ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53647.1— 2009

МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ БИЗНЕСА

Часть 1

Практическое руководство

BS 25999-1:2006
Business continuity management. Part 1: Code of practice
(IDT)

Издание официальное

БЗ 9—2009/559

Москва
Стандартинформ
2011

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 стандарта, указанного в разделе 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 998-ст

4 Настоящий стандарт идентичен национальному стандарту Великобритании BS 25999-1:2006 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство» (BS 25999-1:2006 «Business continuity management. Part 1: Code of practice»)

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, 2011

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 Термины и определения 1
3 Краткий обзор менеджмента непрерывности бизнеса 4
4 Политика в области непрерывности бизнеса 7
5 Управление программой МНБ 8
6 Анализ непрерывности бизнеса организации 11
7 Определение стратегии МНБ 15
8 Разработка и внедрение ответных мер МНБ 19
9 Применение, поддержка и анализ МНБ 27
10 Внедрение МНБ в культуру организации 30
Библиография 33

Введение

Требования настоящего стандарта следует применять наряду с нормативно-правовыми актами в области обеспечения безопасности, которые имеют обязательную силу на территории Российской Федерации. Нормативно-правовые нормы РФ и обязательные процедуры в области обеспечения безопасности должны быть интегрированы в систему менеджмента непрерывности бизнеса организации. По возможности следует избегать дублирования в документации по обеспечению непрерывности бизнеса действующих документов организации.

В качестве синонимов термина «менеджмент непрерывности бизнеса» часто используют термины «управление непрерывностью бизнеса», «управление непрерывностью деятельности», «управление бесперебойностью работы». Выбор термина зависит от потребностей организации и требований ее причастных сторон.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МЕНЕДЖМЕНТ НЕПРЕРЫВНОСТИ БИЗНЕСА

Часть 1

Практическое руководство

Business continuity management.
Part 1. Code of practice

Дата введения — 2010—12—01

1 Область применения

Настоящий стандарт устанавливает процессы, принципы и терминологию менеджмента непрерывности бизнеса (МНБ). Целью настоящего стандарта является установление основных положений для понимания, разработки и внедрения менеджмента непрерывности бизнеса в организации и обеспечения доверия к продукции или услугам организации со стороны потребителей и партнеров. Стандарт может помочь организации последовательно измерять и оценивать свою способность к обеспечению непрерывности бизнеса.

Настоящий стандарт предназначен для использования специалистами, ответственными за коммерческие операции и/или предоставление услуг, начиная от высшего руководства организации до сотрудников всех уровней; от организаций, работающих на национальных рынках, до транснациональных корпораций; от индивидуальных предпринимателей, организаций малого и среднего бизнеса, до организаций, в которых трудятся тысячи человек. Таким образом, стандарт может быть применен любым лицом, ответственным в организации за любую операцию и обеспечение ее непрерывности.

Настоящий стандарт не может быть использован для планирования действий в чрезвычайной ситуации, поскольку этот вопрос регламентируется соответствующими нормами и правилам МЧС и законодательством РФ в целом.

Примечание — Независимо от затраченных усилий и вложенных инвестиционных ресурсов в менеджмент непрерывности бизнеса, организация все же может столкнуться с непредвиденным инцидентом или комбинацией непредвиденных инцидентов.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

2.1 **деятельность** (activity): Процесс или система процессов, осуществляемых организацией с целью производства одного или более видов продукции, оказания услуг или их поддержки.

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

2.2 **непрерывность бизнеса** (business continuity): Стратегическая и тактическая способность организации планировать свою работу в случае инцидентов и нарушения ее деятельности, направленная на обеспечение непрерывности деловых операций на установленном приемлемом уровне.

2.3 **менеджмент непрерывности бизнеса; МНБ** (business continuity management; BCM): Полный процесс управления, предусматривающий идентификацию потенциальных угроз и их воздействие на деятельность организации, который создает основу для повышения устойчивости организации к инцидентам и направлен на реализацию эффективных ответных мер против них, что обеспечивает защиту

Издание официальное

интересов ключевых причастных сторон, репутации организации, ее бренда и деятельности, добавляющей ценность.

Примечание — Менеджмент непрерывности бизнеса включает в себя управление восстановлением или продолжением деятельности организации в случае нарушений в ее работе, а также общей программой обеспечения непрерывности бизнеса организации путем обучения, практического применения и анализа непрерывности бизнеса, разработкой и актуализацией планов непрерывности бизнеса.

2.4 **жизненный цикл менеджмента непрерывности бизнеса** (business continuity management lifecycle): Совокупность действий по обеспечению непрерывности бизнеса, которые охватывают все аспекты и элементы программы менеджмента непрерывности бизнеса.

Примечание — Этапы жизненного цикла менеджмента непрерывности бизнеса приведены на рисунке 1.

2.5 **программа менеджмента непрерывности бизнеса** (business continuity management programme): Процесс постоянного менеджмента, поддерживаемый со стороны высшего руководства и обеспечиваемый необходимыми ресурсами, направленный на осуществление необходимых мер по идентификации воздействия потенциальных потерь, поддержку жизнеспособной стратегии непрерывности бизнеса и планов восстановления бизнеса, а также на обеспечение непрерывности производства продукции и оказания услуг путем обучения и проведения учений, внедрения, анализа и поддержания в рабочем состоянии непрерывности бизнеса организации.

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

2.7 **стратегия непрерывности бизнеса** (business continuity strategy): Способы обеспечения непрерывности бизнеса в организации, направленные на восстановление и продолжение ее деятельности в случае инцидентов, вызывающих нарушение в ее работе.

2.8 **анализ воздействия на бизнес** (business impact analysis): Процесс исследования функционирования бизнеса и последствий воздействия на него разрушающих факторов.

2.9 **гражданская чрезвычайная (аварийная) ситуация** (civil emergency): Событие или ситуация, представляющие серьезную угрозу для благосостояния людей, окружающей среды в конкретной местности и/или безопасности страны в целом.

2.10 **последствие** (consequence): Результат инцидента, который может повлиять на достижение целей организации.

Примечания

1 Для каждого инцидента должно быть проведено ранжирование последствий.

2 Последствия могут быть определенными и неопределенными, а также могут иметь позитивное или негативное воздействие на достижение целей организации.

2.11 **анализ эффективности затрат** (cost-benefit analysis): Финансово-экономический метод, применение которого позволяет оценить затраты на МНБ, сопоставить их с полученной от его внедрения выгодой.

Примечание — Выгода может быть определена с позиции финансов, репутации, производства продукции, предоставления услуг, выполнения обязательных требований и т.п.

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

2.13 **нарушение 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) событием или явлением.

2.14 **планирование действий в аварийных ситуациях** (emergency planning): Разработка и поддержание в рабочем состоянии согласованных процедур организации, направленных на предупреждение, уменьшение масштабов воздействия, смягчение последствий и принятие других мер в случае возникновения аварийных и/или чрезвычайных ситуаций.

2.15 **учения** (exercise): Мероприятия, в процессе которых частично или полностью проходит отработка действий (репетиция), предусмотренных планом(ами) обеспечения непрерывности бизнеса,

направленные на то, чтобы план(ы) содержал(и) необходимую информацию и при выполнении приводил(и) к запланированным результатам.

Примечание — Учения обычно включают в себя инициирование процедуры непрерывности бизнеса, но чаще объявленную или необъявленную имитацию инцидента нарушения непрерывности бизнеса, в процессе которого участники инсценируют возможную ситуацию с целью оценки потенциальных проблем, связанных с их преодолением до наступления реального инцидента.

2.16 **выгоды** (gain): Положительные последствия.

2.17 **воздействие** (impact): Оцененные последствия для конкретного случая.

2.18 **инцидент** (incident): Ситуация, которая может произойти и привести к нарушению деятельности организации, разрушениям, потерям, чрезвычайной ситуации или кризису в бизнесе.

2.19 **план управления инцидентом** (incident management plan): Точно установленный и документально оформленный план действий, предназначенный для использования при возникновении инцидента, который обычно охватывает вовлеченный персонал, необходимые ресурсы и действия, которые должны быть выполнены в процессе управления инцидентом.

2.20 **инициирование работы** (invocation): Объявление о приведении в действие плана обеспечения непрерывности бизнеса организации с целью обеспечения бесперебойности поставки ключевой продукции и/или услуг.

2.21 **возможность реализации** (likelihood): Шансы реализации события, которые определены, измерены и/или оценены объективно или субъективно в терминах общих описаний (маловероятно, вероятно, почти наверняка), частоты или вероятности.

Примечание — Возможность может быть выражена качественно или количественно.

2.22 **потери** (loss): Негативные последствия.

2.23 **максимально приемлемый период нарушения** (maximum tolerable period of disruption): Период времени, по истечении которого существует угроза окончательной потери жизнеспособности организации в том случае, если поставка продукции и/или предоставление услуг не будут возобновлены.

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

Пример — Компания, корпорация, фирма, предприятие, учреждение, благотворительная организация, предприятие розничной торговли, ассоциация, а также их подразделения или комбинация из них.

Примечание

1 Распределение обычно является упорядоченным.

2 Организация может быть государственной или частной

[ИСО 9000:2005].

2.25 **продукция и услуги** (products and services): Результат деятельности организации, который она предоставляет своим потребителям, получателям и причастным сторонам, например промышленные товары, страхование, медицинское обслуживание и др.

2.26 **целевой срок восстановления** (recovery time objective; RTO): Время, запланированное для:

- возобновления производства продукции или оказания услуг после инцидента;
- возобновления деятельности после инцидента;
- восстановления информационной системы и/или прикладных программ после инцидента.

Примечание — Целевой срок восстановления должен быть меньше, чем максимально приемлемый период нарушения.

2.27 **устойчивость** (resilience): Способность организации противостоять воздействию инцидента.

2.28 **риск** (risk): Сочетание вероятности события и масштабов его последствий, а также его воздействие на достижение целей организации.

Примечание

1 Термин «риск» обычно используют только тогда, когда существует возможность негативных последствий.

2 В некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата.

3 Применительно к безопасности см. [2].

[ИСО/МЭК Руководство 73:2009]

4 Риск обычно определяют по отношению к конкретной цели, поэтому для нескольких целей существует возможность оценить риск для каждого источника опасности.

5 В качестве количественной оценки риска часто используют сумму произведений последствий на вероятность соответствующего опасного события. Однако для количественной оценки диапазона возможных последствий необходимо знание распределения вероятностей. Кроме того, может быть использовано стандартное отклонение.

2.29 **допустимый совокупный риск** (risk appetite): Величина совокупного риска, который организация готова допустить или которому готова подвергнуться в любой момент времени.

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

2.31 **менеджмент риска** (risk management): Структурированная разработка и применение культуры, политики, процедур и методов менеджмента к задачам идентификации, анализа, оценки и обработки риска.

2.32 **причастная сторона** (stakeholder): Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечание

1 Лицо, принимающее решение, также является причастной стороной.

2 Причастная сторона включает в себя заинтересованную сторону, но имеет более широкое значение, чем заинтересованная сторона

[ИСО/МЭК Руководство 73:2009].

2.33 **высшее руководство** (top management): Лицо или группа работников, осуществляющих направление деятельности и управление организацией на высшем уровне

[ИСО 9000:2005, статья 3.2.7]

Примечание — Высшее руководство, особенно в большой транснациональной корпорации, не всегда может быть непосредственно вовлечено в МНБ, однако в этом случае высшее руководство несет ответственность через утвержденный в организации порядок соподчиненности. В малой организации высшее руководство может быть владельцем этого процесса.

3 Краткий обзор менеджмента непрерывности бизнеса

3.1 Определение МНБ

Менеджмент непрерывности бизнеса — это процесс, связанный с собственниками бизнеса и активизирующий работу других процессов, в рамках которого устанавливают стратегические цели и структуру управления в соответствии с целями организации в области непрерывности бизнеса, которые:

- активно улучшают устойчивость организации, обеспечивают стабильность ее способности достигать основные поставленные цели;
- обеспечивают отработанный метод восстановления способности организации поставлять ключевые продукцию и услуги на установленном уровне в пределах согласованного времени после возникновения нарушения деятельности;
- обеспечивают верифицированную способность организации управлять нарушениями функционирования и защищать ее бизнес, репутацию, конкурентоспособность и бренд.

Отдельные процессы непрерывности бизнеса могут изменяться в зависимости от размеров, структуры и назначения организации, однако основные принципы остаются постоянными для организаций некоммерческого, частного или государственного сектора, независимо от их размера, области или сложности деятельности.

3.2 МНБ и стратегия организации

Все организации, большие или малые, имеют свои цели и задачи, такие как обеспечение роста и развития, расширение сферы услуг и/или приобретение других организаций. Эти цели и задачи обычно реализуются путем выполнения стратегических планов и достижения кратко-, средне- и долгосрочных установленных показателей организации. На самом высоком уровне понимания МНБ организация обеспечивает достижение этих целей и задач в условиях возникновения угрозы неожиданного нарушения ее деятельности.

Инциденты могут быть различны по характеру и размерам последствий. Последствия могут привести к потере жизни людей, активов или доходов, либо неспособности поставлять продукцию и оказывать услуги, от которых порой зависит выполнение стратегий, сохранение репутации или даже само существование организации.

В рамках МНБ необходимо признать стратегическое значение известных причастных сторон. Часто последствия нарушений деятельности организации разворачиваются во времени и могут появиться новые причастные стороны, оказывающие прямое воздействие на возможную степень и масштабы повреждений и ущерба. Например, суммарный объем проблем может оказывать сильное давление на организацию в период нарушений деятельности или разрушений.

Решение всех этих проблем представляет собой стратегические интересы организации.

3.3 Взаимосвязь МНБ с менеджментом риска

МНБ является дополнительной структурой по отношению к менеджменту риска, которая позволяет осознать существующие опасности для деятельности и бизнеса организации, а также последствия возникновения опасных событий.

Менеджмент риска ориентирован на управление риском по ключевым вопросам поставки продукции и предоставления услуг организацией. Производство продукции и оказание услуг могут быть разрушены широким спектром разнообразных инцидентов, многие из которых трудно не только спрогнозировать, но и проанализировать их причины.

Ориентируясь на воздействие нарушений, в процессе МНБ идентифицируют продукцию и услуги, от которых зависит выживание организации, а также необходимые условия для продолжения деятельности и непрерывности выполнения организацией своих обязательств. Внедрение МНБ позволит организации еще до реализации инцидента выявить необходимые ответные меры для защиты людей, производственных площадей, технологий, информации, системы поставок, причастных сторон и репутации организации.

На этом этапе организация может получить реальное представление о том, как и когда произойдет нарушение ее деятельности. Это необходимо для достижения уверенности в том, что организация способна справиться с любыми последствиями без недопустимой задержки поставки продукции или оказания услуг.

Организация, которая принимает соответствующие меры по МНБ в конкретной ситуации, может использовать в своих интересах дополнительные возможности даже при высоком уровне риска.

3.4 Причины применения организацией МНБ

МНБ является важным элементом успешного управления бизнесом и предпринимательской дальновидности.

Руководители и владельцы организации несут ответственность за поддержание способности организации функционировать без перебоев. Организация постоянно берет на себя различные обязательства, в том числе по поставке продукции и оказанию услуг, заключает договоры и совершает иные действия, направленные на рост доходов и достижение ожидаемых результатов. У всех организаций существуют моральные и социальные обязанности, особенно если они обеспечивают работу в чрезвычайных ситуациях или оказывают государственные или благотворительные услуги. В некоторых случаях для организаций установлены законодательные или обязательные требования по применению МНБ.

Нормальное функционирование любых видов деятельности организации может быть нарушено посредством воздействия на него таких разрушающих факторов, как технологические отказы, наводнения, прорыв коммуникаций и терроризм. МНБ обеспечивает способность реагировать надлежащим образом на текущее нарушение деятельности организации, защищая благосостояние и безопасность конкретных людей и общества в целом.

МНБ целесообразно рассматривать не как дорогостоящий процесс планирования, а как процесс, добавляющий ценность организации.

3.5 Выгоды от реализации эффективной программы МНБ

Организация может получить следующие выгоды от реализации эффективной программы МНБ (перечень может быть дополнен):

- способность активно идентифицировать нарушения работы производственных процессов;
- возможность применить эффективные ответные меры на нарушения и тем самым снизить до минимума отрицательные воздействия на организацию;
- способность управлять неисследованным риском;
- развитие способности и поощрение к совместной работе междисциплинарных групп специалистов различных подразделений;
- возможность продемонстрировать предусмотренные ответные меры на нарушение деятельности организации во время учений по МНБ;
- возможность повысить репутацию;
- возможность создания конкурентных преимуществ путем демонстрации способности организации поддерживать непрерывность поставок.

3.6 Результаты внедрения эффективной программы МНБ

Результатами внедрения эффективной программы МНБ являются:

- идентификация, защита от негативных воздействий и обеспечение непрерывной поставки ключевых продукции и услуг;
- способность управлять инцидентом, достаточная для обеспечения эффективных ответных мер в конкретной ситуации;
- разработка, документирование и понимание организацией себя и своих отношений с другими организациями, соответствующими законодательными и правительственными структурами, органами местного самоуправления и аварийными службами;
- обучение персонала выполнению эффективных ответных мер в случае инцидента или нарушений деятельности организации;
- понимание и установление требований причастных сторон;
- обеспечение персонала необходимой поддержкой и средствами обмена информацией в случае возникновения инцидентов и нарушений деятельности организации;
- дополнительная защита цепи поставок организации;
- дополнительная защита репутации организации;
- сохранение устойчивости организации при выполнении обязательных и законодательных требований.

3.7 Элементы жизненного цикла менеджмента непрерывности бизнеса

Жизненный цикл МНБ включает шесть элементов (см. рисунок 1). Элементы жизненного цикла могут быть внедрены организациями различных размеров и секторов экономики: государственными, частными, некоммерческими, образовательными, производственными и т.д. Область применения и структура программы МНБ могут быть различны. Затраченные на внедрение МНБ усилия зависят от индивидуальных потребностей организации, однако в любом случае эти шесть существенных элементов должны быть выполнены.



Рисунок 1 — Этапы жизненного цикла менеджмента непрерывности бизнеса

a) управление программой МНБ (см. раздел 5)

Управление программой МНБ дает возможность установить и поддерживать способность к непрерывности бизнеса способом, наиболее соответствующим размеру и сложности организации.

b) анализ непрерывности бизнеса организации (см. раздел 6)

Деятельность, связанная с анализом непрерывности бизнеса организации, которая направлена на получение информации, позволяющей расставить приоритеты для продукции и услуг организации и определить актуальность действий МНБ. На основе анализа непрерывности бизнеса организация может установить требования, позволяющие выбрать стратегии МНБ.

c) определение стратегии МНБ (см. раздел 7)

Данный элемент позволяет провести оценку нескольких стратегий. Стратегия МНБ позволяет выбрать соответствующие ответные меры на негативные события для каждой продукции или услуги таким образом, чтобы организация могла продолжать поставлять эту продукцию и оказывать услуги:

- на приемлемом уровне;
- в пределах приемлемого периода

в процессе и после нарушения функционирования ее деятельности.

Выбор стратегии следует осуществлять с учетом способности организации к восстановлению (устойчивости) и принимать во внимание контрмеры, уже применяемые в организации.

d) разработка и внедрение в МНБ ответных мер на негативное событие (см. раздел 8)

Разработка и внедрение в МНБ ответных мер на негативное событие приводит к созданию структуры менеджмента и управления при возникновении инцидента, планов непрерывности бизнеса и планов восстановления бизнеса, подробно описывающие ответные меры, которые должны быть предприняты в процессе и после инцидента для поддержки или восстановления деятельности организации.

Комментарий к 3.7 d) —Термин «инцидент» использован в настоящем стандарте для отражения масштаба событий от малого до большого, которые могут повлиять на организацию. Один или несколько инцидентов могут привести к серьезным нарушениям способности организации выполнять свои обязательства. При правильном управлении ситуация в условиях инцидента не может развиться в кризис. Однако некоторые события могут вызвать такие серьезные нарушения планов по достижению целей организации, что их возникновение можно считать кризисом.

Размах инцидента может превысить степень готовности организации, даже если ответные меры на ожидаемый уровень нарушений ее деятельности были тщательно разработаны. Поэтому крайне важно, чтобы структуры процесса менеджмента и вспомогательных процессов гибко изменялись согласно обстоятельствам. План обеспечения непрерывности бизнеса никогда не заменяет взвешенного и компетентного управленческого решения руководства.

e) меры по применению, поддержке и анализу МНБ (см. раздел 9)

Меры по применению, поддержке, анализу и аудиту МНБ делают организацию способной:

- демонстрировать степень полноты, актуальности и точности ее стратегий и планов;
- выявлять возможности для улучшения своей деятельности.

f) внедрение МНБ в культуру организации (см. раздел 10)

Внедрение МНБ в культуру организации позволяет этой системе стать частью наиболее ценных активов организации, что вызывает доверие всех причастных сторон в способности организации справляться с возникающими трудностями и нарушениями функционирования.

4 Политика в области непрерывности бизнеса

4.1 Краткий обзор

4.1.1 Политика МНБ определяет следующие процессы:

- организационную деятельность по установлению способности к непрерывности бизнеса;
- непрерывный менеджмент и поддержку способности к обеспечению непрерывности бизнеса.

4.1.2 Организационная деятельность включает в себя установление требований и полного цикла непрерывности бизнеса от проектирования, построения, внедрения до первоначального применения проверки способности организации к непрерывности бизнеса.

4.1.3 Непрерывная поддержка и менеджмент включают в себя: внедрение непрерывности бизнеса в организации; проведение регулярных учений по применению планов обеспечения непрерывности бизнеса; актуализацию и обмен информацией в соответствии с этим планом, особенно, если происходят существенные изменения в производственных площадях, персонале, организационной структуре, производственных и технологических процессах или рыночных условиях.

Комментарий к 4.1 — Целями установления политики непрерывности бизнеса являются:

- *обеспечение согласованности, управляемости и выполнимости всех действий МНБ;*

- достижение способности к непрерывности бизнеса, которая отвечает изменяющимся потребностям бизнеса и соответствует размеру, сложности и характеру организации;

- установление четко определенной структуры для непрерывной способности организации к МНБ.

4.2 Цели применения

Политика в области МНБ должна соответствовать природе, масштабу, сложности, географии и критичности видов деятельности организации, отражать ее культуру, взаимосвязанные области и деловую среду. Политика в области МНБ определяет требования к процессу обеспечения непрерывности бизнеса и должна обеспечивать соответствие действий в области непрерывности бизнеса потребностям организации в случае возникновения инцидента, а также развитие способности организации к непрерывности бизнеса. Способность к МНБ должна быть интегрирована в деятельность организации по управлению изменениями таким образом, чтобы способность к непрерывности бизнеса способствовала росту номенклатуры продукции и объема услуг.

4.3 Разработка политики непрерывности бизнеса

Организация должна разработать политику в области непрерывности бизнеса, которая отвечает целям МНБ организации. Первоначально она может быть выпущена в виде заявления о намерениях, утвержденного на самом высоком уровне организации, которое может быть доработано, расширено и улучшено по мере развития в организации МНБ.

Политика в области непрерывности бизнеса должна обеспечивать организации документированные принципы и цели, к которым должна стремиться организация и на соответствие которым необходимо проводить измерение способности к непрерывности бизнеса. Политика в области МНБ должна быть утверждена на самом высоком уровне организации, например, генеральным директором или председателем совета директоров.

При разработке политики в области МНБ организация должна определить:

- области применения МНБ в организации;
- необходимые ресурсы для МНБ;
- принципы, руководящие указания и минимальное количество стандартов организации в области МНБ;
- ссылки на соответствующие стандарты, инструкции или другие нормативные акты организации, которые должны быть включены в документы или могут быть использованы как точки отсчета.

Организация должна поддерживать в рабочем состоянии политику, стратегии, планы и решения в области МНБ и проводить их анализ через запланированные интервалы времени в соответствии с потребностями организации.

В политике организации должны быть точно установлены все применяемые ограничения или исключения в области МНБ, например исключения по географическому признаку или по виду продукции.

4.4 Область применения МНБ

Высшее руководство должно определить область применения МНБ путем идентификации ключевой продукции и услуг, которые способствуют достижению установленных целей и выполнение обязательных и законодательных требований организации. Определение области применения МНБ должно в целом быть совместимо с анализом воздействия на бизнес (см. 6.2).

4.5 Услуги сторонних организаций[1)]

Если продукция, услуги или деятельность были произведены с привлечением сторонних организаций, риск, связанный с продукцией, услугой или деятельностью, несет организация. Следовательно, организация должна убедиться, что ее ключевые поставщики и привлекаемые сторонние организации (партнеры) принимают эффективные меры по МНБ в своей деятельности. Одним из методов выполнения этого требования является получение свидетельства по результатам аудита, внедрения и осуществления планов обеспечения непрерывности бизнеса, программ учений и поддержки МНБ ключевых поставщиков.

5 Управление программой МНБ

Управление программой МНБ — это основа процесса МНБ. Эффективное управление программой устанавливает общий подход к непрерывности бизнеса, принятый в организации.

Участие высшего руководства является ключевым фактором для обеспечения правильного введения, соответствующей поддержки и установки процесса МНБ как части культуры организации.

[1)] Аутсорсинг (Прим. — пер.).



5.1 Краткий обзор

Выполнение программы МНБ обеспечивает достижение целей, установленных политикой непрерывности бизнеса (см. 4.3). Управление программой МНБ включает три шага:

- распределение ответственности и полномочий (см. 5.2);
- осуществление непрерывности бизнеса в организации (см. 5.3);
- постоянный менеджмент непрерывности бизнеса (см. 5.4).

5.2 Распределение ответственности и полномочий

5.2.1 Высшее руководство организации должно назначить:

- лицо из числа высшего руководства, наделенное соответствующими полномочиями, ответственное за политику в области МНБ и ее внедрение;
- одного или несколько лиц, ответственных за выполнение и поддержку программы МНБ.

Комментарий к 5.2.1 — Лица, занятые в процессе выполнения и поддержки программы непрерывности бизнеса, могут участвовать во многих областях деятельности организации в зависимости от ее размера, масштаба и сложности. Существенно, однако, что лицо, наделенное соответствующими полномочиями (например, собственник, председатель совета директоров или генеральный директор), должно нести полную ответственность за МНБ и являться непосредственно ответственным за обеспечение длительного успеха реализации этой способности.

5.2.2 Если позволяет соподчиненность организационной структуры, высшее руководство может назначить уполномоченного представителя в соответствии с функциями или местом расположения бизнеса для помощи в создании программы МНБ.

Обязанности, подотчетность, ответственность и полномочия персонала должны быть установлены в рабочих и должностных инструкциях.

Анализ этих обязанностей необходимо проводить в процессе аудита организации.

Надлежащее выполнение обязанностей в области обеспечения непрерывности бизнеса может быть усилено путем их включения в политику организации в области аттестации, компетентности и поощрения персонала.

Комментарий к 5.2.2 — В крупных организациях может возникнуть потребность в создании группы представителей по непрерывности бизнеса с различными зонами ответственности и полномочиями. В малых организациях ответственность за непрерывность бизнеса может быть возложена на одного или нескольких сотрудников.

5.3 Осуществление непрерывности бизнеса в организации

5.3.1 Деятельность по выполнению программы непрерывности бизнеса должна включать в себя проектирование, разработку и внедрение программы.

Организация должна осуществлять следующие действия:

- обмен информацией о программе с причастными сторонами;
- организацию и/или обеспечение соответствующего обучения персонала;
- проведение учений по обеспечению непрерывности бизнеса (см. раздел 9).

5.3.2 Организация может адаптировать признанные методы менеджмента для обеспечения эффективного управления программой непрерывности бизнеса.

5.4 Постоянный менеджмент непрерывности бизнеса

5.4.1 Краткий обзор

Действия по постоянному менеджменту должны обеспечивать внедрение процесса непрерывности бизнеса в организации. Каждый компонент способности организации к непрерывности бизнеса должен быть проанализирован, внедрен и актуализирован через запланированные интервалы времени. Кроме того, принимаемые меры и планы по непрерывности бизнеса должны также подвергаться анализу и актуализации всякий раз, когда происходят существенные изменения в рабочей среде, персонале, производственных и технологических процессах организации, а также в случаях, когда при внедрении мероприятий или возникновении инцидента в каких-либо областях деятельности организации выявлены недостатки.

5.4.2 Непрерывная поддержка МНБ в рабочем состоянии

Вне зависимости от обеспечения МНБ соответствующими ресурсами существуют действия, которые следует непрерывно выполнять. К таким действиям относятся:

- определение области применения, распределение ответственности и полномочий для МНБ;
- назначение соответствующего лица или группы лиц для управления непрерывной поддержкой к МНБ;
- поддержка актуальности программы непрерывности бизнеса путем внедрения передового опыта;
- продвижение непрерывности бизнеса на всех уровнях и во всех подразделениях организации и за ее пределами (если применимо);
- управление программой учений;
- проведение регулярного анализа и обновления МНБ через запланированные интервалы времени, включая анализ и актуализацию оценок риска и анализа воздействия на бизнес;
- поддержание в рабочем состоянии документации МНБ в соответствии с размером и сложностью организации (см. 5.5);
- мониторинг способности организации к обеспечению непрерывности бизнеса;
- управление затратами на обеспечение непрерывности бизнеса;
- установление и мониторинг управления изменениями и системы обеспечения преемственности.

5.5 Документация МНБ

Лица, ответственные за поддержание в рабочем состоянии непрерывности бизнеса, должны создать и поддерживать в рабочем состоянии документацию в области непрерывности бизнеса. Эта документация должна включать в себя:

a) политику в области МНБ:
   - положение об области применения МНБ,
   - область применения МНБ;
b) анализ воздействия на бизнес (АВБ);
c) оценку риска;
d) стратегию (и) МНБ;
e) программу обеспечения компетентности в области непрерывности бизнеса;
f) программу обучения в области непрерывности бизнеса;
g) планы управления инцидентом(ами);
h) планы обеспечения непрерывности бизнеса;
i) планы восстановления бизнеса;
j) график и программу учений, а также отчетность об их проведении;
k) соглашения и договоры об уровне работоспособности системы МНБ.

6 Анализ непрерывности бизнеса организации



Цель данного элемента жизненного цикла МНБ состоит в обеспечении понимания и анализа организацией непрерывности своего бизнеса путем идентификации ее ключевой продукции и услуг, а также поддерживающих их критических видов деятельности и ресурсов. Этот элемент должен обеспечивать соответствие программы МНБ установленным целям организации, а также обязательным и законодательным требованиям.

6.1 Введение

6.1.1 Анализ непрерывности бизнеса организации основан на:

- идентификации целей организации, обязательств перед причастными сторонами, установленных законодательных и обязательных требований, особенностей рабочей среды и условий функционирования организации;

- идентификации видов деятельности, активов и ресурсов организации (включая внешние), которые поддерживают поставку продукции и услуг;

- оценке воздействий и долговременных последствий отказов, отсутствия активов и ресурсов при выполнении вышеуказанных видов деятельности (см. 6.2);

- идентификации и оценке осознанных угроз, которые могут нарушить производство и поставку ключевой продукции и услуг организации, поддерживающие их критические виды деятельности, активы и ресурсы (см. 6.5).

6.1.2 Для организации важно понять:

a) взаимосвязь ее видов деятельности;

b) любую зависимость деятельности организации от внешних организаций, равно как и других сторон от деятельности организации.

6.2 Анализ воздействия на бизнес (АВБ)

6.2.1 Организация должна определить и документально оформить воздействие нарушений на деятельность, поддерживающую ее ключевые продукцию и услуги. Этот процесс обычно называют анализом воздействия на бизнес.

6.2.2 Для каждого вида деятельности, поддерживающей производство и поставку ключевой продукции и услуг, в рамках области применения программы МНБ, организация должна:

a) оценить воздействие нарушений деятельности, которые могут произойти по прошествии длительного времени;

b) установить максимально приемлемый период нарушения каждого вида деятельности путем идентификации:

- максимального периода времени после начала нарушения, в пределах которого деятельность должна быть возобновлена;
- минимального уровня выполнения этой деятельности после ее возобновления,
- периода времени, в пределах которого должен быть возобновлен нормальный уровень осуществления деятельности;

Комментарий к 6.2.2 b) — При нарушении деятельности воздействие, как правило, возрастает со временем и по-разному влияет на каждый вид деятельности. Воздействие нарушений функционирования может также изменяться в зависимости от дня, месяца или этапа жизненного цикла бизнеса.

c) идентифицировать любые взаимозависимые виды деятельности, активы, инфраструктуру или ресурсы, которые следует непрерывно поддерживать в рабочем состоянии и/или восстанавливать в установленные сроки.

6.2.3 При оценке воздействий должны быть рассмотрены вопросы, касающиеся целей и задач бизнеса организации и ее причастных сторон. Они должны включать оценку:

- воздействий на благосостояние персонала или общества;
- воздействий повреждений или потерь на производственные площади, технологии или информацию организации;
- воздействий нарушения законодательных и обязательных требований;
- потери репутации;
- снижения финансовой устойчивости;
- ухудшения качества продукции или услуги;
- ущерба окружающей среде.

Организация должна документировать метод оценки воздействия нарушений деятельности организации, полученные выходные данные и результаты их анализа.

6.3 Идентификация критических видов деятельности

Организация может классифицировать виды своей деятельности в соответствии с их приоритетностью для их восстановления. Деятельность, идентифицированная в процессе АВБ, потеря которой может оказать в краткосрочный период времени максимальное негативное воздействие на организацию, и которая должна быть восстановлена в кратчайшие сроки, является «критическим видом деятельности». Каждый критический вид деятельности обычно поддерживает одну или более ключевую продукцию или услугу.

При планировании непрерывности деятельности организация может предпочесть ориентироваться на критические виды деятельности, но необходимо учитывать, что другие виды деятельности должны быть также восстановлены в пределах их максимально приемлемого периода нарушения и могут также потребовать по отношению к ним предупреждающих действий.

Комментарий к 6.3 — Максимальный период восстановления деятельности может изменяться от нескольких секунд до нескольких месяцев в зависимости от характера деятельности. Для деятельности, наиболее чувствительной к воздействию времени, максимальный период времени ее восстановления должен быть определен с большей степенью точности, например, в минутах или в часах. Для менее чувствительной ко времени деятельности может потребоваться меньшая точность.

Максимально приемлемый период нарушения воздействует на целевой срок восстановления каждого вида деятельности, который устанавливают при определении стратегии МНБ (см. раздел 7).

6.4 Определение требований к непрерывности

Организация должна оценить ресурсы, необходимые для возобновления каждого вида деятельности. Они могут включать в себя:

a) человеческие ресурсы, в том числе определение количества и квалификации персонала (персонал);

b) рабочие места, производственные помещения и объекты (производственные площади);

c) технологические процессы, средства производства, машины и оборудование (технологии);

d) обеспечение информацией (на электронном или бумажном носителе) об опыте предыдущей работы и/или текущем незавершенном производстве, которая для эффективного обеспечения непрерывности деятельности организации на установленном уровне должна быть актуализированной и точной (информация);

е) обеспечение поставок, услуги сторонних организаций и поставщиков (запасы).

При определении необходимого уровня ресурсов организация должна учесть потребности причастных сторон.

Комментарий к 6.4 — Технологии подразумевают использование оборудования в самом широком смысле в соответствии с потребностями организации. Технологии могут включать: программное обеспечение и оборудование в области ИТ, телекоммуникационное оборудование, специализированные станки, оборудование для пищевой промышленности, герметизации, а также другую технику, существенно важную для производства.

Недоступность, неточность или недостаточная актуализация записей или информации по незавершенному производству могут помешать или существенно задержать возобновление деятельности организации. Требования по обеспечению подобной информацией необходимо учитывать при выборе способа управления записями в общей стратегии МНБ (см. раздел 7).

6.5 Оценка угроз критическим видам деятельности организации

6.5.1 В зависимости от целей применения МНБ необходимо проводить анализ риска с точки зрения непрерывности критических видов деятельности организации и риска их нарушения. Критические виды деятельности должны поддерживаться такими ресурсами, как персонал, производственные площади, технологии, информация, запасы и причастные стороны. Организация должна оценить потенциальные угрозы для этих ресурсов, уязвимость каждого вида ресурса и потенциальное воздействие при превращении угрозы в инцидент, который может вызвать нарушение ее деятельности.

6.5.2 Выбор подхода к оценке риска — это самостоятельное решение организации, однако важно, чтобы этот подход соответствовал всем требованиям организации.

6.5.3 ИСО/МЭК 27001 (см. [4]) устанавливает структуру подхода к оценке риска и обязательные элементы, которые должны включать процесс оценки риска. Типовыми элементами являются:

- определение критериев принятия риска. Должны быть описаны условия, при которых организация может принять риск;
- идентификация приемлемых уровней риска. Независимо от выбранного подхода к оценке риска организация должна идентифицировать приемлемый риск;
- анализ риска. Необходимо, чтобы подход организации к оценке риска учитывал все понятия и положения, рассмотренные в 6.5.4— 6.5.6.

6.5.4 Конкретные угрозы могут быть описаны как опасные события или действия, которые могут в какой-то момент оказать негативное воздействие на ресурсы, например, такие угрозы, как пожар, наводнение, нарушение энергоснабжения, потеря персонала, невыход персонала на работу, компьютерные вирусы или отказ компьютерных аппаратных средств.

6.5.5 Уязвимые места — это недостатки («слабые места») в ресурсах, которые могут подпасть под воздействие угроз, например, неустойчивость работы одного элемента системы, отдельные несоответствия в противопожарной защите, неустойчивость к скачкам напряжения электросети, неукомплектованность персоналом, незащищенность или неустойчивость отдельных частей информационных технологий и т.д.

6.5.6 Воздействие на бизнес (см. 6.2.3) может явиться следствием воздействия опасных событий на уязвимые места.

Комментарий к 6.5 — При оценке угроз целесообразно использовать регистры риска, составленные другими подразделениями организации и/или сторонними организациями.

6.6 Выбор действий

6.6.1 Краткий обзор

В результате АВБ и оценки риска организация должна идентифицировать соответствующие меры для того, чтобы:

- уменьшить вероятность нарушений деятельности;
- сократить период нарушений деятельности;
- ограничить воздействие нарушений на ключевые виды продукции и услуги организации.

Эти предпринимаемые меры известны как снижение потерь и обработка риска.

Стратегии снижения потерь могут быть использованы в сочетании с другими вариантами, когда не все риски могут быть предотвращены или уменьшены до приемлемого уровня. Организация может применить одну, более одной или все стратегии (6.6.2—6.6.5) для каждого критического вида деятельности.

6.6.2 Непрерывность бизнеса

Если организация решила применить для ключевой продукции или услуги стратегию непрерывности бизнеса, то должен быть установлен «целевой срок восстановления» и в соответствии с этим показателем проведена оценка стратегии непрерывности бизнеса (раздел 7).

Стратегии непрерывности направлены на повышение устойчивости организации к нарушениям и разрушениям. Это достигается путем обеспечения непрерывности критических видов деятельности и/или их восстановления на приемлемом минимальном уровне и в сроки, установленные в результате АВБ.

6.6.3 Принятие риска

Риск может считаться приемлемым без необходимости предпринимать дальнейшие действия. Даже если конкретный риск неприемлем, в некоторых ситуациях сделать что-либо с небольшим по величине риском может быть трудно или стоимость предпринятых ответных мер непропорциональна полученной выгоде. В этих случаях решением может быть принятие существующего уровня риска, если высшее руководство считает подобный риск приемлемым и его значение находится в границах допустимого совокупного риска организации. В некоторых обстоятельствах воздействие риска может быть вне допустимого совокупного риска организации, однако из-за низкой вероятности возникновения соответствующего опасного события и/или экономической нецелесообразности затрат на управление данным риском, высшее руководство может принять риск.

Принятие риска может быть дополнено разработкой и применением плана обработки риска в ситуации, когда произойдет соответствующее опасное событие.

6.6.4 Передача риска

В некоторых случаях лучшим решением может быть передача риска. Это достигается путем применения обычных страховых или договорных соглашений, либо путем оплаты третьему лицу, которое принимает на себя риск любым способом. Подобный выбор особенно хорош для того, чтобы смягчить финансовый риск или риск, связанный с активами. Риск может быть передан для уменьшения подверженности организации риску или по причине того, что другая организация имеет больше возможностей для эффективного управления риском. Важно отметить, что некоторые виды риска вообще не могут быть переданы, в частности невозможно передать риск потери репутации, даже если в договоре предусмотрен отказ от поставки услуги.

Заключение договоров страхования может стать частью стратегии обработки риска и обеспечить некоторую финансовую компенсацию за понесенные потери. Однако не все потери можно полностью застраховать (например, незастрахованные инциденты, урон, нанесенный бренду или репутации, снижение стоимости активов причастных сторон, сокращение доли рынка и последствия для здоровья человека). Одно только финансовое урегулирование не всегда позволяет полностью защитить ее способом, удовлетворяющим ожидания причастных сторон. Установление объема страхования, вероятнее всего, следует использовать совместно с другими стратегиями.

6.6.5 Изменение, приостановка или прекращение производства

В некоторых обстоятельствах может быть уместно изменение, приостановка или прекращение производства продукции, оказания услуги, деятельности функционального подразделения или процесса. Этот вариант необходимо рассматривать только тогда, когда он не противоречит установленным целям организации, законодательным и обязательным требованиям и ожиданиям причастных сторон. Данный вариант в основном применим при ограниченном сроке жизни услуги, продукции, деятельности, функционального подразделения или процесса.

Примечание — Эти четыре элемента иногда называют моделью «4 Т»[1)] «Обработка» (непрерывность бизнеса), «Допустимость» (принятие риска), «Передача» и «Прекращение производства».

6.7 Утверждение

Высшее руководство должно утвердить перечень ключевой продукции и услуг, анализ воздействия на бизнес и оценки риска для обеспечения того, чтобы работа была выполнена должным образом и соответствовала потребностям организации.

[1)] «4 T» model: «Treat» (business continuity), «Tolerate» (accept the risk), «Transfer» and «Terminate».

7 Определение стратегии МНБ



Данный элемент жизненного цикла МНБ логически следует за элементом «анализ непрерывности бизнеса организации». В результате предыдущего анализа организация имеет возможность выбрать соответствующие стратегии непрерывности бизнеса согласно установленным целям.

7.1 Введение

При выборе стратегии МНБ организация должна учитывать необходимость:

a) разработки мер уменьшения вероятности появления инцидентов и/или снижения их возможных последствий;

b) разработки мер по ослаблению последствий инцидентов и восстановлению деятельности организации после них, а также мер по обеспечению устойчивости работы организации;

c) обеспечения непрерывности критических видов деятельности во время инцидента и после него;

d) учета видов деятельности, которые не были идентифицированы как критические.

Комментарий к 7.1 — Раздел 7 и все последующие разделы касаются тех ключевых видов продукции и услуг, для которых принято решение о внедрении системы непрерывности бизнеса. Во всех других случаях (например, в случае приостановки и прекращения данного вида деятельности или принятия риска), если подход МНБ не охватывает продукцию или услуги, то они не могут быть признаны соответствующими настоящему стандарту.

7.2 Выбор стратегии

7.2.1 Организация должна выбрать стратегию непрерывности для своих критических видов деятельности, а также ресурсы, необходимые для восстановления каждого из них. При выборе стратегии необходимо учитывать следующие факторы:

- максимально приемлемый период нарушения критического вида деятельности;
- затраты на внедрение стратегии;
- последствия бездействия.

7.2.2 Для реализации стратегии могут потребоваться следующие ресурсы организации:

- персонал (см. 7.3);
- производственные площади (см. 7.4);
- технологии (см. 7.5);
- информация (см. 7.6);
- запасы (см. 7.7);
- причастные стороны (см. 7.8).

В каждом конкретном случае организация должна минимизировать вероятность невыполнения решения по обеспечению непрерывности из-за воздействия инцидента, вызвавшего нарушение ее деятельности.

7.3 Персонал

Организация должна идентифицировать соответствующие стратегии для поддержания квалификации, основных навыков и знаний персонала. Этот анализ, кроме персонала, должен охватывать подрядчиков[1)] и другие причастные стороны, специалисты которых должны также обладать соответствующей квалификацией, обширными специальными навыками и знаниями. Стратегии защиты или обеспечения подобных навыков могут включать в себя:

a) документирование способа осуществления критических видов деятельности;

b) обучение разносторонним навыкам персонала и подрядчиков;

c) разделение основных навыков для снижения концентрации риска (это может повлечь за собой распределение персонала с основными навыками или обеспечение того, что у более чем одного работника имеются необходимые основные навыки);

d) привлечение третьих лиц;

e) планирование преемственности;

f) хранение знаний и управление ими.

7.4 Производственные площади

Организация должна разработать стратегию снижения воздействия опасной ситуации, при которой обычное рабочее место (рабочие места) и/или производственные площади (объекты) становятся недоступны. Стратегия может включать одно или более следующих положений:

a) предоставление альтернативных производственных площадей, включая перемещение из этих мест видов деятельности в организации;

b) предоставление альтернативных производственных площадей партнерскими организациями (это может быть взаимное или одностороннее предоставление производственных площадей на договорной основе);

c) предоставление альтернативных производственных площадей специалистами третьей стороны;

d) работа на дому или в удаленных производственных площадях;

e) предоставление других согласованных подходящих производственных площадей;

f) использование альтернативной рабочей силы на существующих рабочих местах или производственных площадях.

Примечание

1 — Если работники должны быть переведены в альтернативные производственные площади, эти площади должны располагаться не слишком далеко от обычного места, чтобы работники хотели и были в состоянии переместиться туда, принимая во внимание все вероятные трудности, вызванные инцидентом. Однако альтернативные производственные площади не должны располагаться слишком близко, так как может возникнуть вероятность воздействия на них того же самого инцидента.

2 — Способ применения альтернативной производственной площади (единолично самой организацией или совместно с другими) должен быть точно идентифицирован, поскольку он влияет на использование производственной площади для целей обеспечения непрерывности бизнеса. Если альтернативная производственная площадь используется совместно с другими организациями, должен быть разработан и зарегистрирован план совместного использования и/или план действий при недоступности этой площади.

3 — Может быть целесообразным перемещение объема работ (производственной деятельности), а не персонала, например перемещение производственной линии или диспетчерского отдела.

Комментарий к 7.4 — Стратегии размещения рабочих мест и производственных площадей могут значительно изменяться и могут быть приняты различные решения. Различные типы инцидентов или угроз могут потребовать создания различных или множественных решений по вопросу рабочих мест и производственных площадей. То, насколько правильно выбрана стратегия, отчасти зависит от размера, сферы и распространения деятельности организации, причастных сторон или географического месторасположения. Например, государственные органы власти должны осуществлять свою деятельность в границах своей же территории.

7.5 Технологии

7.5.1 Технологические стратегии зависят от характера используемых технологий и их связи с критическими видами деятельности, но обычно включают одну или более стратегий, связанных с:

- поставками внутри организации;

[1)] Партнеры по аутсорсингу.

- услугами и поставками для организации;
- услугами, предоставленными третьим лицом за пределами организации.

Комментарий к 7.5.1 — Технологические стратегии у различных организаций могут значительно отличаться в зависимости от размера, характера и сложности бизнеса организации. Должны быть разработаны специальные стратегии для защиты, сохранения, замены и/или восстановления специализированных или предложенных потребителем технологий с большой продолжительностью производственного цикла.

Организация (если применимо) должна обеспечивать условия для ручного производства до тех пор, пока не будут восстановлены все технологические процессы.

7.5.2 Технологические стратегии могут включать:

- географическое распределение технологий, т.е. поддержку одной технологии на различных территориях, которые не могут быть затронуты одним и тем же инцидентом нарушения деятельности организации;
- сохранение старого оборудования, предназначенного для использования либо в качестве замены основного оборудования при чрезвычайных ситуациях, либо в качестве запасных частей;
- снижение дополнительного риска для уникального оборудования или оборудования с большой продолжительностью производственного цикла.

7.5.3 Для информационных технологий (ИТ) часто требуются комплексные стратегии непрерывности бизнеса. Если существует потребность в подобных стратегиях, должны быть рассмотрены следующие показатели:

- целевой срок восстановления для систем и прикладных программ, обеспечивающих поддержку ключевых видов деятельности, идентифицированных в АВБ;
- расположение и расстояние между местами размещения технологического оборудования ИТ;
- количество мест размещения технологического оборудования ИТ;
- удаленный доступ;
- использование мест размещения технологического оборудования ИТ без участия персонала в противоположность технологиям с привлечением персонала;
- подключение к телекоммуникационным системам и наличие дублирующих маршрутов телекоммуникационных соединений;
- характер «преодоления отказа»[1] (ручное или автоматизированное переключение на альтернативное ИТ);
- соединение, предоставленное третьей стороной, и внешние каналы связи.

Примечания

1 Если принята стратегия «передачи отказа» от одного места размещения технологического оборудования ИТ к другому, то расстояние маршрута сети между этими двумя местами размещения должно быть тщательно продумано и исследовано, поскольку дистанция между ними может оказывать негативное воздействие на работу ИТ систем.

2 Если технологическое оборудование ИТ организации расположено более, чем на одном месте размещения, то может быть использована стратегия взаимного восстановления ИТ. При этом системы, сети и хранилище данных на каждом месте размещения технологического оборудования ИТ должны позволять дублировать функции, обрабатывать объединенный трафик и выполнять работу других систем в дополнение к собственной работе.

3 Если принято решение о перемещении работников в альтернативные производственные площади, то им должен быть предоставлен удаленный доступ к ИТ через коммуникационное соединение или через Интернет с использованием виртуальной частной сети[2] (VPN) или аналогичных технологий.

4 Рекомендации по ИТ и телекоммуникационному оборудованию приведены в [4], [5], [6] и [7].

7.6 Информация

Информационные стратегии должны обеспечивать защиту и восстановление жизненно важной информации для деятельности организации в сроки, установленные на этапе АВБ.

Примечание — Более детальные рекомендации приведены в ИСО/МЭК 27001. Хранение и восстановление подобной информации должно соответствовать законодательным и обязательным требованиям.

---

[1] Процесс передачи функций управления дублирующему узлу при отказе основного с перераспределением ролей основного и дублирующего узлов — (Прим. пер.).

[2] Удаленная локальная сеть, для доступа к которой через Интернет используется протокол PPTP — (Прим. пер.).

Вся информация, требуемая для обеспечения поставок по критическим видам деятельности организации, должна иметь следующие качества:

- конфиденциальность;
- целостность;
- доступность;
- актуальность.

Должны быть документированы информационные стратегии для восстановления информации, которая еще не скопирована или для которой не создана резервная копия, хранящаяся в безопасном месте.

Информационные стратегии должны охватывать:

- физические форматы информации (документальные копии);
- виртуальные форматы информации (электронные копии) и т.д.

Примечание — Во всех случаях информация должна быть восстановлена до установленного момента времени, согласованного с высшим руководством организации. Могут быть использованы различные методы копирования, такие как резервные копии в электронном виде, на магнитной ленте, микрофишы[1)], фотокопии, создание двойных экземпляров во время производства и т.д. Время восстановления должно соответствовать «целевому сроку восстановления».

7.7 Запасы

7.7.1 Организация должна идентифицировать и поддерживать в рабочем состоянии перечень основных запасов (сырья и материалов), которые обеспечивают критические виды деятельности организации. Стратегии обеспечения запасов могут включать в себя:

- хранение дополнительных запасов в альтернативных местах размещения;
- заключение соглашений с третьими лицами о срочных внеплановых поставках запасов в критических ситуациях;
- изменение пункта назначения поставок «точно в срок»[2)];
- хранение материалов на товарных складах или погрузочно-разгрузочных участках;
- передача сборочных операций на альтернативные производственные площади, в которых существует возможность бесперебойного снабжения;
- идентификация альтернативных поставок (субститутов).

7.7.2 Если критические виды деятельности зависят от специализированных запасов, организация должна идентифицировать ключевых поставщиков и единственные (безальтернативные) источники поставок. Стратегии управления непрерывностью таких поставок могут включать в себя:

- увеличение количества поставщиков;
- поощрение поставщиков (или установление требований к ним) к наличию валидированной способности к обеспечению непрерывности бизнеса;
- установление договорных отношений и/или соглашений о техническом обслуживании с ключевыми поставщиками на согласованном уровне;
- идентификацию альтернативных, способных к бесперебойной работе поставщиков.

Комментарий к 7.7 — В офисных и банковских учреждениях запасы могут охватывать банковские чеки и т.п. На промышленных предприятиях могут быть идентифицированы запасы товара на складе и поставки «точно в срок», необходимое топливо для транспортных средств и др.

7.8 Причастные стороны

7.8.1 При определении стратегии МНБ организация должна рассматривать и защищать интересы своих ключевых причастных сторон. Эти стратегии должны учитывать соответствующие социальные и культурные аспекты.

7.8.2 Организация должна идентифицировать соответствующие стратегии управления взаимоотношениями с ключевыми причастными сторонами, партнерами по бизнесу, поставщиками и подрядчиками. Каждая группа может потребовать отдельного анализа. Стратегии защиты интересов ключевых причастных сторон могут включать в себя специальные меры по обеспечению благосостояния причастных сторон с особыми потребностями, такими как нетрудоспособность, болезнь или беременность.

7.8.3 Организация должна идентифицировать лицо или группу лиц, ответственных за проблемы благосостояния причастных сторон после возникновения инцидента.

[1)] Карточки с несколькими кадрами микрофильма — (Прим. пер.).

[2)] Концепция управления, предполагающая поставку ресурса непосредственно к началу момента его использования — (Прим. пер.).

7.9 Гражданские чрезвычайные ситуации

7.9.1 При определении, внедрении или валидации стратегий управления инцидентом и менеджмента непрерывности бизнеса организация на начальной стадии должна наладить контакт с территориальными государственными органами экстренного реагирования, поскольку именно они несут ответственность за работу по прогнозированию, оценке, предупреждению, подготовке мероприятий и действий по восстановлению при возникновении гражданских чрезвычайных ситуаций.

Примечание — В РФ ответственность за действия в чрезвычайных ситуациях возложена на МЧС (Министерство по чрезвычайным ситуациям). При возникновении гражданских чрезвычайных ситуаций организации должны руководствоваться требованиями нормативно-правовых актов Российской Федерации, в т.ч. утвержденными МЧС РФ.

7.9.2 Основные государственные органы экстренного реагирования обеспечивают официальное оповещение о гражданской чрезвычайной ситуации, в том числе:

- оповещение о начале и окончании инцидента (например, оценке риска);
- предупреждение об опасности, обмен информацией и консультации;
- совместные меры по восстановлению после гражданской чрезвычайной ситуации.

Примечание — Гражданские чрезвычайные ситуации могут привести к смертельным случаям среди людей и/или причинению им физических повреждений (травм); они могут оказать серьезное и долгосрочное воздействие на психологическое, социальное и экономическое благосостояние людей и общества. Чрезвычайная ситуация может быстро привести к существенному нарушению в работе общественного транспорта, основных коммуникаций, критических видов инфраструктуры, перебоям в поставках товаров, работ, услуг и истощению запасов. В свете потенциальных нарушений работы и разрушений организации могут ознакомиться с соответствующими официальными планами мероприятий государственных органов власти при возникновении чрезвычайных ситуаций.

7.10 Утверждение

Высшее руководство должно утвердить документированные стратегии для подтверждения того, что стратегии обеспечения непрерывности бизнеса выполнены должным образом и учитывают вероятные характеристики причин и последствий нарушений, и что выбранные стратегии соответствуют поставленным целям организации в пределах допустимого совокупного риска организации.

8 Разработка и внедрение ответных мер МНБ



Данный элемент жизненного цикла МНБ связан с разработкой и внедрением соответствующих планов и мероприятий по обеспечению непрерывности критических видов деятельности и управлению инцидентом.

8.1 Введение

В разделах 6 и 7 приведены методы, применяемые организацией с целью:

- идентификации своих критических видов деятельности;
- оценки потенциальных угроз для данных критических видов деятельности;
- выбора соответствующих стратегий по уменьшению вероятности возникновения инцидентов и их последствий;
- выбора соответствующих стратегий обеспечения непрерывности бизнеса или восстановления его критических видов деятельности.

Набор и диапазон угроз должны быть определены в соответствии с допустимым совокупным риском организации.

8.2 Структура ответных мер на инцидент

8.2.1 Организация должна определить структуру управления ответными мерами на инцидент, которая позволит обеспечить эффективную ликвидацию нарушений и восстановление нормального функционирования бизнеса в организации.

8.2.2 В любой ситуации, связанной с инцидентом, должна быть установлена простая и удобная форма структуры управления, которая позволяет организации:

- подтвердить характер и степень инцидента;
- контролировать ситуацию;
- сдерживать развитие инцидента;
- проводить эффективный обмен информацией с причастными сторонами.

Та же структура должна приводить в действие соответствующие ответные меры по обеспечению непрерывности бизнеса. Эта структура может быть названа группой управления инцидентом (IMT[1)]) или группой кризисного менеджмента (CMT[2)]).

8.2.3 Группа управления инцидентом должна иметь планы, процессы и процедуры управления инцидентом, а также использовать вспомогательные методы и инструменты обеспечения непрерывности бизнеса для восстановления критических видов деятельности.

8.2.4 Группа управления инцидентом должна иметь план по инициированию своей работы, планы действий, координации и обмена информацией об ответных мерах при возникновении инцидента.

На рисунке 2 показаны три главных этапа развития инцидента, а также взаимосвязь управления инцидентом и обеспечения непрерывности бизнеса.

Примечание — В некоторых случаях инициирование в организации процедур управления инцидентом, обеспечения непрерывности бизнеса и планов восстановления бизнеса может быть выполнено либо в быстрой последовательности, либо одновременно.

8.2.5 Организация может разработать специальные планы восстановления или возобновления операций возврата к «нормальному» состоянию (планы восстановления). Однако в некоторых инцидентах невозможно определить состояние объекта до инцидента, поэтому невозможно или проблематично своевременно применить планы восстановления. Поэтому организация должна стремиться предусмотреть в планах обеспечения непрерывности бизнеса время на разработку планов восстановления до нормального состояния.

Комментарий к 8.2 — В малых организациях ответственность за инцидент и менеджмент непрерывности бизнеса может быть возложена на одного человека. Крупные организации могут использовать многоуровневый подход и создавать различные группы, ориентированные на управление инцидентом, обеспечение непрерывности бизнеса и восстановление бизнеса. В некоторых случаях эти группы могут сотрудничать с другими группами, наделенными ответственностью за конкретные виды деятельности, такими как обмен информацией со СМИ и решение проблем, связанных с человеческим фактором (например, отделом кадров).

[1)] IMT — Incident management team.

[2)] CMT — Crisis management team.

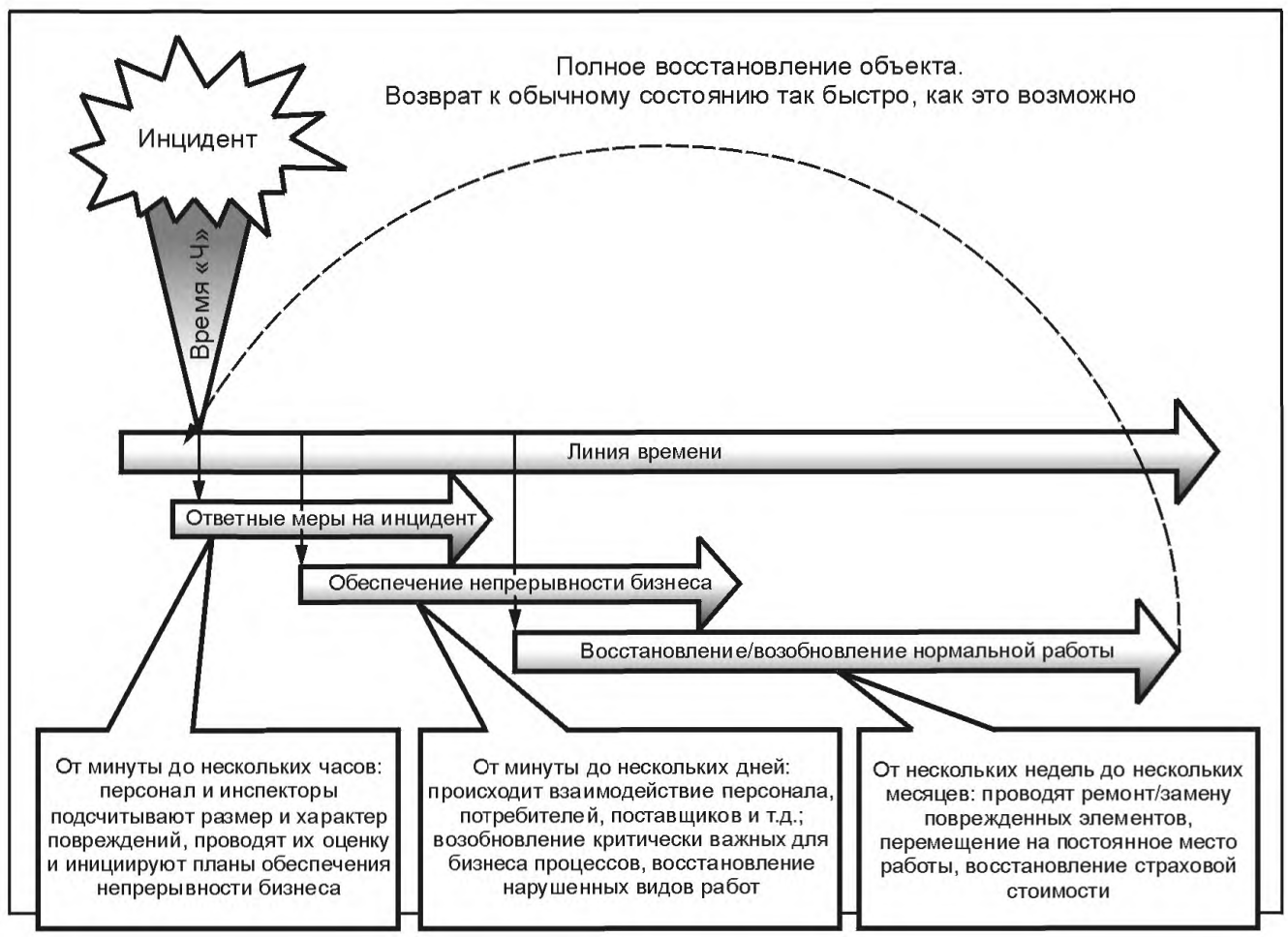

Рисунок 2 — Развитие инцидента во времени

8.3 Инициирование планов

8.3.1 Введение

Все планы (планы управления инцидентом, планы обеспечения непрерывности бизнеса и/или планы восстановления бизнеса) должны быть краткими, понятными и доступными для соответствующих ответственных лиц. Планы должны содержать элементы, описанные в 8.3.2—8.3.6.

Комментарий к 8.3.1 — В малых организациях может быть один общий план, который охватывает все требования бизнеса и все его процедуры. В крупных организациях возможна разработка и применение нескольких планов, каждый из которых посвящен:

- *отдельной части бизнеса;*
- *отдельной производственной площади;*
- *отдельному сценарию*

и может предусматривать отдельную документацию для разных этапов: инцидента, обеспечения непрерывности и восстановления.

8.3.2 Цель и область применения

Цель и область применения каждого конкретного плана должны быть определены, утверждены высшим руководством и понятны лицам, на которых возложено выполнение этого плана. В планах должны быть точно указаны все использованные ссылки и связи с другими планами или документами организации, а также описан метод хранения и доступа к этим планам.

В каждом плане управления инцидентом, обеспечения непрерывности бизнеса и восстановления бизнеса должна быть установлена приоритетность целей с точки зрения:

- критических видов деятельности, подлежащих восстановлению;
- временного графика восстановления;
- уровней восстановления, необходимых для каждого критического вида деятельности;
- ситуации, в которой каждый план должен быть введен в действие.

Комментарий к 8.3.2 — В каждом плане может быть достаточно четко установлено, что и почему в результате его реализации должно быть достигнуто.

8.3.3 Обязанности и ответственность

Обязанности и ответственность отдельных лиц и групп, наделенных соответствующими полномочиями (с точки зрения принятия решений и финансовой ответственности) в процессе и после инцидента должны быть точно документированы.

Лицо или группы лиц, вовлеченные в работу по этим планам, должны быть точно установлены.

Комментарий к 8.3.3 — Планы могут содержать (если применимо) процедуры и перечень контрольных вопросов (вопросники), облегчающих анализ ситуации после инцидента.

8.3.4 Инициирование плана

Метод, с помощью которого план управления инцидентом, обеспечения непрерывности бизнеса или восстановления бизнеса вводят в действие, должен быть документирован. Этот процесс должен учитывать существующие планы или их части для того, чтобы в самый короткий срок инициировать работы после нарушения деятельности организации.

Организация должна установить и документально оформить точные руководящие принципы, обстоятельства и набор критериев, в соответствии с которыми лицо (группа лиц), наделенные соответствующими полномочиями, может инициировать работу по плану(ам).

Процесс инициирования работ может потребовать немедленной мобилизации ресурсов организации. План должен включать в себя ясное и точное описание:

- способа сбора группы;
- места экстренного сбора;
- последующего места совещаний для группы и подробного описания любых альтернативных мест встречи (в больших организациях эти места сбора могут быть названы центрами по управлению инцидентами, центрами управления и др.).

Организация должна четко и точно документировать процесс роспуска группы (групп) и возврат вовлеченных лиц к обычной деятельности.

Комментарий к 8.3.4 — Время, потраченное на выполнение ответных мер на инцидент, никогда не может быть восполнено. Почти всегда лучше собрать группу для выполнения ответных мер на инцидент и впоследствии распустить ее, чем пропустить возможность отреагировать на инцидент на ранней стадии и допустить его эскалацию.

Организация может разложить инцидент на определенные составляющие и согласованные этапы его развития в соответствии с точными руководящими указаниями, полученными из экспертных источников, например Всемирной организации здравоохранения по пандемиям.

8.3.5 Владелец документа и лицо, ответственное за актуализацию документа

Организация должна назначить основного владельца плана, а также идентифицировать и документально оформить назначение лиц, ответственных за анализ, пересмотр и актуализацию плана через регулярные запланированные интервалы времени.

Организация должна использовать систему управления версиями документов. Изменения должны быть доведены до всех заинтересованных сторон в соответствии с формальным планом распределения документов. Записи об этом должны поддерживаться в рабочем состоянии и постоянно актуализироваться.

8.3.6 Подробное описание контактной информации

Каждый план должен содержать описание или ссылку на описание важной контактной информации для всех ключевых причастных сторон.

Комментарий к 8.3.6 — Записи о контактной информации могут включать в себя подробное описание данных о формах связи с ответственными лицами во внерабочее время. Если планы имеют подобную частную информацию, то необходимо обеспечить защиту личных данных от несанкционированного доступа.

8.4 План управления инцидентом

Цель плана управления инцидентом состоит в обеспечении управления организацией на первоначальной (наиболее острой) стадии развития инцидента.

План управления инцидентом должен:

a) быть гибким, выполнимым и соответствовать поставленным целям;

b) быть легко читаемым и понятным;

c) обеспечивать основу для управления и решения всех возможных проблем, включая проблемы причастных сторон и внешние проблемы, стоящие перед организацией в процессе инцидента.

План управления инцидентом также должен:

1) иметь поддержку со стороны высшего руководства, включая председателя совета директоров (если применимо);

2) поддерживаться соответствующим бюджетом для разработки, поддержания в рабочем состоянии и проведения обучения.

8.5 Содержание плана управления инцидентом

8.5.1 Общие положения

В дополнение к содержанию, рекомендуемому в 8.3, план управления инцидентом должен включать в себя информацию, описанную в 8.5.2—8.5.8.

8.5.2 Перечень задач и действий

План управления инцидентом должен включать в себя контрольный перечень задач и действий для управления ближайшими последствиями нарушения деятельности организации. Эти задачи и действия должны:

- обеспечивать, в первую очередь, безопасность людей при возникновении нарушений функционирования и разрушений;
- быть основаны на результатах АВБ организации;
- иметь структуру, направленную на поддержку стратегических и тактических целей и решений организации (см. раздел 7);
- помогать в предупреждении дальнейших потерь, при невозможности осуществления критических видов деятельности и доступа к обеспечивающим ресурсам (см. раздел 7).

8.5.3 Контактная информация в чрезвычайной ситуации

В план управления инцидентом должно быть включено описание того, как и при каких обстоятельствах организация должна обмениваться информацией о чрезвычайной ситуации с персоналом, их родственниками, друзьями и другими причастными к чрезвычайной ситуации лицами. В некоторых случаях может потребоваться описание подробной контактной информации, необходимой при возникновении чрезвычайной ситуации, в отдельном документе.

Информация о ближайших родственниках и контактных лицах для связи в случае возникновения чрезвычайных ситуаций для всего персонала организации должна быть актуализированной и доступной для быстрого использования.

Комментарий к 8.5.3 — В зависимости от масштаба организации и размера инцидента может потребоваться назначение компетентного и обученного персонала для ответов на телефонные запросы об инциденте.

8.5.4 Действия людей

План управления инцидентом должен учитывать интересы лиц, благосостояние которых может подвергнуться риску в результате возникновения инцидента, принимая во внимание соответствующие социальные и культурные аспекты (см. 7.8.2).

План управления инцидентом должен идентифицировать лицо (лиц), ответственное(ых) за проблемы благосостояния после возникновения инцидента (см. 7.8.3), деятельность которого(ых) включает в себя:

a) обеспечение мест эвакуации (включая действия во внутренних убежищах);

b) мобилизацию групп по обеспечению безопасности, групп оказания первой и скорой медицинской помощи или групп помощи при эвакуации;

c) поиск и учет лиц, находящихся в месте событий и/или в непосредственной близости от них;

d) постоянный обмен информацией с работниками и потребителями, брифинги и инструктаж по обеспечению и технике безопасности.

Организация должна подготовить персонал, наделенный соответствующими полномочиями, для обеспечения связи с аварийными службами (если применимо).

Примечание — Аварийно-спасательные службы играют первостепенную роль в защите жизни и оказании помощи людям во время чрезвычайных ситуаций. Поэтому обращение к ним на ранних стадиях возникновения инцидента, предварительное планирование и координирование работ во время инцидента в режиме реального времени между организацией, ее первыми респондентами и аварийно-спасательными службами, могут повысить эффективность ответных мер защиты и восстановления организации.

Организация может обеспечить опрос и консультации с пострадавшим и вовлеченным персоналом после инцидента. Подобные услуги могут быть предоставлены внешними сторонами или оказываться в дополнение к существующим программам по охране и безопасности труда персонала.

Комментарий к 8.5.4 — Организации несут непосредственную ответственность за защиту благосостояния работников, подрядчиков, посетителей и потребителей, если инцидент представляет прямую угрозу для их жизни, средств к существованию и благосостоянию. Отдельное внимание должно быть направлено на группы лиц с ограниченными возможностями или других лиц с особыми требованиями (например, беременных, временно нетрудоспособных лиц из-за ранения и т.д.). Пред-

варительное планирование взаимодействий с подобными лицами во время инцидента помогает снизить риск и возможные потери.

Нельзя недооценивать долгосрочное воздействие инцидентов. Разработка соответствующих стратегий в поддержку благосостояния людей может непосредственно помочь физическому и эмоциональному восстановлению людей в организации после инцидента.

8.5.5 Взаимодействие со СМИ

Формы взаимодействия организации со СМИ должны быть документированы в плане управления инцидентом и включать в себя:

a) стратегию обмена информацией об инциденте;

b) приоритетные средства массовой информации во время инцидента;

c) рекомендации и/или шаблоны для составления заявления, которое будет предоставлено СМИ на самой ранней стадии (в зависимости от реальных возможностей) после возникновения инцидента;

d) необходимое количество обученного, компетентного и уполномоченного персонала для общения и предоставления информации СМИ;

e) обеспечение (если применимо) подходящего места для связи и встреч с представителями СМИ или другими группами причастных сторон.

В некоторых случаях может быть необходимо:

- разработать отдельный документ для обеспечения подробной информации о взаимодействии со СМИ;

- выделить необходимый компетентный и обученный персонал для ответа на телефонные запросы прессы;

- подготовить материал об организации и ее деятельности (эта информация должна быть повторно согласована перед выпуском в СМИ);

- обеспечить доступность для СМИ всей необходимой информации (без неуместной задержки).

Комментарий к 8.5.5 — Предварительная подготовка информации может быть особенно полезной на начальных стадиях инцидента. Это позволяет организации предоставить подробную информацию об организации и ее бизнесе, в то время как подробности инцидента все еще устанавливаются. Организация может использовать все применимые средства, такие как веб-сайты, представителей для связей со СМИ, источники новостей и общие заявления на брифингах для предоставления информации в течение и после инцидента.

8.5.6 Управление взаимодействием с причастными сторонами

В план управления инцидентом также должен быть включен процесс идентификации ключевых причастных сторон и расстановки их приоритетности с точки зрения обмена с ними информацией при инциденте. Может возникнуть необходимость разработки отдельного плана управления взаимодействием с причастными сторонами для обеспечения критериев расстановки приоритетов и распределения лиц по причастным сторонам или группам причастных сторон.

Комментарий к 8.5.6 — Должна быть также учтена возможность влияния или давления отдельных лиц, групп лиц и/или коллективных действий людей на организацию в период инцидента.

8.5.7 Место управления инцидентом

Организация должна определить надежное и заранее установленное место (помещение), из которого будет осуществляться управление инцидентом. После определения этого места оно должно стать центром управления инцидентом. Должны быть также утверждены альтернативные места сбора и проведения совещаний в различных местах расположения на случай, если возможность доступа к первично запланированному месту отсутствует. К каждому утвержденному месту должен быть обеспечен доступ необходимых ресурсов, с помощью которых группа по управлению инцидентом может без задержки начать эффективные действия по восстановлению.

Выбранное место должно быть пригодным для этих целей и включать в себя:

a) эффективные первичные и вторичные средства коммуникаций;

b) средства для доступа, распределения и обмена необходимой информацией, включая мониторинг новостей в СМИ.

Комментарий к 8.5.7 — Место управления инцидентом — это центр, из которого возможно управление инцидентом. В процессе управления инцидентом важными факторами являются получение и распространение ключевой информации, установление целей, назначение задач, управление ресурсами, идентификация и прослеживание проблем, а также принятие обоснованных решений. Поэтому надежный и качественный обмен информацией становится существенным фактором в этом процессе. Использование центров управления позволяет преодолеть ситуации, в которых телефонные линии перегружены.

Место расположения центров управления может быть очень простым, таким, как номер гостиницы или дом сотрудника. Место управления инцидентом может носить комплексный характер и быть, например, «командным центром», обеспеченным компьютерной техникой, видео- и конференц-связью, многоканальными телефонами.

Первоначально для быстрого принятия ключевых решений может потребоваться проведение виртуальных совещаний или совещаний вне места расположения центра управления, например, с помощью телефона, теле- или видеоконференции.

8.5.8 План управления инцидентом

План управления инцидентом должен содержать актуализированное подробное описание контактной информации и плана мобилизации любых соответствующих агентств, организаций и ресурсов, которые могут потребоваться для поддержки стратегии реализации ответных мер организации на инцидент.

План управления инцидентом должен включать журналы или формы регистрации (в т.ч. логи) жизненно важной информации об инциденте, такой как хронометраж инцидента, подробное описание пострадавших, принятые решения, потраченные денежные средства, оценку повреждений, а также информацию, распространенную и полученную в процессе инцидента, и любую другую существенную для организации информацию, необходимую для проведения анализа после инцидента.

План управления инцидентом может также включать в себя или иметь ссылку на:

a) карты, диаграммы, планы, фотографии и другую необходимую информацию, относящуюся к инциденту;

b) документированные стратегии ответных мер, согласованные с третьими лицами (партнеры совместного предприятия, подрядчики, поставщики и т.д.);

c) подробное описание участков подготовки производства и складов хранения оборудования;

d) планы доступа к производственным площадям;

e) процедуры управления требованиями, которые должны охватывать все страховые и юридические обязательства организации, отвечать обязательным, законодательным и договорным требованиям.

8.6 План обеспечения непрерывности бизнеса

Целью плана(ов) обеспечения непрерывности бизнеса является обеспечение для организации возможности в случае возникновения нарушений поддерживать или восстанавливать свою деятельность до нормального состояния.

План обеспечения непрерывности бизнеса должен быть инициирован для обеспечения непрерывности выполнения критических видов деятельности, необходимых для достижения целей организации. Он может быть введен в действие полностью или частично на любой стадии развития и ликвидации последствий инцидента.

Комментарий к 8.6 — Компоненты и содержание планов обеспечения непрерывности бизнеса в различных организациях отличаются друг от друга и имеют различный уровень детализации, в зависимости от среды функционирования и технологической сложности организации.

Для крупных организаций может потребоваться разработка отдельных документов для каждого из критических видов работ, тогда как для малых организаций все критические виды работ могут быть описаны в одном документе.

8.7 Содержание плана обеспечения непрерывности бизнеса

8.7.1 Общие сведения

В дополнение к разделам, рекомендуемым в 8.3, план обеспечения непрерывности бизнеса должен содержать элементы, приведенные в 8.7.2—8.7.5.

8.7.2 План действий/перечень задач

План действий должен включать структурированный контролируемый перечень действий и задач, расположенных в порядке приоритетности. В плане должны быть указаны:

a) способ инициирования плана обеспечения непрерывности бизнеса;

b) лицо (лица), ответственное(ые) за инициирование плана обеспечения непрерывности бизнеса;

c) процедура принятия ответственным лицом конкретного решения;

d) лицо (лица), с которым(и) необходимо консультироваться перед принятием конкретного решения;

e) лицо (лица), которое(ые) должно(ы) быть проинформировано(ы) о принятии конкретного решения;

f) кто, где, когда и как должен действовать;

g) какие услуги (службы) доступны в конкретном месте и когда (включая способы мобилизации внешних ресурсов организации и ресурсов, принадлежащих третьей стороне);

h) как и когда следует проводить обмен информацией о конкретных действиях;

i) если применимо, подробные процедуры восстановления системы вручную и т.д.

Комментарий к 8.7.2 — Планы должны включать ссылки на персонал, производственную площадь, технологии, информацию, запасы и причастные стороны, идентифицированные на этапе определения стратегий (см. раздел 7). Должны быть четко описаны принятые предположения и все ресурсы, необходимые для осуществления планов. Если нехватка услуг или ресурсов не приводит к достижению целей плана, должны быть определены варианты эскалации данной проблемы и точная процедура ее решения.

8.7.3 Требования к ресурсам

Ресурсы, необходимые для обеспечения непрерывности и восстановления бизнеса, должны быть идентифицированы с учетом различных моментов времени. Ресурсы могут содержать:

a) персонал, включая:
- его безопасность,
- транспортную логистику,
- потребности в благосостоянии,
- непредвиденные расходы;

b) производственную площадь;

c) технологии, включая обмен информацией;

d) информацию, включая:
- финансовые аспекты (например, фонд оплаты труда),
- учетные записи клиентов,
- подробное описание поставщиков и причастных сторон,
- юридические документы (например, контракты, страховые полисы, документы о праве собственности и т.д.),
- другие документы по услугам (например, соглашение о техническом обслуживании);

e) запасы;

f) управление взаимоотношениями с причастными сторонами и обмен информацией с ними.

8.7.4 Ответственное лицо (лица)

Организация должна идентифицировать назначенное лицо (лиц), ответственное за управление непрерывностью бизнеса и этапами восстановления бизнеса.

Комментарии к 8.7.4 — Во многих случаях организация может назначить ответственным за непрерывность бизнеса то же лицо (лиц), которое идентифицировано(ы) в плане управления инцидентом и привлечь его (их) к управлению долгосрочными проблемами.

8.7.5 Формы и приложения

План обеспечения непрерывности бизнеса (если применимо) должен содержать актуализированную подробную контактную информацию для соответствующих внутренних и внешних агентств, организаций и поставщиков, на которых возложена обязанность по поддержке организации в конкретной ситуации.

План обеспечения непрерывности бизнеса должен включать журналы или формы для регистрации инцидента, ведения записей о жизненно важной информации, особенно относительно принятых решений.

Комментарий к 8.7.5 — План обеспечения непрерывности бизнеса может также включать в себя формы регистрации административных данных, например, используемых ресурсов, зарегистрированных расходных материалов, карт, рисунков и планов рабочих мест и офисов, особенно связанных с любыми альтернативными средствами, такими как области восстановления рабочего пространства и места хранения.

9 Применение, поддержка и анализ МНБ



Данный элемент жизненного цикла МНБ обеспечивает валидацию мероприятий МНБ организации путем применения, анализа и поддержки их актуализации.

9.1 Общие положения

Меры по обеспечению непрерывности бизнеса и управлению инцидентом не могут считаться надежными до тех пор, пока не будут полностью отработаны в процессе регулярных учений. Применение и проведение учений являются существенным фактором для развития рабочих групп, компетентности, доверия, навыков и знаний их участников, которые жизненно необходимы во время инцидента.

Мероприятия МНБ должны быть верифицированы путем аудита и самооценки для обеспечения их соответствия целям организации.

9.2 Программа проведения учений

Программа проведения учений должна быть совместима с областью применения плана(ов) непрерывности бизнеса и учитывать соответствующие законодательные и обязательные требования. Учения по программе позволяют организации:

- предвидеть ожидаемые последствия, например заблаговременно планировать последствия и масштабы распространения инцидентов;
- позволить организации разрабатывать инновационные решения.

Программа проведения учений должна быть разработана так, чтобы со временем обеспечить уверенную работоспособность МНБ в соответствии с планом.

Программа должна предусматривать:

- отработку применения технических, логистических, административных, процедурных и других функциональных систем МНБ;
- проведение учений по выполнению мероприятий и применению инфраструктуры МНБ (в т.ч. обработку ролей и обязанностей персонала, использование альтернативных рабочих мест и центров управления инцидентом и т.д.);
- валидацию способности к восстановлению технологий и телекоммуникаций, включая доступность и передислокацию соответствующего персонала.

Кроме того, эта программа может привести к улучшению способности организации к МНБ путем:

- приобретения практического опыта организации по восстановлению бизнеса после инцидента;
- верификации того, что МНБ включает все критические виды деятельности организации, их взаимосвязь и приоритеты;
- выявления предположений, которые должны быть пересмотрены;
- установления взаимного доверия среди участников проведенных учений;

- повышения общественной осведомленности о непрерывности бизнеса в данной организации путем публичного распространения информации о проведении учений;
- валидации эффективности и своевременности восстановления критических видов деятельности;
- демонстрации компетентности первичных групп по выполнению ответных мер в случае инцидентов и их альтернатив.

Комментарий к 9.2 — Учения обеспечивают документальные свидетельства компетентности и способности организации к непрерывности бизнеса и управлению инцидентом. Затраченные время и ресурсы обеспечивают доказательство того, что принятые стратегии МНБ путем применения планов непрерывности бизнеса приведут к установленному уровню способности организации к МНБ. Независимо от того, насколько хорошо разработаны и продуманы стратегия МНБ и планы обеспечения непрерывности бизнеса, после проведения учений обязательно будут выявлены области деятельности, требующие коррекции с точки зрения непрерывности бизнеса.

9.3 Проведение учений в области МНБ

9.3.1 Условия проведения учений должны быть реалистичны, тщательно спланированы и согласованы с причастными сторонами для того, чтобы свести к минимуму риск нарушения бизнес-процессов. Проведение учений должно быть спланировано таким образом, чтобы минимизировать риск возникновения инцидента, являющегося прямым результатом проведения учений.

9.3.2 Все проводимые учения должны иметь четко поставленные цели и задачи. Для анализа степени достижения поставленных целей и выполнения задач учений должен быть проведен анализ результатов учений. По результатам учений должен быть составлен отчет, содержащий сведения о проведенных учениях, время их проведения и практические рекомендации, выработанные на основе их результатов.

9.3.3 Масштаб и сложность учений должны соответствовать целям организации по восстановлению бизнеса.

9.3.4 Планы обеспечения непрерывности бизнеса и планы управления инцидентом должны быть отработаны на учениях для обеспечения их правильного выполнения, проверки их содержания, полноты и актуальности в случае возникновения реальной угрозы для организации.

Комментарии к 9.3.4 — Учения, в результате которых выявлены серьезные недоработки или упущения в МНБ, должны быть проведены повторно после выполнения корректирующих действий. Диапазон подходов и стратегий проведения учений в области МНБ приведен в таблице 1.

9.3.5 В программе проведения учений должны быть учтены роли всех сторон, включая ключевых поставщиков, привлекаемые к работам и услугам сторонние организации и др., которые потенциально будут участвовать в восстановительных действиях. Организация может привлекать такие стороны к своим учениям.

Таблица 1 — Типы и методы стратегий проведения учений по МНБ

Уровень сложности	Способ проведения учений	Процессы	Варианты действий	Периодичность проведения[a)]
Простой	Кабинетная проверка	Анализ/внесение поправок в содержание Исследование содержания МНБ	Актуализация/валидация Аудит /верификация	Не реже одного раза в год Ежегодно
Средний	Критический анализ плана	Исследование содержания МНБ	Включает отработку взаимодействия и валидацию обязанностей участников	Ежегодно
	Моделирование	Использование «искусственных» ситуаций для валидации того, что МНБ содержит необходимую и достаточную информацию для успешного восстановления бизнеса	Отработка соответствующих планов	Ежегодно или дважды в год
	Проведение учений по критическим видам деятельности	Инициирование управляемой ситуации, которая не подвергает опасности работу бизнеса в обычном нормальном режиме	Проведение определенных операций на альтернативных участках в течение фиксированного времени	Не более одного раза в год

Окончание таблицы 1

Уровень сложности	Способ проведения учений	Процессы	Варианты действий	Периодичность проведения[a)]
Сложный	Проведение учений по всему плану непрерывности бизнеса, включая управление инцидентом	Широкомасштабные учения в строениях/территориях/запрещенных зонах		Не более одного раза в год
[a)] Периодичность учений следует назначать в зависимости от потребностей организации, условий ее работы и требований причастных сторон. Однако программа учений должна быть гибкой, учитывать степень и направление изменений организации, а также результаты предыдущих учений. Вышеупомянутые методы поведения учений могут быть использованы для отдельных компонентов плана, одного и нескольких планов.				

9.4 Меры по поддержке МНБ

Должна быть установлена четко определенная и документированная программа поддержки МНБ. Эта программа должна обеспечивать анализ любых изменений (внутренних или внешних), воздействующих на организацию. Должны быть также идентифицированы любые новые продукция, услуги и связанные с ними виды деятельности, которые должны быть включены в программу поддержки МНБ.

В соответствии с программой поддержки МНБ организация должна:

- проводить анализ и актуализацию всех предположений, использованных в любых компонентах МНБ организации;
- доводить до сведения специалистов, ответственных за процесс управления изменениями, обновленные, исправленные или измененные политику, стратегии, решения, процессы и планы в области МНБ.

Примечание — В случае возникновения существенных изменений в бизнесе должен быть проведен пересмотр АВБ. Другие компоненты программы МНБ должны быть исправлены в соответствии с этими изменениями.

Результатами процесса поддержки МНБ являются:

- документированные свидетельства превентивного характера менеджмента организации и управления программой непрерывности ее бизнеса;
- верификация результатов учений и компетентности персонала, который должен осуществлять стратегию и планы в области МНБ;
- верификация мониторинга и управления риском в области непрерывности бизнеса;
- документированные свидетельства того, что существенные изменения структуры, продукции и услуг, действий, целей, штата и задач организации учтены в планах обеспечения непрерывности бизнеса и управления инцидентом организации.

Комментарий к 9.4 — Целью процесса поддержки МНБ является обеспечение компетентности и способности организации к МНБ, которые должны оставаться эффективными, актуальными и пригодными для достижения поставленных целей.

Действия по поддержке МНБ должны предусматривать изменение графика существующих учений при возникновении существенных изменений в стратегии, решениях или бизнес-процессах.

9.5 Анализ мер по МНБ

9.5.1 Высшее руководство организации через запланированные интервалы времени должно анализировать способность организации к МНБ, обеспечивать ее непрерывную пригодность, адекватность и эффективность. Этот анализ должен быть зарегистрирован.

9.5.2 Анализ мер по МНБ должен верифицировать соответствие политики организации в области МНБ всем применимым законам, нормам, стандартам, стратегиям, структурам и руководящим указаниям по успешной практике организаций.

9.5.3 Анализ мероприятий МНБ должен быть направлен на возможные потребности в изменениях политики, стратегии, целей и других элементов системы МНБ в соответствии с результатами проведенных учений, изменениями обстоятельств и обязательств по постоянному улучшению.

Комментарий к 9.5.3 — В контексте постоянного улучшения организация может исследовать сведения о новейших технологиях и практическом опыте в области МНБ, включая новые инструменты и методы. Эти знания должны быть оценены для установления их пригодности для организации.

9.5.4 Анализ может принять форму внутреннего или внешнего аудита или самооценки. Частота и выбор времени анализа могут быть обусловлены законодательными и обязательными требованиями в зависимости от размера, характера и юридического статуса организации. Анализ может быть инициирован под влиянием требований причастных сторон.

Аудит или самооценка программы МНБ организации должны верифицировать следующие положения:

- все ключевые продукция и услуги, поддерживающие их критические виды деятельности, и необходимые для этого ресурсы, идентифицированы и включены в стратегию непрерывности бизнеса организации;
- политика, стратегии, структура и планы в области непрерывности бизнеса организации точно отражают приоритеты, требования и задачи организации;
- компетентность и способность организации к МНБ эффективны, пригодны для достижения целей и дают возможность эффективного менеджмента, руководства, контроля и координации инцидента;
- решения организации в области непрерывности бизнеса являются эффективными, актуализированными и пригодными для достижения целей, а также соответствуют уровню риска организации;
- программы по поддержке и проведению учений в области непрерывности бизнеса организации эффективно внедрены;
- стратегии и планы МНБ включают в себя улучшения, необходимость которых выявлена во время инцидентов и проведения учений, и адекватно отражены в программе по поддержке МНБ;
- в организации существует непрерывная программа обучения и повышения осведомленности персонала в области МНБ;
- проводится эффективный обмен информацией по процедурам МНБ с соответствующим персоналом, сотрудники понимают свои роли, обязанности и ответственность;
- процессы управления изменениями работают в конкретных местах и эффективно функционируют.

9.5.5 Аудит

Организация должна обеспечить независимый аудит своей компетентности и способности к МНБ, чтобы идентифицировать фактические и потенциальные несоответствия. Должны быть установлены, внедрены и поддерживаться в рабочем состоянии процедуры проведения аудита. Независимый аудит должен проводиться компетентными лицами (внутренними или внешними).

9.5.6 Самооценка

Процесс самооценки МНБ играет большую роль в обеспечении наличия у организации разумной, эффективной и пригодной для достижения поставленных целей МНБ. Самооценка обеспечивает качественную верификацию способности организации к восстановлению бизнеса после инцидента. Самооценка должна быть проведена в соответствии с поставленными целями организации. Должны быть также учтены соответствующие промышленные стандарты и передовой опыт в данной области.

10 Внедрение МНБ в культуру организации



Для получения положительного результата непрерывность бизнеса должна стать частью системы ценностей и менеджмента организации, независимо от ее размера или сферы деятельности. На каждой стадии процесса МНБ существуют возможности для создания и повышения культуры обеспечения непрерывности бизнеса в организации.

10.1 Общие положения

В результате построения, развития и внедрения МНБ в культуру организации МНБ становится частью основных активов и эффективного менеджмента организации.

Внедрение МНБ в культуру организации позволяет:

- более эффективно разрабатывать и развивать программу МНБ;
- вызывать большее доверие со стороны причастных сторон (особенно персонала и потребителей) к способности организации справляться с любыми нарушениями функционирования бизнеса;
- увеличить устойчивость организации в долгосрочной перспективе путем возможности применения МНБ при принятии решений на всех уровнях;
- минимизировать вероятность возникновения нарушений и размер их последствий.

Внедрение МНБ в культуру организации должно быть основано на:

- лидерстве руководителей организации;
- распределении ответственности и полномочий (см. 5.2);
- повышении осведомленности персонала об МНБ;
- обучении навыкам работы в МНБ;
- отработке планов во время учений.

Комментарий к 10.1 — Создание МНБ и его внедрение в организации может оказаться длительным и сложным процессом, который может усугубляться значительным сопротивлением со стороны персонала. Понимание существующей культуры внутри организации может помочь в разработке соответствующей программы внедрения и развития в ней культуры МНБ.

Все сотрудники должны понять, что МНБ — это серьезная задача для организации, и они играют важную роль в поддержке непрерывности поставки продукции и услуг их клиентам и потребителям.

10.2 Осведомленность

Организация должна установить процесс идентификации и определения требований к осведомленности об МНБ в организации и оценки эффективности создания и повышения осведомленности персонала.

Персонал, вовлеченный в МНБ, должен постоянно пополнять свои знания об МНБ из внешних источников. Этого можно достичь путем сотрудничества с руководством аварийно-спасательных служб, органов местного самоуправления и других подобных организаций.

Организация должна повышать, улучшать и поддерживать осведомленность путем внедрения программы непрерывного образования и информирования об МНБ всего персонала.

Такая программа может включать в себя:

- консультации с персоналом на всех уровнях организации относительно создания программы МНБ;
- обсуждение вопросов МНБ в информационных бюллетенях организации, при проведении инструктажа, в рамках вводных программ или в журналах;
- описание МНБ на веб-сайте и/или во внутренней сети организации;
- изучение опыта внутренних и внешних инцидентов;
- внесение МНБ в качестве пункта повестки дня различных совещаний;
- отработку в рамках учений планов обеспечения непрерывности на альтернативном рабочем месте или производственной площади (например, на участке восстановления деятельности);
- посещение установленных альтернативных рабочих мест или производственных площадей (например, участка восстановления деятельности).

Организация может расширить свою программу осведомленности об МНБ на ее поставщиков и другие причастные стороны.

Комментарий к 10.2 — Для повышения и поддержания осведомленности об МНБ всего персонала необходимо обеспечить понимание персоналом важности МНБ для организации. Персонал должен быть уверен, что МНБ — это долгосрочная инициатива, имеющая постоянную поддержку со стороны высшего руководства.

10.3 Обучение навыкам

Организация должна установить процесс идентификации потребностей в обучении требованиям МНБ, проведения этого обучения для соответствующих участников МНБ и оценки его эффективности.

Организация должна организовать обучение:

a) персонала, вовлеченного в МНБ, для таких задач, как:
- управление программой МНБ;
- проведение анализа воздействия на бизнес;
- разработка и внедрение МНБ;
- реализация программы учений по МНБ;
- оценка риска и угроз;
- обмен информацией со СМИ.

b) персонала, не вовлеченного в МНБ, от которого требуется наличие соответствующих навыков для выполнения ответных мер при появлении инцидента и/или восстановления бизнеса.

Навыки для выполнения таких ответных мер и компетентность персонала организации должны развиваться с помощью практического обучения, включая активное участие в учениях в области МНБ.

Библиография

[1] ISO 9000:2005 Quality management systems — Fundamentals and vocabulary (ИСО 9000:2005 Системы менеджмента качества. Основные положения и словарь)[1)]
[2] ISO/IEC Guide 51: 1999 Safety aspects — Guidelines for their inclusion in standards (ИСО/МЭК Руководство 51:1999 Аспекты безопасности. Руководящие указания по включению их в стандарты)[2)]
[3] ISO Guide 73:2009 Risk management. Vocabulary. (ИСО Руководство 73:2009 Управление риском. Словарь)[3)]
[4] ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements (ИСО/МЭК 27001:2005 Информационная технология. Методы безопасности. Информационные системы управления безопасности. Требования)[4)]
[5] PAS 77:2006 IT Service Continuity Management. Code of Practice (PAS 77:2006 Менеджмент непрерывностью ИТ услуг. Практическое руководство)
[6] ISO/IEC 20000-1:2005 Information technology — Service management — Part 1: Specification (ИСО/МЭК 20000-1: 2005 Информационные технологии. Сервисный менеджмент. Часть 1. Спецификация)
[7] ISO/IEC 20000-2:2005 Information technology — Service management — Part 2: Code of practice (ИСО/МЭК 20000-2: 2005 Информационные технологии. Сервисный менеджмент. Часть 2. Общепринятая практика)

[1)] ГОСТ Р ИСО 9000—2008 «Системы менеджмента качества. Основные положения и словарь» идентичен ИСО 9000:2005.

[2)] ГОСТ Р 51898—2002 «Аспекты безопасности. Правила включения в стандарты» идентичен ИСО/МЭК Guide 51:1999.

[3)] ГОСТ Р 51897—2002 «Менеджмент риска. Термины и определения» идентичен ИСО/МЭК Guide 73:2002.

[4)] ГОСТ ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» идентичен ИСО/МЭК 27001:2005.

УДК 658:562.014:006.354 ОКС 03.100.01 Т59

Ключевые слова: непрерывность бизнеса, менеджмент непрерывности бизнеса, программа менеджмента непрерывности бизнеса, стратегия обеспечения непрерывности бизнеса, воздействие, инцидент, план управления инцидентом, чрезвычайная ситуация, последствие, разрушение бизнеса, критические виды деятельности, риск, допустимый совокупный риск, оценка риска, устойчивость организации

Редактор *А.Д. Стулова*
Технический редактор *В.Н. Прусакова*
Корректор *М.В. Бучная*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 18.01.2011. Подписано в печать 04.02.2011. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 4,65. Уч.-изд. л. 4,30. Тираж 114 экз. Зак. 69.

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.

gost.e-ecolog.ru