ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53647.4— 2011/ISO/PAS 22399:2007

МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ БИЗНЕСА

Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности

ISO/PAS 22399:2007
Societal security — Guideline for incident preparedness and operational continuity management
(IDT)

Издание официальное

Москва
Стандартинформ
2012

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Научно-исследовательский центр контроля и диагностики технических систем» (АНО «НИЦ КД») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в разделе 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 697-ст

4 Настоящий стандарт идентичен международному документу ISO/PAS 22399:2007 «Социальная безопасность. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности» (ISO/PAS 22399:2007 «Societal security — Guideline for incident preparedness and operational continuity management»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (подраздел 3.5).

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

© Стандартинформ, 2012

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

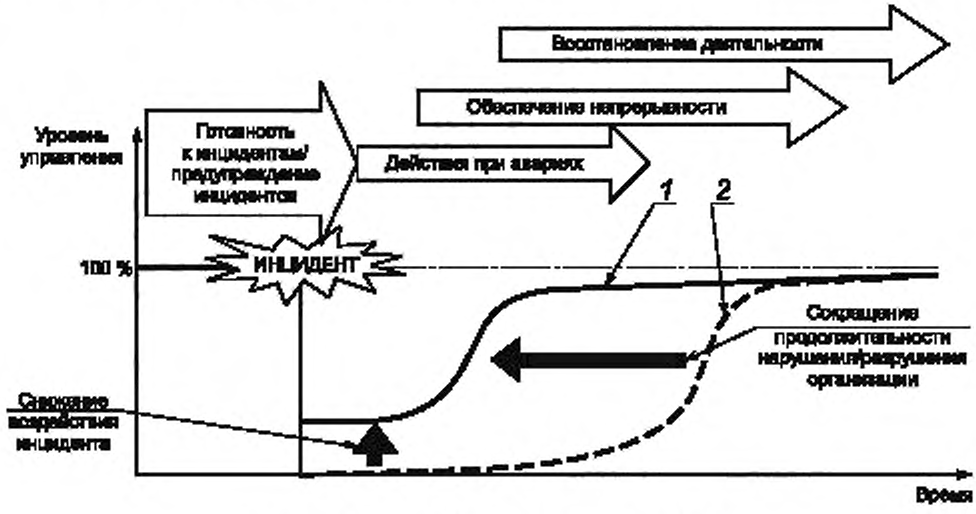
Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 2
3 Термины и определения . . . 2
4 Общие положения . . . 7
5 Политика . . . 8
6 Планирование . . . 10
7 Внедрение и функционирование . . . 16
8 Оценка . . . 18
9 Анализ со стороны руководства . . . 21
Приложение А (справочное) Процедура анализа воздействий на деятельность организации . . . 22
Приложение В (справочное) Программа управления неотложными аварийными мероприятиями . . . 24
Приложение С (справочное) Программа обеспечения непрерывности деятельности . . . 26
Приложение D (справочное) Внедрение системы обеспечения готовности к инцидентам и непрерывности деятельности . . . 28
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерациии . . . 29
Библиография . . . 30

Введение

Настоящий стандарт устанавливает процесс, основные принципы и термины в области обеспечения готовности к инцидентам и непрерывности деятельности (IPOCM[1)]) организации. Целью настоящего стандарта является установление основных положений для понимания, разработки и внедрения процессов обеспечения готовности к инцидентам и непрерывности деятельности организации, а также создания доверия общества, партнеров, потребителей и клиентов к организации. Настоящий стандарт содержит методы, которые могут позволить государственным и частным организациям исследовать воздействующие факторы при возникновении неумышленных, преднамеренных или природных инцидентов (например, авария, кризис или стихийное бедствие) и разработать необходимые действия, направленные на контроль за инцидентом и принятие надлежащих мер для обеспечения непрерывной деятельности организации. Настоящий стандарт также позволяет организации оценить в соответствии с общепринятыми методами свою способность к обеспечению готовности к инцидентам и непрерывности деятельности. Стандарт содержит общую схему обеспечения готовности к инцидентам и непрерывности деятельности, применимую к организациям всех видов деятельности и размеров, позволяющую учесть разнообразие их географических, культурных, экономических, национальных, политических и социально-бытовых особенностей.

Причастные стороны (заинтересованные стороны) требуют от организации быть заранее готовой к возможным инцидентам и нарушениям/разрушениям, чтобы не допустить приостановки критических видов деятельности, и, если произошла их полная остановка, быть способной быстро восстановить деятельность, поставку продукции и предоставление услуг (см. рисунок 1). Обеспечение готовности к инцидентам и непрерывности деятельности является процессом менеджмента, в рамках которого следует идентифицировать возможные негативные воздействия на организацию и создать структуру управления, направленную на минимизацию их воздействий.



1 — после внедрения IPOCM; 2 — до внедрения IPOCM

Рисунок 1 — Концепция готовности к инцидентам и IPOCM

В настоящем стандарте приведен полный набор средств управления, основанных на передовых методах IPOCM, используемых на всех этапах руководства и управления организацией. Стандарт будет полезен специалистам, ответственным за оперативное управление организацией как государственного, так и частного сектора, директорам и руководителям всех уровней организации, малым и средним предприятиям, а также большим и транснациональным корпорациям.

[1)] IPOCM — Incident preparedness and operational (business) continuity management — Обеспечение готовности к инцидентам и непрерывности деятельности.

Настоящий стандарт подробно описывает общие процессы планирования и управления, которые помогут организации при:

- анализе среды функционирования организации, ограничений и угроз для ее работы, которые могут привести к существенным разрушениям;
- количественной оценке воздействия нарушений/разрушений на критические виды деятельности и процессы организации;
- определении видов ее деятельности, которые являются критическими для достижения целей в краткосрочной и долгосрочной перспективе;
- идентификации инфраструктуры и ресурсов, необходимых организации для обеспечения непрерывности деятельности на минимальном уровне;
- документировании ключевых ресурсов, инфраструктуры, целей и распределении ответственности, необходимых для поддержки критических видов деятельности в случае возникновения нарушений/разрушений;
- установлении процессов, актуализации используемой информации и учета изменений риска и производственной среды;
- повышении осведомленности вовлеченного персонала, заказчиков, поставщиков и других причастных сторон об обеспечении готовности к инцидентам и непрерывности деятельности организации и, при необходимости, применении в организации всех требуемых процедур;
- выполнении принятых решений и обеспечении постоянного улучшения всех процессов.

Очевидно, что эффективное внедрение IPOCM требует основательных изменений деятельности организации, включая исследование и принятие решений в условиях неопределенности. На всех уровнях организации должно быть понимание того, что риск присущ каждому принимаемому решению и виду деятельности и может вызвать ее нарушение/разрушение. Поэтому на всех уровнях организации должен быть проведен анализ способов управления в условиях нарушения/разрушения.

Настоящий стандарт позволяет государственным и частным организациям оценить и управлять риском с целью повышения устойчивости и бесперебойной долгосрочной работы организации. Стандарт не устанавливает конкретную модель применения. Существуют различные признанные модели и методы, которые помогают внедрить систему IPOCM в деятельность организации, что позволяет сделать более эффективной и конкурентоспособной ее деятельность и гибко реагировать на любые возникающие проблемы. Настоящий стандарт предоставляет ряд методов идентификации и поиска решений по обеспечению готовности к инцидентам и непрерывности деятельности. Применяя динамические системные модели процессов управления, основанные на оценке риска, к системе обеспечения готовности к инциденту и непрерывности деятельности, следует учитывать имеющиеся ресурсы организации. Выбранная модель должна быть внедрена для обеспечения непрерывности деятельности организации.

Обычно модели управления включают в себя общие элементы: разработку политики, планирование, внедрение и функционирование, оценку выполнения, постоянное улучшение и анализ управления. В настоящем стандарте дано общее представление о содержании этих элементов, разработке и внедрении модели управления с учетом потребностей организации и ее места в обществе.

Выбранная организацией модель управления должна содержать полный спектр мероприятий, установленный IPOCM. IPOCM напрямую связана с организационным менеджментом и внедрением передового мирового опыта менеджмента. Система IPOCM устанавливает стратегическую и тактическую структуру опережающего менеджмента и обеспечения устойчивости работы организации в условиях разрушения, нарушения, перебоев или потерь при поставке продукции и предоставлении услуг. Эта система не должна носить только корректирующий характер и не должна быть направлена исключительно на устранение последствий инцидента. Одним из основных требований системы IPOCM является всестороннее планирование деятельности и составление программ развития организации. В связи с этим устойчивость организации обеспечивается квалификацией персонала, а также применением современных технологий и холистического подхода при внедрении модели или методов IPOCM.

К наилучшим результатам для всех причастных (заинтересованных) сторон может привести систематическая адаптация и внедрение набора методов IPOCM. Однако применение только одного настоящего стандарта не позволит обеспечить высокую степень готовности к инцидентам и непрерывности деятельности организации. Для достижения целей программы обеспечения готовности к инцидентам и непрерывности деятельности следует поощрять применение передового мирового опыта, методов и технологий, если они подходят организации и экономически обоснованы. Необходимо также учитывать рентабельность внедрения методов, технологий и мирового опыта.

Внедрение IPOCM требует координации и согласования различных элементов и субъектов в государственных и частных секторах (таких как правительственные и общественные организации на различных уровнях, торгово-промышленные объединения, неправительственные организации и отдельные

граждане). У каждого из них существуют свои собственные интересы, цели, задачи и обязательства, ресурсы и возможности, правила, методы и процедуры работы. Необходимо учитывать, что ключевые элементы программы IPOCM связаны и взаимодействуют с функциями и интересами различных субъектов, которые могут быть вовлечены при возникновении инцидента. Поэтому ключевые положения программы IPOCM необходимо рассматривать с учетом всех вышеназванных элементов и субъектов и их связи с программой IPOCM.

Реакция организации на опасные события, целью которой является минимизация их воздействия и сокращение социальных потерь, должна способствовать повышению социальной ответственности организации. В период разрушительных инцидентов необходимо понимать, что сотрудничество и помощь другим организациям в распределении человеческих и материальных ресурсов является существенным фактором в обеспечении непрерывности деятельности самой организации, поскольку собственные ресурсы, необходимые для восстановления в период инцидента, могут оказаться недостаточными или нерационально размещенными. Организация должна активно работать совместно с гражданским населением, местными органами власти, службами чрезвычайного реагирования и другими вовлеченными сторонами, принимая участие в аварийно-восстановительных работах, предоставляя необходимые ресурсы и помогая в действиях, направленных на спасение человеческих жизней. Организация должна также сотрудничать с представителями общественности и партнерами, чтобы учитывать их позицию в своей деятельности.

Организация может выбрать область применения элементов настоящего стандарта, ограничиваясь его использованием к конкретным услугам, продукции или в одном, или в нескольких регионах. Любое подобное ограничение области применения требований стандарта должно быть зарегистрировано.

Необходимо отметить, что настоящий стандарт не устанавливает абсолютные требования к системе IPOCM, при ее разработке следует учитывать обязательства, принятые в политике организации, установленные законодательные, обязательные и иные требования, мероприятия по предупреждению риска, предотвращению нарушений/разрушений и постоянному внедрению усовершенствований. Настоящий стандарт можно применять к системе постоянного улучшения, однако его положения не могут быть использованы в качестве критериев для оценки соответствия.

Поправка к ГОСТ Р 53647.4—2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности

В каком месте	Напечатано	Должно быть
Предисловие, пункт 3	№ 697-ст	№ 679-ст

(ИУС № 2 2013 г.)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ БИЗНЕСА

Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности

Business continuity management. Guideline for incident preparedness and operational continuity management

Дата введения — 2012—12—01

1 Область применения

Настоящий стандарт содержит общее руководство по установлению критериев оценки обеспечения готовности к инцидентам и непрерывности деятельности и разработке соответствующей системы менеджмента организации. Стандарт устанавливает основные положения для разработки и внедрения системы обеспечения непрерывности деятельности организации, а также обеспечения доверия со стороны общества, причастных сторон, потребителей и клиентов. Стандарт содержит методы оценки устойчивости организации к инцидентам и нарушениям/разрушениям ее деятельности.

Стандарт применим к организациям любых размеров и форм собственности, заинтересованных в обеспечении непрерывности поставки своей продукции, услуг или работы основных процессов. Применение настоящего стандарта помогает:

- проанализировать внешнюю и внутреннюю среду организации;
- идентифицировать критические для организации цели деятельности;
- проанализировать барьеры, опасные события, угрозы, риск и нарушения/разрушения, которые могут препятствовать достижению критических целей;
- оценить остаточный и приемлемый риск для понимания полученных результатов от применения стратегий снижения риска и внедрения средств управления риском;
- планировать способы обеспечения непрерывности достижения организацией поставленных целей при возникновении инцидента;
- разработать процедуры ответных мер на инциденты и аварийные ситуации, процедуры обеспечения непрерывности деятельности и процедуры восстановления ее нарушений/разрушений, вызванных инцидентом;
- определить обязанности, ответственность и обязательства, а также необходимые ресурсы для выполнения ответных мер, направленных на обеспечение непрерывности бизнеса в условиях инцидента;
- оценить соответствие действующим законодательным, обязательным и иным требованиям;
- обеспечить взаимопомощь с другими организациями и общественную поддержку;
- взаимодействовать со службами экстренного реагирования и средствами массовой информации (СМИ);
- изменить культуру организации и признать, что риск присущ каждому решению и действию и необходимо применять эффективный менеджмент организации.

Настоящий стандарт устанавливает общие принципы и элементы обеспечения готовности к инцидентам и непрерывности деятельности организации. Степень их применения зависит от таких факторов, как политика организации, особенности ее деятельности, выпускаемой продукции и предоставляемых услуг, месторасположения и условий организации производства.

Область применения настоящего стандарта не включает в себя действия в чрезвычайных ситуациях, такие как помощь при стихийных бедствиях и восстановление социальной инфраструктуры, которые

Издание официальное

выполняют государственные службы в соответствии с действующим законодательством. Однако следует координировать действия организации с действиями аварийных служб и регистрировать все выполненные действия в этой ситуации.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующий документ:

Руководство ИСО/МЭК 73:2002 Менеджмент риска. Термины и определения. Руководящие указания по использованию в стандартах (ISO/IEC Guide 73:2002, Risk management. Vocabulary. Guidelines for use in standards)[1)]

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **критические виды деятельности** (critical activities): Виды деятельности организации, которые должны быть выполнены для обеспечения поставки ключевой продукции и услуг, позволяющие достигать наиболее важных целей организации.

3.2 **последствие** (consequence): Результат воздействия события на объект.

Примечание 1 — Результатом воздействия события может быть одно или несколько последствий.

Примечание 2 — Последствия могут быть определенными или неопределенными, могут быть ранжированы от позитивных до негативных.

Примечание 3 — Последствия могут быть выражены качественно или количественно.

Примечание 4 — Первоначальные последствия могут вызвать эскалацию следующих последствий по принципу «домино».

[Руководство ИСО/МЭК 73]

3.3 **кризис** (crisis): Инцидент(ы) и происшествия, причиной которых является человеческий фактор и/или воздействие природных явлений и окружающей среды, требующие срочного вмешательства и действий для защиты жизни человека, имущества или окружающей среды.

3.4 **бедствие** (disaster): Событие, вызывающее большие повреждения или потери.

3.5 **нарушение, разрушение (деятельности организации)** (disruption): Невозможность поставки продукции или оказания услуг, установленных в соответствии с целями организации, или перебои в этой деятельности, вызванные ожидаемым (например, забастовка рабочих) или непредвиденным (например, отключение электрической энергии) инцидентом.

Примечание — Нарушение/разрушение может быть вызвано положительными и отрицательными факторами, которые нарушают нормальный ход деятельности.

3.6 **авария**[2)] (emergency): Внезапное, экстренное, обычно неожиданное происшествие или событие, требующее принятия безотлагательных мер.

Примечание — Авария обычно является разрушающим событием или условием, которое можно предвидеть и к которому можно подготовиться, однако точно спрогнозировать момент его появления достаточно сложно.

3.7 **учения** (exercising): Мероприятия, в процессе которых частично или полностью проходит отработка (репетиция) действий, обязанностей, способов восстановления и обеспечения непрерывности работы систем организации (например, технологий, систем связи и управления), предусмотренных программой IPOCM[3)], предназначенных для оценки содержания программы, ее соответствия запланированным результатам и компетентности персонала.

[1)] Международный документ Руководство ИСО/МЭК 73:2002 заменен на документ Руководство ИСО 73:2009 «Менеджмент риска. Словарь» (ISO Guide 73:2009 Risk management — Vocabulary).

[2)] В соответствии с ГОСТ 22.0.05—97 «Безопасность в чрезвычайных ситуациях. Техногенные чрезвычайные ситуации. Термины и определения» опасное техногенное происшествие, создающее на объекте, определенной территории или акватории угрозу жизни и здоровью людей и приводящее к разрушению зданий, сооружений, оборудования и транспортных средств, нарушению производственного или транспортного процесса, а также к нанесению ущерба окружающей природной среде.

Примечание: Крупная авария, как правило, с человеческими жертвами, является катастрофой.

[3)] IPOCM — Incident preparedness and operational (business) continuity management (Обеспечение готовности к инцидентам и непрерывности деятельности).

Примечание 1 — Учения включают в себя действия, выполняемые обычно с целью обучения и поддержания навыков членов рабочих групп и персонала в сложных ситуациях и в условиях инцидента, с целью достижения максимальной отработки необходимых ответных мер.

Примечание 2 — Учения обычно включают в себя действия процедур по обеспечению непрерывности бизнеса, но чаще объявленную или необъявленную имитацию инцидента, нарушающего непрерывность бизнеса, в процессе которого участники инсценируют возможную ситуацию, что позволяет оценить возможные проблемы до наступления реального инцидента.

3.8 **событие** (event): Возникновение или изменение специфического набора условий.

Примечание 1 — Событие может быть единичным или повторяющимся и иметь несколько причин.

Примечание 2 — Событие может быть определенным или неопределенным.

Примечание 3 — Для описания события могут быть использованы термины «инцидент», «происшествие», «опасное событие» или «несчастный случай».

Примечание 4 — Событие без последствий может также быть названо «угрозой возникновения опасного события», «инцидентом», «угрозой происшествия», «угрозой поражения» или «угрозой возникновения аварийной ситуации».

[Руководство ИСО/МЭК 73]

3.9 **опасность** (hazard): Возможный источник вреда, причиной которого могут быть естественные или техногенные явления, который способен привести к неблагоприятным воздействиям и последствиям.

3.10 **воздействие** (impact): Влияние разрушающих факторов, оцененное для конкретного события.

3.11 **анализ воздействия** (impact analysis): Процесс исследования функционирования системы и последствий воздействия на нее разрушающих факторов.

3.12 **инцидент** (incident): Событие, реализация которого может привести к нарушению/разрушению деятельности организации, потерям, аварии или кризису.

3.13 **план управления в условиях инцидента** (incident management plan): Детально разработанный и документально оформленный план действий, предназначенный для использования в условиях инцидента, в котором установлены необходимые для управления в условиях инцидента персонал, ресурсы и действия.

3.14 **готовность к инцидентам** (incident preparedness): Действия, программы и системы, разработанные и внедренные до возникновения инцидента, которые могут помочь организации смягчить последствия и выбрать эффективные ответные меры при возникновении инцидента, а также ускорить восстановление организации после разрушений, бедствий, критических ситуаций или аварий.

3.15 **обеспечение готовности к инцидентам и непрерывности деятельности** (incident preparedness and operational continuity management), IPOCM: Систематические и скоординированные действия, с помощью которых организация рационально управляет своими рисками и деятельностью в условиях возможных угроз и опасных воздействий.

3.16 **политика в области IPOCM** (IPOCM policy): Общие намерения и направления деятельности организации в области обеспечения готовности к инцидентам и непрерывности деятельности, официально сформулированные высшим руководством.

3.17 **уменьшение (последствий)** (mitigation): Ограничение негативных последствий конкретного инцидента.

3.18 **соглашение о взаимопомощи** (mutual aid agreement): Заранее разработанное соглашение между двумя или более субъектами об оказании, при необходимости, помощи и поддержки сторонам соглашения.

3.19 **непрерывность деятельности** (operational continuity), OC: Стратегическая и тактическая способность организации к функционированию на установленном приемлемом уровне при нарушениях ее деятельности, вызванных инцидентами.

Примечание — Термин «непрерывность деятельности» применим не только к коммерческим компаниям, но и к организациям любой формы собственности, таким как некоммерческие организации, общественные объединения и государственные организации.

3.20 **обеспечение непрерывности деятельности** (operational continuity management), OCM: Полный процесс управления, предусматривающий идентификацию возможных угроз и их воздействия на деятельность организации, который создает основу для повышения устойчивости деятельнос-

ти организации в условиях инцидента и разработки эффективных ответных мер, обеспечивающих защиту интересов ключевых причастных сторон, репутации организации, ее бренда и деятельности, добавляющей ценность.

Примечание — Обеспечение непрерывности деятельности включает в себя управление восстановлением или продолжением деятельности организации в случае инцидента, а также общей программой обеспечения непрерывности деятельности организации, предусматривающей обучение персонала, проведение учений и анализа деятельности, а также актуализацию соответствующих планов и программ.

3.21 **программа обеспечения непрерывности деятельности** (operational continuity management program): Процесс управления, поддерживаемый высшим руководством и обеспечиваемый необходимыми ресурсами, направленный на осуществление необходимых мер по идентификации воздействия возможных угроз, поддержку стратегии непрерывности деятельности и планов восстановления деятельности, а также на обеспечение непрерывности производства продукции и оказания услуг путем обучения персонала и проведения учений, внедрения, анализа и поддержания в рабочем состоянии системы обеспечения непрерывности деятельности организации.

3.22 **координационный совет обеспечения непрерывности деятельности** (operational continuity management team): Группа должностных лиц организации, уполномоченных и ответственных за разработку и исполнение планов обеспечения непрерывности деятельности, а также за инициирование работ при возникновении аварий и кризисов и непосредственное координирование работ в процессе восстановления после инцидента.

Примечание — Координационный совет обеспечения непрерывности деятельности может включать в себя представителей различных организаций, а также служб экстренного реагирования, причастные стороны и другие стороны.

3.23 **план обеспечения непрерывности деятельности** (operational continuity plan), OCP: Набор документированных процедур и информации, которые разработаны, обобщены и актуализированы с целью их использования в случае возникновения инцидента.

3.24 **стратегия обеспечения непрерывности деятельности** (operational continuity strategy): Способ обеспечения непрерывности деятельности организации, предусматривающий возможность восстановления и продолжения функционирования организации в условиях инцидентов, кризисов и других опасных событий.

3.25 **группа обеспечения непрерывности деятельности** (operational continuity team): Группа должностных лиц организации, ответственных за разработку, реализацию, инициирование и поддержку плана обеспечения непрерывности деятельности, включая процессы и процедуры, а также за проведение учений.

3.26 **организация** (organization): Группа работников и необходимых средств с распределением ответственности, полномочий и взаимоотношений.

Примечание — Организация может быть государственной или частной. Примерами организаций могут быть компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, предприятие розничной торговли, ассоциация, а также их подразделения или комбинация из них.

3.27 **предупреждающие (меры)** (prevention): Меры, позволяющие организации избежать, предотвратить или ограничить воздействие нарушений/разрушений деятельности организации.

3.28 **вероятность** (probability): Мера возможности появления события.

Примечание 1 — В ИСО 3534-1:1993 (пункт 1.1) приведено математическое определение вероятности. «вероятность — действительное число в интервале от 0 до 1, характеризующее случайное событие». Вероятность может отражать относительную частоту появления события в серии наблюдений или степень уверенности в том, что событие произойдет. При высокой степени уверенности в появлении события вероятность близка к единице.

Примечание 2 — При описании риска вместо «вероятности» может быть использовано понятие «частота».

Примечание 3 — Степень уверенности в появлении события может быть выражена с помощью отнесения события к определенному классу или разряду, таким как:

- крайне редко/маловероятно/вероятно/почти наверняка;
- невозможно/крайне маловероятно/редко/иногда/вероятно/часто.

[Руководство ИСО/МЭК 73]

3.29 **целевой срок восстановления** (recovery time objective); RTO: Плановое время возобновления деятельности и восстановления ресурсов, установленное на основе максимально приемлемого периода нарушения/разрушения деятельности организации.

3.30 **остаточный риск** (residual risk): Риск, оставшийся после обработки риска.

3.31 **устойчивость организации** (resilience): Способность организации противостоять воздействию инцидента, осуществляя свою деятельность.

3.32 **программа ответных мер** (response program): План, процессы и ресурсы для выполнения работ и услуг, необходимых для сохранения и защиты жизни людей, собственности, критических видов деятельности и активов организации.

Примечание — Этапы программы ответных мер обычно включают в себя распознавание инцидента, уведомление о нем, оценку инцидента, заявление об инциденте, план мероприятий и его реализацию, обмен информацией и управление ресурсами.

3.33 **риск** (risk): Следствие влияния неопределенности на достижение поставленных целей[1)].

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

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

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

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

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

[Руководство ИСО/МЭК 73]

3.34 **принятие риска** (risk acceptance): Обоснованное решение принять риск.

Примечание 1 — Решение о принятии риска может быть принято без обработки риска или в процессе обработки риска.

Примечание 2 — Необходимо проводить мониторинг и анализ принятого риска.

[Руководство ИСО/МЭК 73]

3.35 **оценка риска** (risk assessment): Общий процесс идентификации, анализа и сравнительной оценки риска.

[Руководство ИСО/МЭК 73]

Примечание — Оценка риска включает в себя процесс идентификации внутренних и внешних угроз и уязвимостей, идентификацию вероятности опасного события, возникшего при реализации этих угроз или уязвимостей, определение критических видов деятельности, для которых необходимо обеспечение бесперебойной работы, определение средств управления на местах, необходимых для снижения распространения последствий опасного события, и оценка стоимости таких средств управления.

3.36 **обмен информацией о риске и консультации в области риска** (risk communication and consultation): Непрерывные итеративные процессы, выполняемые организацией для обеспечения, распространения или получения информации и участия в диалоге с причастными сторонами по вопросам, относящимся к менеджменту риска.

Примечание 1 — Информация может относиться к существованию, природе, форме, правдоподобности, уровню, оценке, приемлемости, обработке или другим аспектам риска и менеджменту риска.

[1)] При применении стандарта следует учитывать, что, в соответствии с ФЗ «О техническом регулировании» от 27.12.2002 № 184-ФЗ, «риск — это вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда».

Примечание 2 — Консультации являются двухсторонним процессом обмена информацией между организацией и ее причастными сторонами по проблеме до принятия решения или определения действий по этой проблеме. Консультация это:

- процесс, который способствует принятию решения на основе убеждения, а не под давлением;
- процесс, который предшествует процессу принятия решения, но не объединяется с ним.

[Руководство ИСО/МЭК 73]

3.37 **критерий риска** (risk criteria): Совокупность факторов, по сопоставлению с которыми оценивают значимость риска.

Примечание 1 — Критерии риска основаны на установленных целях организации, внешней и внутренней области применения организации.

Примечание 2 — Критерии риска могут быть сформированы на основе требований стандартов, политики, законодательных и иных требований.

[Руководство ИСО/МЭК 73]

3.38 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в области риска.

Примечание — Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и обмен информацией о риске.

[Руководство ИСО/МЭК 73]

3.39 **снижение риска** (risk reduction): Действия, предпринятые для уменьшения вероятности опасного события, его негативных последствий или того и другого вместе.

3.40 **перенос риска** (risk transfer): Разделение с другой стороной потерь или выгод от риска.

Примечание 1 — Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.

Примечание 2 — Перенос риска может быть осуществлен с помощью страхования или других соглашений.

Примечание 3 — Перенос риска может создавать новый риск или модифицировать существующий риск.

Примечание 4 — Перемещение источника риска не является переносом риска.

3.41 **приемлемый риск** (risk tolerance): Общий суммарный риск, который организация готова принять, выдержать и которому готова быть подвергнута в любой момент времени.

3.42 **обработка риска** (risk treatment): Процесс модификации риска.

Примечание 1 — Обработка риска может включать в себя:

- исключение риска путем принятия решения не начинать или не продолжать деятельность, в процессе или в результате которой может возникнуть опасное событие;
- принятие или повышение риска для обеспечения более широких возможностей;
- устранение источников риска;
- изменение правдоподобности/вероятности опасного события;
- изменение последствий опасного события;
- разделение риска с другой стороной или сторонами (путем включения в контракты или финансирования обработки риска);
- обоснованное решение о сохранении риска.

Примечание 2 — Меры по обработке риска могут включать в себя устранение, предотвращение или снижение риска.

Примечание 3 — При обработке риска могут возникнуть новые риски и могут измениться существующие риски.

[Руководство ИСО/МЭК 73]

3.43 **модельные учения, практические учения** (simulation exercise): Учения, проводимые в условиях, близких к реальным, возникающим при реализации инцидента.

3.44 **источник риска** (source): Объект или деятельность, которые самостоятельно или в комбинации с другими обладают возможностью вызывать повышение риска.

Примечание — Источник риска может быть материальным или нематериальным.

[Руководство ИСО/МЭК 73]

3.45 **причастная сторона**[1] **(заинтересованная сторона)** (stakeholder (interested party)): Лицо или группа лиц, заинтересованных в деятельности или достижениях организации.

Примечание — Причастной стороной являются потребители, партнеры, персонал, акционеры, владельцы, организации службы экстренного реагирования, правительственные и регулирующие органы, ассоциации и др.

3.46 **настольные учения, теоретические учения** (tabletop exercise): Метод обучения, который основан на моделировании разрушения, аварии или кризисного сценария в формате рассказа, в рамках которого участники анализируют и обсуждают, но не выполняют политику, методы, процедуры, координацию мероприятий и распределение ресурсов, связанных с активацией плана.

3.47 **учения** (testing): Мероприятия, в процессе которых частично выполняют план(ы) обеспечения непрерывности деятельности, направленные на проверку того, что план содержит необходимую информацию и при выполнении приводит к запланированным результатам.

3.48 **угроза** (threat): Потенциальная причина инцидента, которая может привести к нанесению вреда людям, системе или организации, окружающей среде или обществу.

3.49 **высшее руководство** (top management): Директор или руководители подразделений, осуществляющие направление деятельности и управление организацией на высшем уровне, обеспечивая эффективность систем менеджмента, включая финансовый мониторинг, и системы контроля, назначенные для защиты активов, обеспечения работоспособности, рентабельности и укрепления репутации организации.

4 Общие положения

Схема процесса обеспечения готовности к инциденту и непрерывности деятельности, а также процесс постоянного улучшения показаны на рисунке 2. IPOCM является организационной структурой, которая требует проведения постоянного мониторинга и периодического анализа для обеспечения эффективного управления при изменении внутренних и внешних воздействующих факторов. Ответственность за работу, направленную на внедрение и совершенствование системы обеспечения готовности к инцидентам и непрерывности деятельности, необходимо распределить на всех уровнях организации. Положения IPOCM могут быть учтены при принятии решений в хозяйственной и административной деятельности всей организации.

[1] В соответствии с Руководством ИСО/МЭК 73 «причастная сторона — это любой индивидуум, группа лиц или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечание — Лицо, принимающее решение, также является причастной стороной».

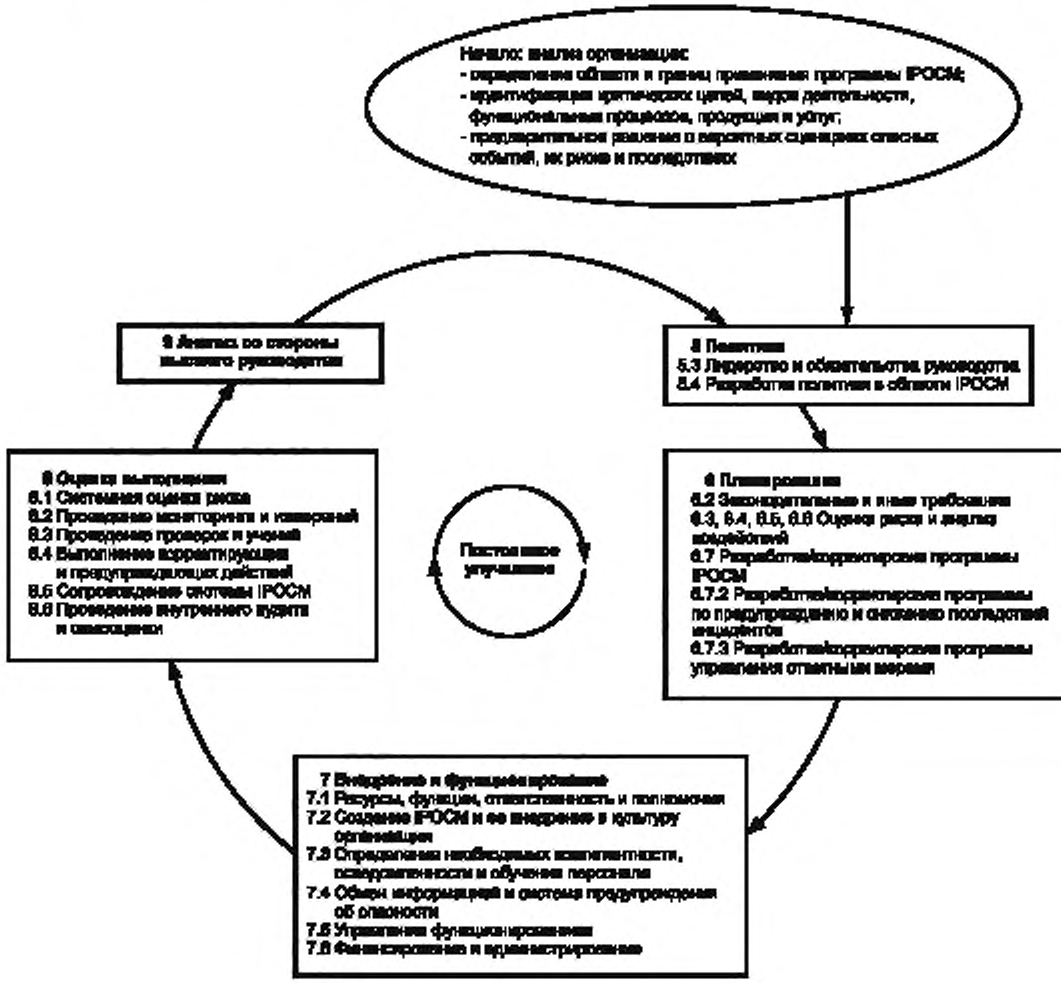


Рисунок 2 — Схема процесса обеспечения готовности к инцидентам и непрерывности деятельности

5 Политика

5.1 Проектирование и разработка программы

Целью создания программы обеспечения готовности к инцидентам и непрерывности деятельности является разработка, согласование и внедрение действий по управлению риском и обеспечению непрерывности деятельности организации. Эти действия должны соответствовать размеру, сложности и характеру деятельности организации и быть направлены на достижение ее способности гибко реагировать на любые возникающие изменения. Необходимо установить структуру управления способностью организации к непрерывности деятельности.

Установленные действия включают в себя проектирование, разработку, внедрение, первоначальные проверки и учения, направленные на внедрение в организации менеджмента непрерывности деятельности. Необходимо на ранних стадиях интегрировать методы и процедуры IPOCM при проектировании организационных или бизнес-процессов, процессов планирования, производства, обучения, разработки финансовой и экономической политики и соответствующих процедур. Работу по

обеспечению непрерывности деятельности необходимо регулярно проверять, актуализировать и пересматривать всякий раз, когда возникают существенные изменения в организации (например, во внешней среде, персонале, процессах или технологиях). IPOCM должна также обеспечивать защиту причастных сторон от возможного неблагоприятного воздействия последствий нарушения/разрушения деятельности организации.

Таким образом, программа IPOCM включает три основных компонента: создание структуры IPOCM, организационные мероприятия по ее внедрению и постоянное обеспечение непрерывности деятельности организации.

5.2 Определение области применения программы

Организация должна установить, зарегистрировать, внедрить, поддерживать в рабочем состоянии, оценивать и постоянно улучшать свои программы обеспечения готовности к инцидентам и непрерывности деятельности.

Организация должна определить критические цели и виды деятельности, идентифицированные в стратегиях, бизнес-планах, политике, задачах, планах менеджмента риска, определить средства управления, такие как анализ SWOT[1)] (сила, слабости, возможности и угрозы), и систему сбалансированных показателей. Критические для непрерывности деятельности процессы должны быть идентифицированы и зарегистрированы. Это позволит сконцентрировать ресурсы, требуемые для поддержания непрерывности критических видов деятельности организации с учетом существующих экономических ограничений.

Организация должна обосновать программу IPOCM, чтобы определить преимущества принятого подхода для всей организации. Обоснование может быть основано на:

- опасных предшествующих событиях, произошедших в организации;
- известной и возможной экспозиции опасных событий;
- тенденциях нарушений/разрушений деятельности с учетом опыта предшествующих инцидентов;
- росте затрат и потери доходов в случае реализации возможных разрушений;
- риске финансовых затрат;
- принятых обязательствах;
- социальной ответственности;
- достижениях и неудачах по другим проектам и программам IPOCM.

Организация должна определить и зарегистрировать область применения своей системы IPOCM, а также имеет право свободно и гибко определять границы системы IPOCM и может внедрить ее во всей организации, только в отдельных подразделениях или применить к отдельным видам деятельности. Следует рассмотреть взаимосвязь с другими организациями (партнерами) и причастными сторонами, которые могут помочь или повлиять на деятельность организации, включая воздействие процессов и действий по аутсорсингу и в цепи поставок. Область применения системы IPOCM должна быть напрямую связана с критическими видами деятельности, функциями, продукцией и услугами организации путем определения параметров оценки риска и разработки программы, основанной на их критическом состоянии, потенциальной вероятности и последствиях инцидента.

5.3 Лидерство и обязательства руководства

Эффективность программы IPOCM напрямую зависит от степени ее интегрирования в процессы менеджмента организации и поддержки со стороны высшего руководства. Программой IPOCM необходимо управлять на функциональном и организационном уровнях.

Привлечение специалистов в области других систем менеджмента может помочь при поддержке и управлении программой IPOCM. Количество требуемых ресурсов зависит от размера организации и разнообразия ее видов деятельности.

5.4 Разработка политики в области IPOCM

Организация должна разработать политику в области IPOCM. Первоначально это может быть заявление о политике на уровне высшего руководства с дальнейшим совершенствованием и углублением данного документа по мере развития и совершенствования обеспечения непрерывности деятельности организации. Политику следует регулярно анализировать и актуализировать в соответствии с потребностями организации.

Политика в области IPOCM должна содержать документированные принципы, к которым необходимо стремиться и в соответствии с которыми можно измерить способность организации к IPOCM.

Процесс установления политики организации должен включать в себя ряд элементов. Высшее руководство должно:

[1)] SWOT — Strengths, Weakness, Opportunities and Threats.

- принять решение о разработке программы IPOCM и довести принятое решение до сведения всей организации;
- установить основу политики в области IPOCM;
- обмениваться информацией о действиях организации по IPOCM с соответствующими внутренними и внешними причастными сторонами;
- обеспечивать доступность ресурсов, таких как бюджет и персонал, необходимых для исполнения действий в соответствии с основой политики в области IPOCM;
- участвовать в процессе разработки программы IPOCM.

5.5 Анализ политики в области IPOCM

Организация должна проводить регулярный пересмотр политики в области IPOCM в соответствии с:
- результатами анализа системы IPOCM;
- изменениями физической среды;
- данными о риске;
- изменениями в персонале, ключевых видах деятельности, услугах, процессах, продукции, поставщиках, дистрибьюторах, источниках финансирования, договорах подряда и конъюнктуре рынка;
- изменением юридического статуса (например, при слиянии и приобретении компаний);
- законодательными и обязательными требованиями.

Анализ политики в области IPOCM должен быть частью процессов оперативного и бизнес-планирования всей организации, одобренных высшим руководством. Политика в области IPOCM должна быть доведена до сведения всех подразделений и всего персонала организации.

5.6 Организационная структура внедрения программы IPOCM

Политику и стратегию внедрения программы IPOCM разрабатывает и реализует рабочая группа. Выбор применения формальной или неформальной структуры управления должен быть основан на:
- требованиях к постоянному визуальному контролю и участию со стороны высшего руководства;
- требованиях к квалификации персонала;
- ресурсах, бюджете и финансовых ограничениях;
- профессиональном уровне специалистов организации;
- специфике вовлеченных подразделений организации.

Организация может назначить координатора по программе IPOCM, на которого должна быть возложена ответственность за ее создание. Координатор программы IPOCM должен нести ответственность за координацию работ по обеспечению готовности к инцидентам и непрерывности деятельности, управление организационной структурой IPOCM, получение и обеспечение одобрения и поддержки со стороны высшего руководства, разработку и внедрение программы IPOCM, проведение обучения, регулярный анализ готовности к инцидентам и обеспечение непрерывности деятельности и др. Ответственность и полномочия высшего руководства должны быть точно определены и установлены в матрице ответственности организации.

Организация может сформировать межфункциональную группу по разработке программы IPOCM. В нее могут войти специалисты по основным направлениям реализации программы IPOCM, что позволит обеспечить решение любых возникающих проблем в организации.

6 Планирование

6.1 Общие положения

Организация должна установить, внедрить и поддерживать в рабочем состоянии процедуры идентификации угроз и опасностей, процедуры оценки риска, уязвимостей и опасностей и процедуры анализа воздействий на деятельность. На данной стадии устанавливают параметры стратегии и планирования, что позволит организации уменьшить вероятность нарушений/разрушений (при возникновении инцидента) и обеспечить непрерывность достижения поставленных целей путем продолжения выполнения критических видов деятельности на приемлемом для организации уровне. Анализ деятельности организации проводят на основе данных по идентификации и оценке потенциального риска и угроз нарушений/разрушений деятельности организации, а также продолжительности нарушений/разрушений, приемлемой для причастных сторон. На этом этапе организация должна провести анализ своей продукции и услуг и обеспечивающих их критических видов деятельности. Составление карты процесса и другие способы управления процессом могут помочь организации в анализе и документировании критических видов деятельности.

6.2 Законодательные и другие требования

Организация должна установить и поддерживать процедуры идентификации и оценки применимых законодательных, обязательных и иных требований, принятых организацией и связанных с угрозами и риском для оборудования, видов деятельности, продукции, услуг, подрядчиков и цепи поставок. Организация должна постоянно актуализировать эту информацию и проводить обмен информацией по законодательным и иным требованиям с персоналом и другими третьими лицами, включая подрядчиков.

Система IPOCM должна обеспечивать выполнение действующих законов и принятых обязательств, соответствовать требованиям стандартов организации, ее политике, а также основываться на исследованиях и применении передового промышленного опыта в области IPOCM.

6.3 Оценка риска и анализ воздействий

Существуют различные методы оценки риска и анализа воздействий на деятельность организации, на основе которых определяют этапы анализа.

6.4 Идентификация угроз, опасностей, риска

Идентификация угроз, опасностей, риска должна включать в себя (перечень может быть дополнен):

- опасности естественного происхождения, не зависящие от воздействия человека, способные прямо или косвенно воздействовать на деятельность, персонал, имущество и/или окружающую среду (геологические, метеорологические и биологические опасности) организации;
- события (случайные и преднамеренные), вызванные деятельностью человека и применяемыми технологиями;
- события, связанные с бизнесом (позитивные или негативные).

Идентификация риска должна стать непрерывной деятельностью. Организация должна выяснить источники и возможности причинения ущерба и идентифицировать опасные события. Организация должна консультироваться с государственными структурами и общественными организациями при идентификации опасностей для организации и причастных сторон.

6.5 Оценка риска

Организация может использовать формальный зарегистрированный процесс оценки риска, чтобы идентифицировать опасные события и угрозы, вероятность их возникновения, а также уязвимость и связанные с ней критические проблемы для персонала, имущества, среды и организации в целом. Организация должна количественно или качественно оценить вероятность возникновения идентифицированных опасных событий и их комбинации. Полученные результаты количественной оценки должны быть использованы как входные данные к процессу сравнительной оценки риска и ранжирования источников риска.

Организация должна оценивать риск на основе разумных критериев, учитывая совокупный риск ее деятельности. Организация должна учитывать различные аспекты, такие как опасность для жизни человека, активы, компенсации, доходы, кредиты и состояние окружающей среды. Организация должна провести анализ информации о риске и выбрать те виды риска, которые могут привести к существенным и/или недопустимым последствиям.

Организация должна обеспечить актуальность и конфиденциальность информации, связанной с оценкой угроз, риска и критических состояний. Эти оценки необходимо пересматривать при изменениях, происходящих в организации или ее операционной среде, процедурах, подразделениях и услугах.

6.6 Анализ воздействия на деятельность

Организация должна провести анализ воздействия нарушений/разрушений на свою деятельность и идентифицировать критические виды деятельности, первоочередные для восстановления, чтобы установить целевой срок восстановления (RTO) (см. приложение А).

Организация должна провести анализ воздействий нарушений/разрушений на свою деятельность, включая (но не ограничиваясь) следующие показатели:

- здоровье и безопасность людей в пострадавших районах в момент инцидента (травмирование и гибель людей);
- здоровье и безопасность персонала, ответственного за выполнение ответных мер в условиях инцидента;
- непрерывность деятельности;
- сохранение имущества, оборудования и инфраструктуры;
- непрерывность предоставления услуг;
- защита окружающей среды;

- благосостояние причастных сторон;
- экономическое и финансовое воздействие (включая анализ экономической эффективности защитных мер);
- выполнение законодательных и обязательных требований, контрактных обязательств;
- сохранение репутации организации или доверия к ней.

Из общего перечня продукции и услуг в системе поставок организация должна идентифицировать наиболее существенные для продолжения работ в критическом режиме.

Организация зависит от комплексной и взаимосвязанной инфраструктуры, включающей электроснабжение, водоснабжение, газоснабжение, транспорт и связь. Практически каждая организация зависит от эффективной работы инфраструктуры и, следовательно, от непрерывности коммунального обслуживания. Таким образом, организация особенно уязвима при возникновении нарушений/разрушений, когда в работе коммунальных или критических инфраструктур происходит сбой. Поэтому следует оценить воздействие сбоя, нарушений или разрушений инфраструктуры на критические виды деятельности.

Организация должна оценить затраты времени и ресурсов, требуемых для восстановления критических функций и точного определения последствий сбоев и разрушений с учетом возможного использования альтернативных способов работы и помощи других организаций в соответствии с соглашением о взаимной поддержке.

6.7 Программа обеспечения готовности к инцидентам и непрерывности деятельности

6.7.1 Общие положения

Программа IPOCM должна оцениваться на соответствие политике в области IPOCM, подтверждать обязательства по предупреждению инцидентов, сбоев, нарушений и разрушений деятельности организации, а также соответствовать действующим законодательным, обязательным и иным требованиям, принятым организацией. Программу IPOCM необходимо постоянно улучшать и совершенствовать. Программа IPOCM обычно включает в себя несколько программ, таких как программа предупреждения и снижения последствий инцидентов, программа управления ответными мерами и программа управления неотложными аварийными мероприятиями.

Организация должна установить, внедрить и поддерживать общую программу IPOCM и все включенные в нее программы для достижения целей и решения задач в области IPOCM на всех соответствующих уровнях и во всех подразделениях организации и определить:

- средства и календарный график, в соответствии с которыми цели будут достигнуты, а задачи решены;
- распределение ответственности за достижение целей и решение задач.

Все разработанные программы должны быть согласованы и, при необходимости, объединены друг с другом таким образом, чтобы исключить возможные конфликты и проблемы из-за пересечения функциональных возможностей, ответных мер, требований к ресурсам или времени. Планы анализа программ в качестве одного из средств интеграции, позволяющего скоординировать информационные потоки и выполняемые ответные меры, должны быть логичными, содержательными и совместимыми, а распределение и использование ресурсов должно быть результативным, эффективным и достижимым. Организация может назначить представителя высшего руководства в качестве общего руководителя или координатора программ IPOCM.

6.7.2 Программа предупреждения и снижения последствий инцидентов

Программа предупреждения и снижения последствий инцидентов должна быть основана на результатах идентификации угроз, опасных событий и оценки риска. В случае возникновения инцидента программа должна помочь минимизировать его воздействие, реагировать на него и быстро восстановить деятельность организации до приемлемого уровня.

В данной программе должны быть использованы приемы исключения, устранения или смягчения угроз и опасностей путем применения соответствующих методов и технологий, опыта других субъектов с учетом финансовых, производственных и бизнес-требований, а также мнения причастных сторон.

Программа предупреждения и снижения последствий инцидентов должна учитывать экономическую эффективность затрат. Она должна включать в себя (но не ограничиваться этим) следующие аспекты: технологические решения, количественную оценку пользы от применения и воздействия IPOCM, характер, размер и стоимость постоянных усилий в этой области, затраты в случае применения стратегий воздействия без IPOCM и возврат инвестированного капитала организации.

В программе предупреждения и снижения последствий инцидентов должны быть рассмотрены следующие аспекты:

- перемещение людей и имущества в случае возникновения опасности;

- перемещение, переоснащение и защита систем или оборудования;
- информационная безопасность, безопасность данных, документов и кибербезопасность;
- установление процедур предупреждения об опасности и обмена информацией;
- создание резерва персонала или дублирование основного персонала, критических систем, оборудования, информации, технологических операций или материалов, включая получаемые от подрядчиков.

План снижения последствий инцидентов должен содержать временные и долгосрочные меры, направленные на устранение опасности, которые воздействуют на объект в целом, и/или меры по уменьшению воздействий опасностей, риска и угроз, которые не могут быть устранены. Организация должна оценить возможность создания этими действиями нового риска. Поэтому при разработке плана снижения инцидентов необходимо внимательно проанализировать и оценить риск, соответствующий принимаемым решениям по предупреждению и снижению опасностей, а также рассмотреть последствия применения стратегий переноса риска.

6.7.3 Программа управления ответными мерами

Организация должна планировать ответные меры и восстановление после возникновения инцидента, учитывая основные виды деятельности, контрактные обязательства, потребности персонала и причастных сторон (например, жителей окрестных территорий), непрерывность деятельности и устранение ущерба, нанесенного окружающей среде. Организация может применить различные подходы к кризисному управлению. Независимо от подхода, существуют три общих взаимосвязанных шага проведения ответных мер, которые требуют приоритетного планирования и внедрения в случае разрушительного инцидента:

- неотложные аварийные меры: начальная реакция на разрушающий инцидент обычно включает в себя защиту людей и имущества от прямого ущерба. Активация руководством плана действий в аварийных ситуациях может стать частью первой ответной реакции организации на инцидент;
- меры обеспечения непрерывности деятельности в условиях инцидента: необходимо обеспечить доступность процессов, средств управления и ресурсов для обеспечения непрерывности деятельности и выполнения критических видов деятельности, обеспечивающих достижение целей организации;
- меры восстановления: следует восстановить процессы, ресурсы и возможности организации для обеспечения нормального хода ее деятельности. Меры восстановления часто включают в себя введение существенных организационных усовершенствований вплоть до переориентации стратегических или производственных целей.

Все планы ответных мер должны содержать общие элементы, включая следующие:

- функции и обязанности внутренних и внешних служб, вовлеченных организаций, подразделений и персонала;
- матрицу ответственности и полномочий для данных служб, вовлеченных организаций, подразделений и персонала;
- требования к компетентности всех участников;
- минимальные требования к ресурсам и их безопасному размещению.

Организация должна также рассмотреть диапазон и характер внешних связей. Необходимо идентифицировать:

- контактную информацию (в рабочее и внерабочее время);
- ожидания причастных сторон (согласованный минимальный уровень предоставления услуг, обязательные требования и т. д.);
- альтернативные способы производственной и функциональной деятельности организации (например, размещение поставок, изменение частоты взаимодействий и т. д.);
- альтернативные источники выполнения контрактных требований.

Следует рассмотреть взаимоотношения с потребителями, поставщиками, стратегическими партнерами, подрядчиками, государственными органами и конкурентами.

Необходимо признать, что в зависимости от серьезности воздействия инцидента высшее руководство организации может принять решение не предпринимать никаких действий по защите от инцидента. В этом случае высшее руководство может определить уровень приемлемости риска организации и принять этот риск. Решение о приемлемости риска должно быть зарегистрировано. В некоторых обстоятельствах воздействие риска может не соответствовать нормальному уровню приемлемости риска организации, однако из соображений низкой вероятности появления опасного события и/или экономической неэффективности рассматриваемых действий высшее руководство может принять подобный риск.

6.7.4 Программа управления неотложными аварийными мероприятиями

Главной целью программы управления неотложными аварийными мероприятиями является сохранение жизни людей и имущества (см. приложение В). Необходимо идентифицировать критерии

или процедуры активации мер управления в условиях инцидента и выполнения неотложных аварийных мероприятий. Управление в условиях инцидента должно быть процессом, который можно быстро инициировать и который следует активировать всякий раз, когда возникновение инцидента становится очевидным. Целями этого процесса являются:

- сокращение времени реагирования;
- оперативное принятие решений о необходимых действиях;
- своевременные действия по сдерживанию и контролю опасного события.

Организация несет непосредственную ответственность за охрану здоровья и благосостояния персонала, подрядчиков, посетителей/потребителей в случае, когда возникший инцидент представляет прямую угрозу для их жизни, лишения их средств к существованию и благосостояния. Особое внимание должно быть обращено на лиц с ограниченными возможностями (например, беременных и нетрудоспособных). Заранее спланированные действия в отношении таких лиц позволяют значительно снизить для них риск нанесения ущерба, снизить их беспокойство при воздействии инцидента. Вследствие значительной зависимости неотложных аварийных мероприятий от времени возможные сценарии следует основывать на оценке риска. Кроме того, необходимо установить систему обмена информацией о риске с причастными сторонами организации, а также систему социальной ответственности для взаимной помощи с другими организациями и причастными сторонами.

Для обеспечения быстрого уведомления высшего руководства о произошедшем инциденте организация должна определить многоуровневую систему определения серьезности и тяжести инцидентов и установить лиц, которые должны быть проинформированы в зависимости от уровня серьезности и тяжести инцидента. Организация должна определить и проводить обмен информацией, в том числе в виде отчетов, о том, что и где случилось, насколько серьезен инцидент, о причине случившегося, как быстро можно все восстановить и необходима ли внешняя помощь.

Запланированные действия должны быть применимы для намеченного уровня ответных мер и включать в себя:

- функции групп реагирования в общей структуре реагирования организации (стратегическая/тактическая/оперативная);
- точно установленный процесс обеспечения руководителей группы информацией, необходимой для принятия обоснованных решений относительно сбора или мобилизации группы реагирования;
- заранее установленные место/комната/пространство для совещаний группы. Это место должно быть командным пунктом реагирования организации на инцидент. Также должно быть определено дополнительное место совещаний в случае, если доступ к первично установленному пункту невозможен.

В программе управления неотложными аварийными мероприятиями должна быть определена стратегия обеспечения бытовых условий, которая включает в себя неотложные аварийные мероприятия и назначение группы лиц с точно установленными функциями и обязанностями для координации действий по обеспечению осуществления данной стратегии. Должны быть подготовлены планы, включающие в себя подготовку персонала для выполнения установленных функций и обязанностей.

Для обеспечения эффективности планы неотложных аварийных мероприятий и кризисного управления должны быть подготовлены и одобрены на уровне высшего руководства организации. Для этого необходимо показать их очевидную выгоду для высшего руководства, разработать должностные инструкции для вовлеченного персонала и согласовать бюджет. В крупных организациях могут быть назначены диспетчер или координатор программ и группа разработки, ответственные за стратегическую разработку программы.

Ресурсы, необходимые для выполнения неотложных аварийных операций, и планы кризисного управления должны быть четко идентифицированы. Ресурсы должны быть доступны и пригодны для предназначенного применения. Ограничения при использовании ресурсов должны быть учтены, ответственность за применение ресурсов не должна быть больше, чем за отказ их использовать. Стоимость ресурсов не должна превышать полученную выгоду.

6.7.5 Программа обеспечения непрерывности деятельности

Планы обеспечения непрерывности деятельности должны быть разработаны и зарегистрированы в полном объеме, что позволяет организации гибко реагировать на самые разные сценарии возможных инцидентов (см. приложение С).

Каждое подразделение организации может иметь свой специализированный план обеспечения непрерывности деятельности и общий план обеспечения непрерывности деятельности организации, направленные на управление действиями каждого подразделения и координацию активов (ресурсов), необходимых для восстановительных действий.

План обеспечения непрерывности деятельности организации – это набор инструментов, которыми может воспользоваться группа управления в условиях инцидента, исходя из сложившейся ситуации. Он содержит набор логических схем и информацию, необходимые для поддержки непрерывности работы организации во время инцидента, разрушающего или нарушающего ее деятельность. Главная цель плана обеспечения непрерывности деятельности состоит в сохранении критически важной для организации деятельности в случае крупного сбоя, воздействующего на нормальную работу. План обеспечения непрерывности деятельности разрабатывают в соответствии с ожидаемыми последствиями инцидентов на основе оценки риска (рассматривая в первую очередь риск, критически важный для организации) и анализа воздействий на деятельность (при этом идентифицируют конкретные виды деятельности, критически важные для организации, которые необходимо безотлагательно восстанавливать). План обеспечения непрерывности содержит детальное описание критических целей, процедур, мер и контактной информации, необходимых в случае возникновения инцидента, разрушающего деятельность организации, воздействующего на способность организации полностью или частично продолжать свою работу на приемлемом уровне, и направлен на стабильное выполнение критических видов деятельности и обеспечение работы подразделений до полного восстановления деятельности организации (в среднесрочной и долгосрочной перспективе).

Элементы и содержание плана обеспечения непрерывности деятельности могут быть разными для разных организаций и иметь разный уровень детализации в зависимости от размера организации, условий, в которых она работает, культуры и технической сложности производства, применяемых решений, информации о риске и особенностей среды функционирования. Для крупных организаций может потребоваться разработка отдельных документов о работе в критическом режиме для каждой из сфер деятельности организации или подразделений, тогда как для малых организаций может быть достаточно единого документа, который будет охватывать все критически важные вопросы обеспечения непрерывности деятельности.

Организация должна идентифицировать оборудование, запасы и взаимодействия в цепи поставок, которые поддерживают ее критические виды деятельности, и разработать стратегии защиты видов деятельности и системы поставок. Стратегии, применяемые в программе обеспечения непрерывности деятельности, направлены на повышение устойчивости организации к инцидентам и обеспечение непрерывности выполнения критических видов ее деятельности на приемлемом уровне и в установленные сроки, определенные на этапах оценки риска и анализа воздействий на деятельность. Окончательная цель программы обеспечения непрерывности деятельности состоит в восстановлении деятельности организации в установленные сроки, сохранении критических видов деятельности, непрерывности поставок ключевых продукции и услуг и исполнении ключевых поставок и обязательств.

6.7.6 Программа управления восстановлением деятельности

Принципиальной целью программы управления восстановлением деятельности организации является поэтапное возвращение к нормальному ходу деятельности с учетом внедрения возможных усовершенствований. Организация должна планировать восстановление своей деятельности после инцидента/разрушения с учетом контрактных обязательств, основных видов деятельности, интересов персонала и близлежащих сообществ, непрерывности деятельности, снижения риска, устранения экологических последствий и усовершенствования процессов.

Программа управления восстановлением должна содержать план восстановления и перечень целей и процедур для осуществления соответствующих действий. После проведения анализа информации о степени повреждений и воздействия на работу организации, собранной группой аварийного реагирования и обеспечения непрерывности деятельности, высшее руководство должно установить критерии и определить этапы восстановления, сроки и распределение ресурсов. В соответствии с ранжированием воздействий на деятельность, организация должна определить приоритет мероприятий с учетом всестороннего анализа степени повреждения оборудования, его фактической пригодности, имеющегося персонала и степени восстановления. На основе установленных приоритетов организация должна установить план распределения ресурсов, таких как персонал и материальное обеспечение.

В плане восстановления необходимо указать высшее руководство, лиц, принимающих решения, и других лиц, принимающих участие в рассмотрении:

- календарного графика восстановления отдельных видов деятельности;
- видов деятельности, подлежащих полной или частичной остановке;
- сроков возобновления всех видов деятельности;
- необходимых дополнительных инвестиционных ресурсов;
- возможностей улучшения процессов, инфраструктуры и отдельных видов деятельности;
- угроз со стороны партнеров и конкурентов и их возможностей;
- приоритетных планов, основанных на полученном опыте.

7 Внедрение и функционирование

7.1 Ресурсы, функции, ответственность и полномочия

Организация должна определить и обеспечить ресурсы, а также заключить соглашения о сотрудничестве, существенно необходимые для внедрения и управления системой IPOCM и постоянного повышения ее эффективности. Ресурсы включают в себя человеческие ресурсы (например, персонал, выполняющий работу), инфраструктуру, технологии, финансовые, информационные и интеллектуальные ресурсы. Персонал должен обладать необходимой компетентностью на основе соответствующего образования, обучения, навыков и опыта.

Функции, обязанности и полномочия персонала и причастных сторон должны быть определены и зарегистрированы, для обеспечения эффективности IPOCM следует обмениваться информацией о них.

Высшее руководство организации должно возглавить весь процесс и назначить представителя(ей) из числа высшего руководства, который(е), независимо от других обязанностей, должен определять функции, обязанности и полномочия для:

- обеспечения создания, внедрения и поддержки элементов и процессов системы IPOCM;
- оценки, анализа и отчета высшему руководству о внедрении системы IPOCM и представления предложений по ее улучшению;
- содействия повышению осведомленности об элементах системы IPOCM персонала организации.

Организация должна установить логистические возможности и процедуры по привлечению, размещению, сохранению, проверке и учету персонала, ресурсов, материалов и средств, произведенных или пожертвованных для поддержки системы IPOCM.

При установлении целей управления ресурсами необходимо проанализировать, как минимум, следующие факторы:

- персонал (необходимость его обучения), оборудование, средства, фонды, мнения экспертов, материалы и календарные сроки, в пределах которых они будут востребованы из общих ресурсов организации или у партнеров;
- время реагирования, возможности, ограничения, затраты, объем и ответственность, связанные с использованием вовлеченных ресурсов.

7.2 Внедрение IPOCM

Создание, распространение и внедрение культуры IPOCM в организации обеспечивает повышение качества корпоративного управления, при этом IPOCM может стать дополнительным активом организации (см. приложение D). При эффективном внедрении IPOCM повышает доверие причастных сторон к способности организации справиться с крупными сбоями и нарушениями деятельности.

Успешное внедрение подразумевает, что IPOCM действует во всей организации, весь персонал должен быть вовлечен в этот процесс. На всех уровнях управления в высшем и среднем звене руководители играют существенную роль в начале, при выборе критических видов деятельности и процессов, поэтому получение их поддержки на начальной стадии жизненно важно. Весь штатный персонал должен быть убежден, что IPOCM — важное направление деятельности для организации, и персонал играет в нем важную роль, обеспечивая непрерывность поставки продукции и услуг их клиентам и потребителям. Уровень осведомленности персонала и программы его обучения должны быть установлены как часть полного внедрения системы IPOCM.

Важна осведомленность персонала организации о том, что будет внедрено в рамках IPOCM и почему. Персонал должен убедиться, что IPOCM — долгосрочная инициатива, которую поддерживают руководители организации. Персонал должен быть уверен, что его работа защищена от воздействия всех инцидентов, разрушающих деятельность организации. Критически важно, чтобы персонал, вовлеченный в реализацию планов IPOCM, знал, какие действия он обязан предпринять при активации соответствующих планов.

Новый персонал организации должен быть ознакомлен с политикой IPOCM и своих функциях в программах IPOCM. Этого можно достичь путем включения материалов IPOCM в программы вводного инструктажа.

Осведомленность о полной программе IPOCM должна постоянно актуализироваться. Методы актуализации могут включать в себя внутренние газеты, электронные письма, интернет, совещания групп и обмен информацией с высшим руководством. Могут пропагандироваться примеры успешного преодоления организацией инцидентов и/или успешного выполнения персоналом поставленной задачи. Организация может также изучить передовой опыт работы с внешними отказами и внедрить его в свою деятельность.

7.3 Компетентность, обучение и осведомленность

Организация должна обеспечить необходимую компетентность персонала на основе соответствующего образования, подготовки, навыков или опыта (записи об этом должны быть зарегистрированы) или причастных сторон, выполняющих работы для организации или от ее имени, которые могут быть вовлечены в деятельность по предупреждению инцидентов, исследованию их причин, выполнению ответных мер, снижению последствий или могут быть подвержены воздействию идентифицированных опасностей или угроз.

Организация должна оценить потребности в обучении персонала, разработать и внедрить план обучения и план повышения уровня образования для поддержки программы IPOCM. Эти планы должны быть направлены на выполнение всех применимых обязательных требований. Целью обучения является повышение осведомленности и навыков, необходимых для разработки, внедрения, поддержки программы IPOCM. Периодичность и программа обучения должны быть идентифицированы.

Организация должна установить, внедрить и поддерживать процедуры обеспечения осведомленности персонала (лиц, работающих для нее или от ее имени) о:

- важности соответствия политике, процедурам и другим элементам системы IPOCM;
- существенных угрозах, опасностях, фактических или потенциальных воздействиях, связанных с работой персонала, и преимуществах усовершенствованных способов ее выполнения;
- своей роли и обязанностях в достижении целей и задач программы IPOCM;
- процедурах сдерживания, снижения, реагирования и восстановления до, во время и после инцидента/разрушения;
- потенциальных последствиях отклонения от указанных процедур.

7.4 Обмен информацией и предупреждение об опасности

Организация должна установить, внедрить и поддерживать процедуры ответов на запросы и распространения информации относительно угроз, опасностей, риска и требований системы IPOCM до, во время и после инцидента/разрушения. Должны быть разработаны процедуры предоставления информации внутренней и внешней аудитории, включая СМИ и их запросы о текущих и аварийных ситуациях, для:

- внутреннего обмена информацией между различными уровнями и подразделениями организации и партнерами;
- получения соответствующего запроса от внешних заинтересованных сторон, его регистрации и своевременного ответа на него;
- адаптации и интеграции национальных или региональных справочных и обучающих систем работы с опасностями или угрозами, или их эквивалентами, а также их внедрения в плановую или текущую работу организации;
- оповещения и приведения в готовность людей, подвергшихся или потенциально подверженных инциденту;
- облегчения структурированного обмена информацией с аварийными службами;
- обеспечения доступности средств связи в ситуации кризиса и разрушений;
- обеспечения способности к разнонаправленному взаимодействию и реагированию организации и персонала;
- регистрации записей жизненно важной информации об инциденте, предпринятых действиях и принятых решениях;
- обеспечения потребности в необходимых средствах связи и концентраторах сети.

Организация должна принимать решения, исходя из принципа обеспечения безопасности жизнедеятельности и здоровья людей, на основе консультаций с причастными сторонами о необходимости внешнего обмена информацией о своих наиболее существенных опасностях, риске и угрозах до и после инцидента и должна зарегистрировать свое решение. Если принято решение о необходимости такого обмена информацией, организация должна установить и внедрить методы внешней связи, сигналы тревоги и сигналы об опасности. При обмене данными должны быть обеспечены защита и целостность секретной информации и разработаны процедуры публичного представления несекретных данных, необходимых для координации IPOCM.

До инцидента организация должна разработать стратегию обмена информацией, основанную на ответах на следующие вопросы:

- кто нуждается в информации;
- какая и когда информация необходима или может быть запрошена;
- какие организационные ограничения и сдерживающие факторы существуют;
- кто наделен полномочиями одобрения и распространения обмена информацией;

- как организован обмен информацией со СМИ;
- как управлять слухами.

Организация может разработать релизы для обмена информацией перед инцидентом, включая руководящие принципы по превентивным действиям и осведомленности о программе IPOCM. В стратегии должны быть также определены средства, с помощью которых различные типы связи будут использованы для каждой из причастных сторон.

Систему обмена информацией IPOCM следует регулярно проверять.

7.5 Управление функционированием

Организация должна установить и внедрить систему документированных процедур и средств управления деятельностью организации в соответствии с политикой в области IPOCM, угрозами, опасностями, риском, критическими видами деятельности, данными анализа воздействий на деятельность и установленными целями. Организация должна планировать эту деятельность, включая этап сопровождения, чтобы обеспечить:

- установление, внедрение и сопровождение документированных внутренних процедур;
- установление соответствующих критериев во внутренних процедурах;
- установление, внедрение и сопровождение процедур, связанных с идентифицированными существенными рисками, угрозами и опасностями организации, применение процедур обмена информацией и выполнение требований к системе поставок (включая требования к подрядчикам).

Чтобы минимизировать вероятность возникновения разрушающего инцидента, эти процедуры должны включать в себя средства управления, относящиеся к функционированию, проектированию, установке, восстановлению деятельности, соответствующих элементов оборудования, инструментов и т. д. и изменению их риска. Если принято решение о внедрении подобных мероприятий и они могут повлиять на текущую работу, организация должна рассмотреть способы минимизации угроз и риска до их внедрения.

Процедуры функционирования и средства управления должны обеспечивать надежность и устойчивость работы организации, безопасность и здоровье людей и защиту собственности и окружающей среды от воздействия разрушительного инцидента.

Организация должна установить процедуры для создания и сопровождения системы документации IPOCM, необходимой для обеспечения эффективного планирования, функционирования и управления процессами системы IPOCM.

7.6 Финансовые и административные процедуры

Организация должна разработать финансовые и административные процедуры для поддержки программы IPOCM до, во время и после инцидента. Такие процедуры должны обеспечивать быстрое принятие финансовых решений на соответствующем уровне руководства и согласно принятым учетным принципам. Процедуры должны включать в себя (но не быть ограничены) следующие аспекты:

- установление и определение обязанностей по программе IPOCM;
- финансовые полномочия, включая отчетность координатору(ам) программы;
- процедуры закупок в соответствии с программой;
- платежные ведомости;
- систему учета и отчетности для анализа и регистрации затрат.

8 Оценка

8.1 Оценка системы

Организация должна оценивать планы, процедуры и возможности системы IPOCM на основе данных регулярного анализа, тестирования, отчетности после инцидента, анализа полученного опыта, оценки эффективности функционирования системы и проведения учений. Все существенные изменения должны быть немедленно отражены в процедурах.

Кроме выполнения принятых требований о соответствии организация должна установить, внедрить и поддерживать в рабочем состоянии процедуры периодической оценки соответствия применимым юридическим требованиям, передовому опыту и собственной политике и целям в области IPOCM.

Организация должна вести записи результатов периодической оценки.

8.2 Мониторинг и измерения

Превентивный мониторинг проводят для проверки соответствия и оценки эффективности программы IPOCM, в то время как текущий мониторинг проводят для исследований, анализа и регистрации отка-

зов системы, опасных событий и разрушений, включая небольшие сбои и пограничные значения показателей.

Организация должна установить и поддерживать процедуры выполнения мониторинга и измерений на регулярной основе. Эти процедуры должны предусматривать:

- качественные и количественные критерии, соответствующие потребностям организации;
- мониторинг степени достижения целей организации в области IPOCM;
- превентивные оценки выполнения работ, мониторинг которых проводят для проверки их соответствия программе IPOCM, критериям функционирования и применимым правовым и регулирующим требованиям в области IPOCM;
- текущие оценки (измерения) для проведения мониторинга событий и разрушений, включая сбои и другие свидетельства неполного функционирования системы IPOCM;
- регистрацию данных и результатов мониторинга и измерений, достаточных для облегчения последующего анализа корректирующих и предупреждающих действий.

8.3 Проверки и учения

Программа учений должна быть совместима с целями организации и соответствующими обязательными требованиями в области IPOCM. Учения могут включать проверки, имеющие предопределенный результат, настольные учения, учения с использованием моделирования ситуации и полномасштабные учения. Учения должны быть основаны на реалистичных сценариях, которые должны быть тщательно спланированы и согласованы с причастными сторонами и должны обеспечивать минимальный риск нарушения рабочих процессов. Для каждого учения должны быть точно поставлены цели и задачи и определена форма отчета после их завершения с указанием дальнейших рекомендаций. Форма отчета должна быть установлена, а отчет своевременно использован для улучшения системы IPOCM.

Учения позволяют провести:

- верификацию того, что программа IPOCM полностью охватывает критические виды деятельности организации, их взаимосвязи и приоритетность;
- ориентацию и тестирование лиц, отвечающих за программу IPOCM, позволяющие провести оценку знания ими своих функций и обязанностей;
- постоянное улучшение программы IPOCM;
- проверку технических, логистических, административных, процедурных и других аспектов планов IPOCM;
- проверку системы IPOCM организации и ее инфраструктуры (включая центры управления и производственную среду);
- оценку технологических и телекоммуникационных ресурсов для обеспечения готовности и перемещения персонала;
- регистрацию достаточного количества данных и результатов проверок и учений для проведения последующего анализа корректирующих и предупреждающих действий.

Проверки должны охватывать (но не быть ограничены) следующее:

- планы действий персонала;
- планы управления в условиях инцидента;
- планы обмена информацией;
- планы восстановления критических видов деятельности;
- планы размещения;
- системы резервного копирования и восстановления данных, физической и компьютерной безопасности;
- соблюдение правовых требований.

8.4 Корректирующие и предупреждающие действия

Организация должна установить, внедрить и поддерживать в рабочем состоянии корректирующие процедуры для работы с фактическими и потенциальными несоответствиями программы и выполнения соответствующих корректирующих и предупреждающих действий.

В процедурах должны быть определены критерии для:

- идентификации и корректировки несоответствий программы и предпринятых действий по снижению их воздействия;
- исследования несоответствий программы, определения их причин и выполнения действий, направленных на исключение их повторного появления;
- оценки потребности в действиях, направленных на предотвращение несоответствий программы и внедрение мер, исключающих их возникновение;

- регистрации результатов предпринятых корректирующих и предупреждающих действий;
- анализа результативности предпринятых корректирующих и предупреждающих действий.

Предпринятые действия должны соответствовать значимости проблем, риска и возможных последствий. Организация должна обеспечивать внесение всех необходимых изменений в документацию системы IPOCM.

8.5 Сопровождение системы IPOCM

Должна быть установлена четко определенная и зарегистрированная программа поддержки IPOCM. Эта программа должна обеспечивать проведение анализа всех изменений системы IPOCM (внутренних или внешних), воздействующих на организацию. Необходимо также идентифицировать все новые критические виды деятельности, включаемые в программу сопровождения системы IPOCM.

В соответствии с программой сопровождения системы IPOCM необходимо периодически:

- исследовать и оценивать предположения, используемые при анализе воздействий на деятельность организации;
- доводить обновленную, исправленную или измененную политику, стратегии, решения, процессы и планы в области IPOCM до сведения ведущих специалистов организации в соответствии с формальным процессом управления изменениями (версиями) в системе IPOCM.

Входными данными процесса сопровождения системы IPOCM являются:

- зарегистрированные объективные свидетельства превентивного руководства и управления программой IPOCM организации;
- данные верификации эффективной работы процессов и процедур управления изменениями (версиями) на местах;
- данные верификации наличия на местах ключевого персонала, осуществляющего стратегию и планы IPOCM;
- результаты идентификации и документирования плана-графика сопровождения системы IPOCM;
- данные верификации мониторинга и управления риском, соответствующим IPOCM организации.

8.6 Внутренний аудит и самооценка

Организация должна обеспечивать регулярное проведение внутреннего аудита и самооценки для определения соответствия системы IPOCM установленным требованиям, а также соответствующего внедрения и сопровождения программы IPOCM. При проведении самооценки необходимо учитывать устойчивость ключевых видов деятельности и результаты предыдущих аудитов.

Процедуры аудита и самооценки должны быть установлены, внедрены, поддерживаться в рабочем состоянии и направлены на обеспечение выполнения обязательств и требований по планированию и проведению аудита. В процедуре должно быть предусмотрено составление отчета о результатах аудита и сохранение записей, определены критерии, область применения, частота и методы аудита. Результаты аудита должны быть предоставлены руководству организации.

При проведении аудита следует обеспечивать объективность и беспристрастность аудиторов.

Самооценка программы IPOCM организации должна включить в себя верификацию того, что:

- критические виды деятельности и вспомогательные работы для них идентифицированы и включены в стратегию IPOCM организации;
- политика, стратегии, структура и планы IPOCM непрерывно и точно отражают приоритеты и требования организации;
- компетентность персонала организации в области IPOCM и способность организации к IPOCM обеспечивают достижение установленных целей и могут результативно и своевременно обеспечить управление, руководство, контроль и координацию в случае инцидента;
- решения организации в области IPOCM являются эффективными, своевременными и обеспечивают достижение установленных целей, а также соответствуют приемлемому уровню риска организации;
- программы сопровождения системы IPOCM и учений в организации успешно внедрены;
- стратегии и планы IPOCM учитывают опыт, полученный при проведении учений, информация о которых содержится в записях об учениях и поправках, внесенных в результате реализации программы сопровождения системы;
- процессы управления изменениями на местах работают результативно.

Проведение самооценки также должно включать в себя определение степени достижения целей организации. При этом необходимо учитывать имеющуюся практику и передовой опыт.

9 Анализ со стороны руководства

Высшее руководство должно проводить через запланированные интервалы времени анализ системы IPOCM организации, направленный на обеспечение ее непрерывной пригодности, адекватности и эффективности. При проведении анализа необходимо оценить возможности для улучшения и потребности в изменениях системы IPOCM, включая политику и цели в области IPOCM. Записи анализа со стороны руководства должны быть сохранены.

Входными данными для анализа со стороны руководства являются, но не ограничены:

- результаты внутреннего аудита и оценки соответствия правовым и обязательным требованиям, применяемым организацией;
- данные обмена информацией с внешними заинтересованными сторонами, включая претензии;
- уровень обеспечения готовности к инцидентам и непрерывности деятельности организации;
- степень достижения установленных целей организации;
- данные о корректирующих и предупреждающих действиях;
- сведения о действиях, предпринятых в результате реализации рекомендаций предыдущего анализа со стороны руководства;
- информация об изменении угроз, опасностей и обстоятельств, в том числе изменении правовых и иных требований, связанных с риском, угрозами и опасностями;
- рекомендации по улучшению.

Выходными данными для анализа со стороны руководства являются все принятые решения и предпринятые действия, связанные с возможными изменениями политики, целей, задач и других элементов системы IPOCM, совместимых с обязательствами по постоянному улучшению системы IPOCM.

Приложение А
(справочное)

Процедура анализа воздействий на деятельность организации

А.1 Общие положения

Организация должна проанализировать и отнести воздействия инцидентов, приводящих к сбоям, нарушениям и разрушениям ее деятельности, к одному из следующих классов:

a) воздействие инцидента, ограниченное производственными площадями организации;

b) воздействие инцидента, распространившегося за границы производственных площадей организации, охватывающее близлежащие области;

c) воздействие инцидента, распространившегося на обширные области территории с нанесением повреждений и/или ущерба людям, другим организациям, общественной инфраструктуре, системе поставок организации.

А.2 Процедура анализа воздействия инцидента на деятельность организации

В зависимости от особенностей критических видов деятельности, на которые воздействует инцидент, организация должна принять общее решение о мерах восстановления, включая, но не ограничиваясь, следующие итеративные шаги:

a) Определение приемлемого времени простоя и обработки инцидента. Максимальное приемлемое время простоя определяют на основе анализа возможной реакции всех причастных сторон, особенно тех, поставка продукции и услуг которым была приостановлена. Необходимо также оценить затраты и нематериальное воздействие инцидента. Организация должна сравнить воздействие событий с высокой вероятностью реализации, выявленных на этапе сравнительной оценки риска, оценить их общее воздействие на управление организацией и провести количественную оценку длительности периода приостановки деятельности вследствие их воздействия;

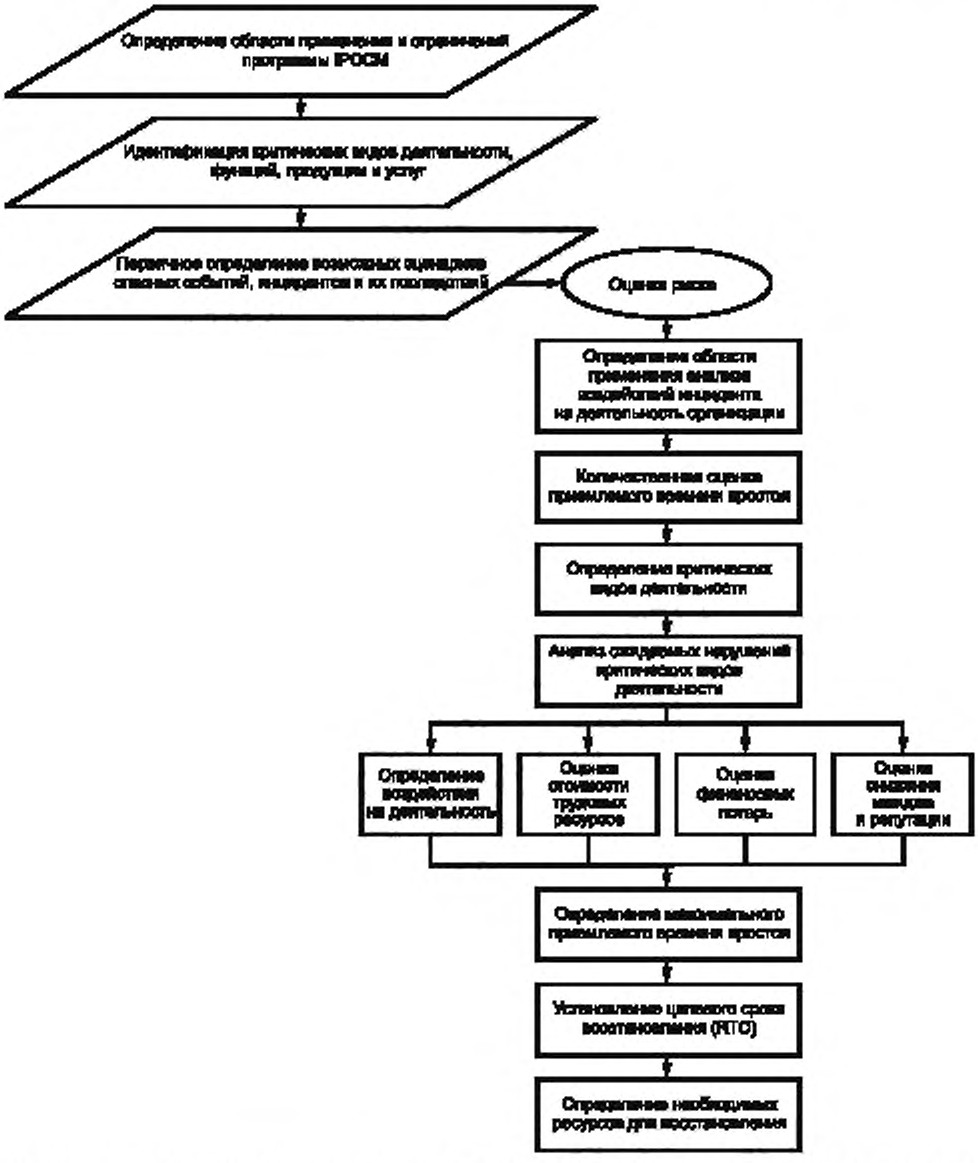
b) определение критических видов деятельности. Организация должна идентифицировать критические виды деятельности, которые являются первоочередными для продолжения жизнедеятельности при реализации опасного события. Организация должна количественно оценить воздействие длительной остановки критических видов деятельности на организацию;

c) анализ возможных нарушений критических видов деятельности. Организация должна оценить степень повреждения критических видов деятельности путем рассмотрения воздействия на различные аспекты деятельности организации, такие как оборудование, персонал, сырье, транспорт, упаковка и потребители. Организация должна сначала рассмотреть возможные повреждения в соответствии с приоритетностью риска. Организация должна учесть остановку своей деятельности, вызванную рассматриваемым повреждением, и реализацию других опасных событий, в том числе неожиданных, произошедших вследствие остановки деятельности,

d) установление целевого срока восстановления (RTO). На основе результатов анализа воздействия на деятельность взаимоотношений с причастными сторонами и социальных задач организация должна установить RTO для восстановления критических видов деятельности путем исследования максимально приемлемой продолжительности остановки критических видов деятельности. Если показатель RTO указан в контрактах, законодательных и нормативных требованиях, организация должна соблюдать такие требования при установлении своего показателя RTO. В случае крупномасштабных разрушений, таких как стихийное бедствие, организация должна осознавать, что сотрудничество с другими организациями при распределении доступных человеческих и материальных ресурсов является существенным фактором для восстановления ее собственной деятельности, потому что собственных ресурсов для восстановления может быть недостаточно или они могут быть недоступны. При проведении количественной оценки продвижения совместных восстановительных работ показатель RTO организации должен быть установлен таким образом, чтобы не препятствовать спасению людей и проведению локальных аварийных работ, и должен обеспечить выполнение совместных мероприятий по восстановлению и оказанию необходимой помощи нуждающимся;

e) идентификация важных ресурсов, существенных для восстановления. На основе анализа ожидаемых нарушений критических видов деятельности организация должна идентифицировать и распределить такие важные ресурсы, как основные средства, оборудование, персонал и информация, существенные для восстановления и возобновления ее деятельности.

Схема процесса анализа воздействий на деятельность организации показана на рисунке А.1.



Примечание — Представленная схема является обобщенной. На практике могут быть использованы другие методы анализа воздействий.

Рисунок А.1 — Схема процесса анализа воздействий инцидентов на деятельность организации

Приложение В
(справочное)

Программа управления неотложными аварийными мероприятиями

В.1 Распределение функций и обязанностей в программе управления неотложными аварийными мероприятиями

При подготовке программы, включая распределение функций и обязанностей специально обученной группы, необходимо (перечень может быть дополнен):

- определить пути эвакуации и пункты сбора;
- предусмотреть обеспечение услуг переводчика;
- предусмотреть обеспечение вспомогательным транспортом и определить его распределение;
- предусмотреть установление связи и обеспечение контактной информацией об аварийных службах и других организациях служб экстренного реагирования;
- определить аварийные способы связи с ближайшими родственниками;
- определить разделение и распределение информации с внутренними и внешними причастными сторонами;
- определить распределение привлеченной рабочей силы или подрядчиков;
- определить управление телефонной справочной службой;
- определить способы реабилитации и помощи людям (материальной и психологической).

В.2 Требования к ресурсам в соответствии с программой неотложных аварийных мероприятий

При разработке программы неотложных аварийных мероприятий должны быть установлены требования к минимальным ресурсам, которые должны включать (перечень может быть дополнен):

- важные записи (в бумажном и электронном виде);
- список контактных лиц;
- процедуры и инструкции по работе;
- процедуры и планы технического восстановления средств информационных технологий (ИТ);
- создание или размещение внешнего хранилища, используемого организацией;
- альтернативное размещение мест работы и офисов (при необходимости);
- полномочия/делегирование полномочий по оплате расходов в условиях инцидента;
- штат квалифицированного персонала, необходимый для каждого вида деятельности;
- инфраструктуру и прикладные приложения ИТ,
- телекоммуникационное сопровождение;
- офисное и специальное оборудование;
- другие ресурсы (вода, электроэнергия и т. д.).

Ресурсы, необходимые для выполнения планов аварийного реагирования и планов неотложных аварийных мероприятий, должны быть точно идентифицированы. Ресурсы должны быть своевременно доступны и пригодны для предназначенного применения. Ограничения при использовании ресурсов должны быть учтены, ответственность за применение ресурсов не должна быть больше, чем за отказ их использовать. Стоимость ресурсов не должна превышать полученную выгоду.

Ресурсы включают в себя, но не ограничены, следующее:

- оборудование, его размещение, количество, доступность, удобство использования, техническое обслуживание и ремонт (например, наличие тяжелых условий работы, необходимость защиты, транспортировки, мониторинга, обеззараживания, применение персонального защитного оборудования);
- запасы (например, медицинские препараты, средства персональной гигиены и др.);
- источники энергии (например, электричество, топливо);
- обеспечение аварийного питания (например, электрогенераторы);
- системы связи;
- пищу и воду,
- техническую информацию;
- одежду и укрытие;
- специализированный персонал (например, медицинские работники, служители религиозных конфессий, добровольцы, персонал аварийных служб, ремонтные рабочие, работники ритуальных организаций, частные подрядчики);
- специализированные группы добровольцев (например, представители Красного Креста, организаций радиолюбительской связи, религиозных и благотворительных организаций);

- добровольные, общественные и аварийные службы поддержки;
- внешние международные, федеральные, региональные и местные агентства.

В.3 Дополнительные элементы программы неотложных аварийных мероприятий

Программа может также включать в себя:

- карты, диаграммы, планы, фотографии и другую информацию, полезную для группы реагирования;
- документированные стратегии ответных мер, согласованные с соответствующими третьими лицами (партнерами по совместному предприятию, подрядчиками, поставщиками и т. д.);
- подробное описание мест размещения оборудования;
- планы мест доступа;
- план управления претензиями, обеспечивающий проверку соответствия страховым и юридическим претензиям к организации или ее претензиям в соответствии с законодательными и договорными требованиями.

Приложение С
(справочное)

Программа обеспечения непрерывности деятельности

С.1 Объединение и документирование программ обеспечения непрерывности деятельности

При объединении и документировании программ обеспечения непрерывности деятельности должны быть идентифицированы следующие элементы (перечень может быть дополнен):

- функции подразделений, виды деятельности и места размещения, упомянутые в плане обеспечения непрерывности деятельности;
- стратегия ответных мер в соответствии с программой обеспечения непрерывности деятельности,
- действия, необходимые для внедрения стратегии ответных мер, действия по обеспечению непрерывности деятельности и ее восстановлению после инцидента;
- специальные точки активации программы обеспечения непрерывности деятельности;
- период выполнения каждого действия в указанных условиях;
- лицо, ответственное за обязательное выполнение этих действий,
- заместители каждого ответственного лица;
- существенные навыки и знания, необходимые для выполнения критических видов деятельности;
- необходимые ИТ, данные и другие применимые технологии, включая резервное копирование информации;
- перечень любой сопроводительной документации или контактной информации, требуемой для выполнения восстановительных действий (включая, но не ограничиваясь, следующее: контактная информация поставщиков, потребителей и персонала по обеспечению ресурсами критических видов деятельности; организационные схемы; требуемая документация в бумажном или электронном виде);
- контактная информация внешних служб поддержки или регистрации (например, партнеров и консультантов, предоставляющих места восстановления, склады, дополнительные места размещения);
- основные или резервные центры управления деятельностью;
- ресурсы и коммунальное обслуживание, требуемые для работы.

С.2 Идентификация оборудования, запасов и взаимодействия в цепи поставок

Организация должна идентифицировать оборудование, запасы и взаимодействие в цепи поставок, которые поддерживают ее критические виды деятельности, и разработать стратегии, обеспечивающие безопасность, бесперебойность работы и систему поставок, включая, но не ограничиваясь, следующее.

- хранение дополнительных запасов в резервных местах размещения,
- заключение соглашений с третьими лицами о поставках в короткие сроки;
- изменение мест поставок «точно в срок» на резервные производственные площади;
- обеспечение наличия и поддержки определенного уровня запасов сырья и материалов на складах или в местах отгрузки;
- перенос предварительных операций на резервные производственные площади;
- сохранение устаревшего оборудования на случай аварийной замены или в качестве резерва;
- принятие дополнительных мер по снижению риска для уникального оборудования или оборудования с длительным сроком выполнения заказа,
- географическую диверсификацию критических процессов;
- дублирование поставщиков;
- резервирование критических систем;
- заключение соглашений с ключевыми поставщиками;
- идентификацию дополнительных поставщиков;
- подготовку предварительных соглашений с партнерами в цепи поставок;
- заключение контрактов с изготовителями оборудования и соглашений о помощи с конкурентами.

С.3 Стратегические варианты программы обеспечения непрерывности деятельности

Варианты включают, но не ограничены:

- передачу или перемещение процесса. Передачу критических видов деятельности либо внутри организации от одного подразделения другому, либо (внешняя передача) третьим лицам, независимо или на основе соглашения о взаимной помощи;
- соглашения о взаимной помощи. Соглашения о взаимной помощи между участниками могут быть эффективным средством получения ресурсов и должны быть разработаны заранее. Соглашения о взаимной помощи должны

быть составлены в письменной форме, юридически грамотными специалистами, утверждены ответственными лицами, должны распределять ответственность и содержать финансово-экономические положения. Соглашение о взаимной помощи может включать в себя совместные соглашения о помощи, договоренности между руководителями или другие положения, обычно используемые для разделения обеспечения ресурсами;

- временная работа. Резервный вариант передачи процесса. Передача может быть выполнена путем внедрения различных способов работы, которые могут привести к тем же самым или подобным, но приемлемым результатам. Такая работа может занять больше времени и/или быть более трудоемкой (например, физический труд вместо автоматизированного). По этим причинам такие виды работ следует рассматривать как краткосрочную альтернативу, они должны быть разрешены стратегией при плановом восстановлении нормальной деятельности организации;

- изменение, приостановка или завершение. При некоторых обстоятельствах могут быть уместны изменение, приостановка или прекращение производства продукции, оказания услуги, вида деятельности или работы процесса. Эту возможность стоит рассматривать в случае, когда это не противоречит достижению целей организации, обязательным требованиям соответствия, ожиданиям причастных сторон. Такой подход часто рассматривают, если продукция или услуга имеют ограниченный срок годности;

- страхование. Покупка страховых обязательств может обеспечить небольшую финансовую компенсацию некоторых потерь, однако не покрывает все затраты (например, незастрахованные события, бренд, репутация, доверие причастных сторон, доля рынка и последствия для человека). Одно применение действий только по финансовому регулированию, как правило, не позволяет удовлетворить ожидания причастных сторон. Страхование, как правило, используют вместе с одной или несколькими другими стратегиями.

Приложение D
(справочное)

Внедрение системы обеспечения готовности к инцидентам и непрерывности деятельности

D.1 Элементы

Для успешного внедрения системы IPOCM необходимо (список может быть дополнен):

- признание высшим руководством организации значимости системы IPOCM, необходимости ее поддержки и признание IPOCM неотъемлемой частью системы менеджмента организации;
- опубликование программного заявления о политике в области IPOCM, утвержденной и одобренной высшим и исполнительным руководством организации;
- понимание персоналом условий внутри и вне организации,
- назначение представителя из числа высшего руководства, ответственного за выполнение политики организации в области IPOCM;
- создание консультационного процесса с руководителями среднего звена, наблюдателями и исполнительным персоналом организации относительно выполнения политики в области IPOCM, который обеспечивает их вовлеченность в программу,
- назначение владельцев процессов IPOCM по всей организации (не только для обслуживания оборудования или ИТ) и лидеров IPOCM по ключевым направлениям деятельности организации;
- проведение и организация обучения персонала и его участия в учениях.

Кроме того, возможны:

- интеграция IPOCM в процессы мотивации и вознаграждений в организации;
- интеграция IPOCM в производственные процессы, процесс оценки и иные процессы;
- включение функций подотчетности, обязанностей и полномочий в области IPOCM, а также требуемых навыков персонала в должностные инструкции организации,
- включение вопросов IPOCM в повестки дня совещаний организации;
- активное участие выгодополучателей, потребителей и высшего руководства в учениях и проверках по IPOCM;
- внедрение программы обеспечения осведомленности ключевых поставщиков и дистрибьюторов информацией об IPOCM и установление у них соответствующих внутренних процессов;
- разработка процессов IPOCM для проведения мониторинга эффективности образования, обучения и оценки осведомленности об IPOCM персонала организации.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
Руководство ИСО 73:2009	IDT	ГОСТ Р 51897—2011/Руководство ИСО 73:2009 «Менеджмент риска. Термины и определения»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] BS 25999-1:2006 Business continuity management — Code of practice, BSI British Standards[1)]

[2] HB 221:2004 *Business continuity management*, Standards Australia/Standards New Zealand, ISBN 0-7337-6250-6

[3] SI 24001:2007 Security and continuity management systems — Requirements and guidance for use, Standards Institution of Israel

[4] NFPA 1600:2004 Standard on disaster/emergency management and business continuity programs, National Fire Protection Association (USA)

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

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

[1)] Стандарту Великобритании BS 25999-1.2006 соответствует стандарт ГОСТ Р 53647.1—2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство».

УДК 658:562.014:006.354 ОКС 03.100.01 Т59

Ключевые слова: критические виды деятельности, кризис, бедствие, нарушение деятельности, авария, опасность, анализ воздействия, инцидент, управление инцидентом, уменьшение последствий, непрерывность деятельности, управление непрерывностью деятельности

Редактор *А.Д. Стулова*
Технический редактор *В.Н. Прусакова*
Корректор *А.С. Черноусова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 06.08.2012. Подписано в печать 30.08.2012. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,60. Тираж 124 экз. Зак. 740.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

Поправка к ГОСТ Р 53647.4—2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности

В каком месте	Напечатано	Должно быть
Предисловие, пункт 3	№ 697-ст	№ 679-ст

(ИУС № 2 2013 г.)

gost.e-ecolog.ru