ее выполнения, будут зависеть от ряда факторов, таких как область применения системы, размер организации, характер деятельности, товары и услуги, цепь поставок.

Стандарт предоставляет общий набор критериев для программ обеспечения безопасности, готовности к кризису и чрезвычайным ситуациям, непрерывности, бедствиям и программам управления восстановлением.

Терминология, используемая в настоящем стандарте, подчеркивает общность понятий, признавая при этом нюансы использования термина в различных дисциплинах. В соответствии с [8] оценка риска — это процесс идентификации, анализа и оценки риска (который включает в себя опасности, угрозы, риски, уязвимость, критичность, последствия и анализ воздействий).

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального и межгосударственного стандарта
ISO 28000:2007	—	*
* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык международного стандарта ISO 28000:2007, официальный перевод данного стандарта находится в Федеральном информационном фонде стандартов.		

Библиография

[1] ISO 9000:2005 — Quality management systems — Fundamentals and vocabulary
(Системы менеджмента качества. Основные положения и словарь)

[2] ISO 9001:2000 — Quality management systems — Requirements
(Системы менеджмента качества. Требования)

[3] ISO 14001:2004 — Environmental management systems — Requirements with guidance for use
(Системы экологического менеджмента. Требования и руководство по применению)

[4] ISO/IEC TR 18044:2004 — Information technology — Security techniques — Information security incident management
(Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности)

[5] ISO 19011:2002 — Guidelines for quality and/or environmental management systems auditing
(Рекомендации по аудиту систем менеджмента качества и/или охраны окружающей среды)

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

[7] ISO/PAS 22399:2007 — Societal security — Guidelines for incident preparedness and operational continuity management
(Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности)

[8] ISO 31000:2009 — Risk management — Principles and quedelines
(Менеджмент рисков. Принципы и руководящие указания)

[9] ISO Guide 73:2002 — Risk management — Vocabulary — Guidelines for use in standards
(Менеджмент риска. Словарь. Руководящие указания по использованию в стандартах)

[10] ISO Guide 73:2009 — Risk management — Vocabulary
(Менеджмент риска. Термины и определения)

[11] ANSI/ASIS.SPC.1:2009 — Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use

УДК 656.614.3.004:006:354 ОКС 03.100.01

Ключевые слова: система менеджмента, безопасность, цепь поставок, развитие, устойчивость, требования, руководство по применению

БЗ 2—2020/39

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.02.2020. Подписано в печать 24.03.2020. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5.45.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва. Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru