ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55235.3— 2012

ПРАКТИЧЕСКИЕ АСПЕКТЫ МЕНЕДЖМЕНТА НЕПРЕРЫВНОСТИ БИЗНЕСА

Применение к информационным и коммуникационным технологиям

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 29 ноября 2012 г. № 1278-ст

4 Настоящий стандарт идентичен международному стандарту BS 25777:2008 «Менеджмент непрерывности информационных и коммуникационных технологий. Практическое руководство» («Information and communications technology continuity management — Code of practice», IDT).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Июнь 2020 г.

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

© Стандартинформ, оформление, 2014, 2020

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 Менеджмент программы обеспечения непрерывности информационных и коммуникационных технологий 4
4 Анализ требований к обеспечению непрерывности информационных и коммуникационных технологий 7
5 Определение стратегий обеспечения непрерывности информационных и коммуникационных технологий 9
6 Внедрение стратегий обеспечения непрерывности информационных и коммуникационных технологий 13
7 Проведение учений и тестов 17
8 Поддержка, анализ и улучшение 21
Приложение А (справочное) Основные этапы менеджмента непрерывности информационных и коммуникационных технологий 24
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документа, указанных в библиографии настоящего стандарта, национальным и межгосударственному стандартам 26
Библиография 27

Введение

Менеджмент непрерывности информационных и коммуникационных технологий и его взаимосвязь с менеджментом непрерывности бизнеса

Процессы производства продукции и предоставления услуг во многих организациях напрямую зависят от информационных и коммуникационных технологий (ИКТ). Сбои в работе информационных и коммуникационных технологий могут представлять собой стратегическую опасность для организации, при возникновении которой может быть нарушены нормальный ход деятельности организации и ее репутация. Последствия нарушения услуг информационных и коммуникационных технологий могут быть разноплановыми, зачастую неочевидными в момент сбоя.

Менеджмент непрерывности информационных и коммуникационных технологий является частью общего процесса менеджмента непрерывности бизнеса (МНБ) организации. Основной целью МНБ является обеспечение непрерывности процессов организации и ее способность быстро и эффективно реагировать на все нарушения и сбои в работе. Поэтому наряду с установленными приоритетами в области МНБ, организация также должна проанализировать и определить требования к обеспечению непрерывности информационных и коммуникационных технологий. Менеджмент непрерывности информационных и коммуникационных технологий обеспечивает непрерывность предоставления услуг информационных и коммуникационных технологий[1)] и возможность их восстановления до требуемого уровня в сроки, устанавливаемые высшим руководством. Результативность МНБ зависит от менеджмента непрерывности информационно-коммуникационных технологий, обеспечивающего достижение установленных целей организации, особенно в моменты сбоев в их работе. Для успешного внедрения МНБ и менеджмента непрерывности информационно-коммуникационных технологий необходимо, чтобы они стали неотъемлемой частью культуры организации (см. рисунок 1).

МНБ и менеджмент непрерывности информационно-коммуникационных технологий обеспечивают эффективность стратегического и оперативного менеджмента, а также устойчивость развития организации. Ответственность за поддержание непрерывности работы организации, в том числе в период нарушений и сбоев, несет высшее руководство. В соответствии с законодательными и обязательными требованиями организации должны иметь выбранные с учетом оценки риска эффективные средства управления, включая МНБ.

Менеджмент непрерывности информационных и коммуникационных технологий и общая стратегия организации

Менеджмент непрерывности информационных и коммуникационных технологий является важным элементом общей стратегии менеджмента информационных и коммуникационных технологий и оказываемых услуг, необходимых для достижения установленных целей организации, а также ее способности непрерывно поставлять ключевые продукцию и услуги при возникновении неблагоприятных ситуаций.

Преимущества внедрения эффективного менеджмента непрерывности информационных и коммуникационных технологий

Все виды деятельности организации могут быть подвергнуты нарушениям и сбоям под воздействием внутренних и внешних событий, таких как технологические отказы, пожары, наводнения, сбои в работе коммунальных сетей, заболевания персонала или преднамеренное нанесение ущерба. Менеджмент непрерывности информационных и коммуникационных технологий обеспечивает устойчивость работы организации путем предупреждения нарушений и сбоев информационных и коммуникационных технологий и восстановления после их возникновения.

Преимуществами внедрения организацией эффективного менеджмента непрерывности информационных и коммуникационных технологий являются:

- анализ, понимание угроз и уязвимостей при предоставлении услуг информационных и коммуникационных технологий;

[1)] Включая поддерживающую информационную и телекоммуникационную инфраструктуру (сети и их компоненты), компьютерные аппаратные средства, программное обеспечение, услуги информационных и коммуникационных технологий и сопровождение (например, служба технической поддержки).

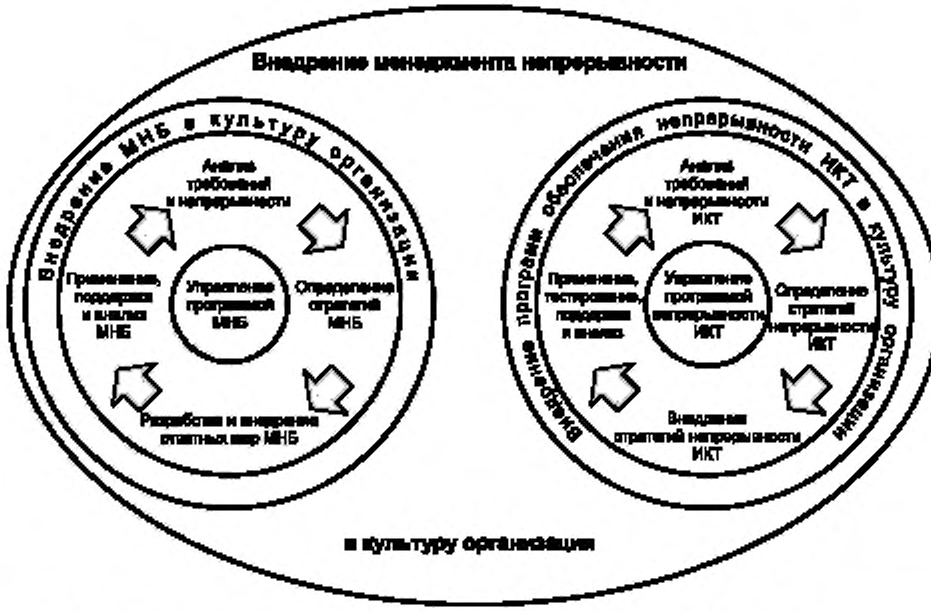


Рисунок 1 — Взаимосвязь между менеджментом непрерывности информационных и коммуникационных технологий и менеджментом непрерывности бизнеса

- идентификация воздействий нарушений и сбоев информационных и коммуникационных технологий;

- обеспечение эффективного сотрудничества между персоналом организации и поставщиками услуг информационных и коммуникационных технологий (внутренними и внешними);

- повышение компетентности персонала в области информационных и коммуникационных технологий путем демонстрации навыков применения ответных мер в соответствии с планами обеспечения непрерывности информационных и коммуникационных технологий и реализации мероприятий по тестированию непрерывности работы информационных и коммуникационных технологий;

- обеспечение гарантированного уровня предоставления услуг информационных и коммуникационных технологий и получения необходимой технической поддержки и обмена информацией в случае сбоя;

- повышение доверия к стратегии непрерывности бизнеса организации путем установления связи между инвестициями в информационные и коммуникационные технологии и требованиями бизнеса, а также предоставление гарантированной защиты услуг информационных и коммуникационных технологий на установленном уровне в соответствии с их приоритетностью для организации;

- обеспечение достаточности инвестиций и экономической эффективности услуг информационных и коммуникационных технологий с учетом:

- уровня зависимости организации от услуг информационных и коммуникационных технологий;

- характера, расположения, взаимозависимости и использования компонентов услуг информационных и коммуникационных технологий;

- повышение репутации организации от внедрения услуг информационных и коммуникационных технологий;

- получение дополнительных конкурентных преимуществ путем демонстрации способности обеспечить непрерывность бизнеса и поставки продукции и услуг в момент возникновения нарушений и сбоев;

- анализ и регистрация ожиданий всех причастных к деятельности организации сторон и связь этих ожиданий с использованием услуг информационных и коммуникационных технологий.

Непрерывность информационных и коммуникационных технологий в рамках общей стратегии их развития можно обеспечить с меньшими затратами уже на стадии проектирования и разработки услуг

информационных и коммуникационных технологий. Внедрение элементов менеджмента непрерывности бизнеса на стадии проектирования помогает лучше интегрировать, понять, уменьшить затраты и упростить поддержку услуг информационных и коммуникационных технологий. Внедрение системы менеджмента непрерывности услуг информационных и коммуникационных технологий может быть сложной и дорогостоящей задачей. Содержание программы обеспечения непрерывности информационных и коммуникационных технологий часто зависит от склонности организации к риску.

Основные направления менеджмента непрерывности информационных и коммуникационных технологий

Менеджмент непрерывности информационных и коммуникационных технологий направлен на определение вероятности и последствий нарушений и/или сбоев, а также на обеспечение способности организации к быстрому их обнаружению и принятию необходимых ответных мер по восстановлению нормального хода деятельности. Для этого организация должна проводить мониторинг услуг информационных и коммуникационных технологий, направленный на обеспечение:

- жизнеспособности услуг и возможности их восстановления на установленном уровне;
- своевременного выявления, анализа и обработки непредвиденных событий при предоставлении услуги;
- исследования связи между услугами информационных и коммуникационных технологий и изменениями внешних факторов[1)] и использования полученной информации для оценки риска и воздействия изменений;
- исследования зависимости деятельности организации от технических компонентов[2)] и использования полученной информации для оценки риска и воздействия изменений.

Процессы и решения в области менеджмента непрерывности информационных и коммуникационных технологий необходимы для обеспечения выполнения законодательных и обязательных требований, таких как защита персональных данных.

Принципы менеджмента непрерывности информационных и коммуникационных технологий

Основой непрерывности информационных и коммуникационных технологий являются шесть ключевых принципов:

a) **Защита:** Защита среды информационных и коммуникационных технологий от инцидентов, сбоев и нарушений путем повышения жизнеспособности услуг информационных и коммуникационных технологий крайне важна для поддержания необходимого уровня доступности услуги для организации.

b) **Выявление:** Выявление инцидентов на ранней стадии минимизирует их воздействие на услуги, уменьшает объем работы по восстановлению и сохраняет качество услуги информационных и коммуникационных технологий.

c) **Реагирование:** Адекватное реагирование на инцидент приводит к более эффективному восстановлению и позволяет снизить время простоя. Неадекватная реакция может привести к превращению незначительного инцидента в серьезную проблему.

d) **Восстановление:** Идентификация и внедрение соответствующей стратегии восстановления обеспечивают своевременное восстановление предоставления услуг и поддержку целостности данных. Расстановка приоритетов при восстановлении позволяет в первую очередь восстановить наиболее важные для организации услуги. Менее важные услуги могут быть восстановлены позднее или, в некоторых случаях, не подлежат восстановлению.

e) **Эксплуатация:** Обеспечение возможности предоставления услуг в режиме аварийного восстановления до полного возвращения системы к рабочему состоянию. Восстановление может потребовать определенного времени и увеличения масштаба операций по аварийному восстановлению услуг, удовлетворяющих возрастающие потребности бизнеса.

f) **Возврат:** Разработка стратегии для каждого плана непрерывности информационных и коммуникационных технологий, обеспечивающей переход организации из режима аварийного восстановления информационных и коммуникационных технологий к состоянию, при котором услуги могут поддерживать нормальный режим функционирования бизнеса.

[1)] Такие как продавцы, клиенты, партнеры в цепи поставок и поставщики услуг по аутсорсингу.

[2)] Примеры приведены в разделе «Элементы услуг информационных и коммуникационных технологий».

Элементы услуг информационных и коммуникационных технологий

Ключевые элементы услуг информационных и коммуникационных технологий включают (см. также приложение А):

a) персонал: специалисты (включая их заместителей), обладающие соответствующими знаниями и способные замещать смежные функции;

b) производственные площади: физическая среда расположения ресурсов в области информационных и коммуникационных технологий;

c) технологии:

1) серверы, средства хранения информации, устройства записи, стеллажи, а также другие аппаратные средства и приспособления;

2) информационно-коммуникационные сети, включая средства передачи данных и голосовой связи, в том числе коммутаторы и маршрутизаторы;

3) программное обеспечение, включая программное обеспечение операционной системы и прикладное программное обеспечение, взаимосвязи и интерфейсы между приложениями и процедурами пакетной обработки.

d) информация: данные приложений, голосовые данные и прочие типы данных;

e) процессы: включая сопроводительную документацию, описывающую конфигурацию ресурсов информационных и коммуникационных технологий и обеспечивающую эффективное функционирование, восстановление и сопровождение услуг информационных и коммуникационных технологий;

f) поставщики: прочие компоненты услуг полного цикла[1)] в случае, если предоставление услуг информационных и коммуникационных технологий зависит от стороннего поставщика услуг или другой организации в цепи поставки, например, поставщика данных о финансовом рынке, телекоммуникационного оператора или поставщика услуг доступа в Интернет.

[1)] От компьютерного зала (который может быть центром данных и узлом связи) к рабочему столу пользователя или другому каналу доставки, такому как веб-приложение, мобильный телефон, пункт продажи и банкомат.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРАКТИЧЕСКИЕ АСПЕКТЫ МЕНЕДЖМЕНТА НЕПРЕРЫВНОСТИ БИЗНЕСА

Применение к информационным и коммуникационным технологиям

Practical aspects of business continuity management.
Code of practice for information and communications technologies

Дата введения — 2013—12—01

1 Область применения

Настоящий стандарт содержит рекомендации по менеджменту непрерывности информационных и коммуникационных технологий в рамках общей структуры менеджмента непрерывности бизнеса[1)].

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

2.1 **деятельность** (activity): Процесс или набор процессов, осуществляемых организацией (или от ее имени), который выпускает или поддерживает один или несколько видов продукции или услуг.

Примечание — Примеры таких процессов включают бухгалтерский учет, обработку вызовов, информационные технологии (ИТ), производство, распространение.

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 операций на установленном приемлемом уровне.

2.3 **менеджмент непрерывности бизнеса** (business continuity management; BCM); МНБ: Полный процесс управления, предусматривающий идентификацию потенциальных угроз и их воздействия на деятельность организации, который создает основу для повышения устойчивости деятельности организации к инцидентам и направлен на реализацию эффективных ответных мер, что обеспечивает защиту интересов ключевых причастных сторон, репутации организации, ее бренда и деятельности.

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, направленных на осуществление и актуализацию планов непрерывности бизнеса.

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

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

2.5 **план обеспечения непрерывности бизнеса; ПНБ** (business continuity plan; BCP): Набор документированных процедур и информации, которые разработаны, взаимоувязаны 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.

[1)] Общая структура менеджмента непрерывности бизнеса установлена в [1].

Издание официальное

2.6 **программа менеджмента непрерывности бизнеса** (business continuity management programme): Программа менеджмента по непрерывному управлению и руководству действия по идентификации воздействия потенциальных потерь, поддержке стратегии непрерывности бизнеса и планов восстановления бизнеса, обеспечению непрерывности производства продукции и предоставления услуг, внедрению, анализу и поддержанию в рабочем состоянии менеджмента непрерывности бизнеса организации путем обучения и проведения учений, которая должна быть обеспечена необходимыми ресурсами.

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

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

2.9 **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.

2.10 **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.

2.11 **нарушение деятельности организации, сбой** (disruption): Невозможность плановой поставки продукции или предоставления услуг или перебои в этой деятельности, вызванные ожидаемым (например, забастовка рабочих) или непредвиденным (например, отключение электрической энергии) событием или явлением.

2.12 **учения** (exercise): Мероприятия, предусмотренных планами обеспечения непрерывности бизнеса, в процессе которых частично или полностью происходит отработка действий (репетиция), направленными на то, чтобы планы содержали необходимую информацию и при их выполнении приводили 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 которых участники инсценируют возможную ситуацию с целью выявления потенциальных проблем, их преодоления до наступления реального инцидента.

2.13 **непрерывность информационных и коммуникационных технологий** (ICT continuity): Способность организации осуществлять планирование и реагировать на инциденты и нарушения деятельности для обеспечения продолжения предоставления услуги информационных и коммуникационных технологий на приемлемом, заранее установленном уровне.

2.14 **восстановление информационных и коммуникационных технологий после нарушения или сбоя** (ICT disaster recovery): Действия и программы, выполняемые при выявлении нарушения, предназначенные для восстановления услуг информационных и коммуникационных технологий организации.

2.15 **услуги**[1] **информационных и коммуникационных технологий** (ICT services): Обеспечение доступа к информации, ее использованию, а также внутреннего и внешнего обмена информацией, на основе данных, персонала, физических и логических активов, состоящих из средств и/или оборудования, которые поддерживают повседневную деятельность организации.

2.16 **воздействие** (impact): Последствие для конкретной ситуации с установленной оценкой.

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

2.18 **план управления в условиях инцидента** (incident management plan): 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 условиях инцидента.

---

[1] В сфере информационных и коммуникационных технологий такие услуги часто называют сервисом.

2.19 **активация плана** (invocation): Объявление о том, что план обеспечения непрерывности бизнеса организации должен быть введен в действие, чтобы продолжить предоставление ключевых услуг или продукции.

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

2.21 **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 комбинации из них.

Примечание 1 — Распределение обычно является упорядоченным.

Примечание 2 — Организация может быть государственной или частной.

[ISO 9000:2005]

2.22 **целевой срок восстановления, директивный срок восстановления** (recovery point objective; RPO): Момент времени, к которому необходимо восстановить данные, чтобы возобновить предоставление услуги информационных и коммуникационных технологий.

2.23 **целевое время восстановления** (recovery time objective, RTO): Период времени, установленный для возобновления деятельности производства продукции, услуги после инцидента.

Примечание — В контексте управления непрерывностью информационных и коммуникационных технологий целевое время восстановления измеряется от момента активации плана до возобновления предоставления услуги. Целевое время восстановления информационных и коммуникационных технологий в целом меньше целевого времени восстановления для продукции, услуг или деятельности.

2.24 **способность к восстановлению** (resilience): Способность системы информационных и коммуникационных технологий обеспечивать и поддерживать приемлемый уровень обслуживания при различных нарушениях нормальной деятельности и сбоях.

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

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

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

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

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

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

2.26 **аппетит риска** (risk appetite): Общая величина риска, который организация готова принять, перенести или действию которого готова подвергнуться в любой момент времени.

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

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

2.29 **причастные стороны** (stakeholders): Лица, заинтересованные в достижении организацией ее целей.

Примечание — Этот термин охватывает штатных сотрудников и сотрудников сторонних организаций-соисполнителей, клиентов, поставщиков, партнеров, дистрибьюторов, инвесторов, страховщиков, акционеров, собственников, правительство и регулирующие органы.

[1)] В соответствии с Федеральным Законом «О техническом регулировании» от 27.12.2002 г. № 184-ФЗ «риск — это вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда».

2.30 **тестирование** (testing): Принудительно вызванный отказ всех или части систем информационных и коммуникационных технологий при определенных условиях с целью проверки качества проведенного восстановления.

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

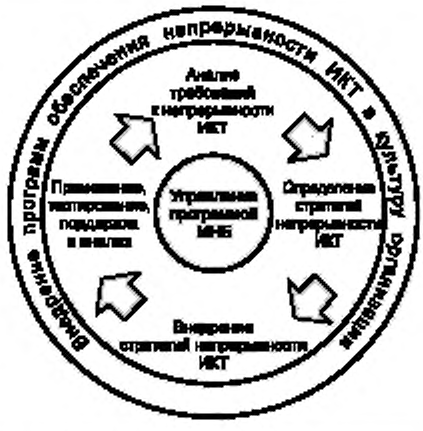
Примечание — Высшее руководство, особенно в крупной корпорации, не всегда может быть непосредственно вовлечено в МНБ, однако в этом случае высшее руководство несет ответственность за установленный в организации порядок соподчиненности. В малой организации высшее руководство может быть владельцем этого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

[ISO 9000:2005]

2.32 **уязвимость** (vulnerability): Слабые стороны услуг информационных и коммуникационных технологий или деятельности, которые могут в определенный момент стать объектом воздействия угрозы.

Примечание — Примерами уязвимостей могут служить: несоответствующая нормативам противопожарная защита, коммунальное снабжение и неадекватность системы безопасности.

3 Менеджмент программы обеспечения непрерывности информационных и коммуникационных технологий



Цель:

Разработка, внедрение и поддержка документированной процедуры по менеджменту непрерывности информационных и коммуникационных технологий

3.1 Создание системы менеджмента непрерывности информационных и коммуникационных технологий

Организация должна разрабатывать, внедрять, поддерживать и постоянно улучшать систему менеджмента непрерывности информационных и коммуникационных технологий. Менеджмент непрерывности информационных и коммуникационных технологий должен обеспечивать:

a) установление целей менеджмента непрерывности информационных и коммуникационных технологий, которые должны быть четко сформулированы, понятны и доведены до сведения соответствующих причастных сторон;

b) демонстрацию приверженности высшего руководства к менеджменту непрерывности информационных и коммуникационных технологий в рамках общего менеджмента непрерывности бизнеса;

c) выделение необходимых ресурсов;

d) обеспечение необходимой компетентности лиц, ответственных за менеджмент непрерывности информационных и коммуникационных технологий, достаточной для его осуществления.

3.2 Область применения системы менеджмента непрерывности информационных и коммуникационных технологий

3.2.1 Общие положения

Организация должна определить область применения и цели системы менеджмента непрерывности информационных и коммуникационных технологий с учетом:

a) требований к непрерывности информационных и коммуникационных технологий;

b) области применения, целей и требований системы менеджмента непрерывности бизнеса, включая законодательные, обязательные и иные требования;

c) приемлемого уровня риска и видов риска, связанных с информационными и коммуникационными технологиями;

d) требований к непрерывности бизнеса;

e) интересов ключевых причастных сторон.

Организация должна идентифицировать системы информационных и коммуникационных технологий, входящие в область применения системы менеджмента непрерывности бизнеса и информационных и коммуникационных технологий.

3.2.2 Политика в области непрерывности информационных и коммуникационных технологий

Высшее руководство должно разработать СМБ и продемонстрировать приверженность политике менеджмента непрерывности информационных и коммуникационных технологий в рамках общей политики МНБ.

Политика должна включать в себя или ссылаться на:

a) стратегию информационных и коммуникационных технологий организации;

b) область применения системы менеджмента непрерывности информационных и коммуникационных технологий, в том числе все ограничения и исключения.

Политика должна быть:

i) утверждена высшим руководством;

ii) доведена до сведения всего персонала, работающего в организации или от ее имени;

iii) проанализирована на постоянную пригодность через запланированные интервалы времени, а также в случае значительных изменений.

3.2.3 Обеспечение ресурсами

Организация должна определить и выделить ресурсы, необходимые для создания, внедрения, функционирования и поддержки системы менеджмента непрерывности информационных и коммуникационных технологий. Функции, обязанности, компетентность и полномочия в области менеджмента непрерывности информационных и коммуникационных технологий должны быть определены и документально оформлены.

Высшее руководство должно:

a) назначить ответственного за политику в области менеджмента непрерывности информационных и коммуникационных технологий, ее внедрение и наделить его соответствующими полномочиями;

b) назначить одного или нескольких ответственных за внедрение и поддержку системы менеджмента непрерывности информационных и коммуникационных технологий.

3.3 Внедрение менеджмента непрерывности информационных и коммуникационных технологий

Цель:

Внедрение менеджмента непрерывности информационных и коммуникационных технологий в повседневные операции информационных и коммуникационных технологий и процессы менеджмента организации путем повышения осведомленности и обучения соответствующего персонала, что должно стать основной ценностью общей системы менеджмента непрерывности бизнеса и информационных и коммуникационных технологий.

3.3.1 Повышение осведомленности

Организация должна:

a) повышать, расширять и поддерживать осведомленность персонала путем проведения постоянного обучения и использования информационных программ;

b) установить процесс оценки результативности процедур повышения осведомленности;

c) обеспечить осведомленность персонала о его участии в достижении целей в области непрерывности информационных и коммуникационных технологий.

3.3.2 Квалификация персонала в области информационных и коммуникационных технологий

Организация должна обеспечивать необходимый уровень квалификации персонала, на который возложены обязанности по менеджменту непрерывности информационных и коммуникационных технологий, путем:

a) определения необходимого уровня квалификации персонала;

b) проведения анализа потребностей в обучении персонала;

c) проведения обучения;

d) обеспечения достижения персоналом необходимого уровня квалификации;

e) ведения записей об обучении, образовании, навыках, опыте и квалификации.

3.4 Документация и записи по менеджменту непрерывности информационных и коммуникационных технологий

В организации должна быть разработана документация по следующим аспектам менеджмента непрерывности информационных и коммуникационных технологий:

a) политике в области менеджмента непрерывности информационных и коммуникационных технологий;

b) перечню критических видов услуг информационных и коммуникационных технологий, утвержденному высшим руководством, для которых должно быть установлено целевое время восстановления;

c) результатам анализа воздействия на бизнес;

d) результатам оценки риска;

e) стратегии обеспечения непрерывности для каждой услуги информационных и коммуникационных технологий;

f) планам менеджмента непрерывности и управления инцидентами для информационных и коммуникационных технологий;

g) актуализированным контактным данным персонала, служб и организаций, а также ресурсам, которые могут потребоваться для поддержки стратегий реагирования;

h) программам и записям о проведении обучения и повышении осведомленности персонала;

i) программам проведения учений и тестов, полученным результатам, а также записям о предупреждающих и корректирующих действиях (см. 8.3);

j) анализу последствий инцидентов;

k) описанию компонентов информационных и коммуникационных технологий и способам их конфигурации и/или взаимодействия для предоставления каждой услуги.

Организация должна управлять, регистрировать и поддерживать записи, необходимые для получения объективных свидетельств эффективности функционирования системы менеджмента непрерывности информационных и коммуникационных технологий.

Организация должна установить документированные процедуры идентификации средств управления документацией и записями в области менеджмента непрерывности информационных и коммуникационных технологий.

3.5 Мониторинг и анализ системы менеджмента непрерывности информационных и коммуникационных технологий

Сотрудник, ответственный за непрерывность информационных и коммуникационных технологий (см. 3.2.3), должен проводить мониторинг и анализ менеджмента непрерывности информационных и коммуникационных технологий, направленный на обеспечение его результативности и эффективности. Анализ должен быть направлен на оценку соответствия политики, целей и области применения системы менеджмента непрерывности информационных и коммуникационных технологий. В соответствии с полученными результатами анализа необходимо определить и санкционировать корректирующие действия и меры по улучшению.

3.6 Предупреждающие и корректирующие действия

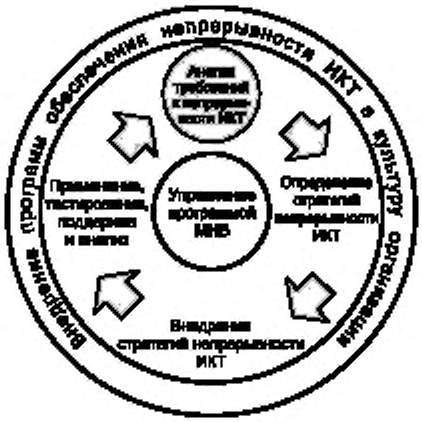
Организация должна постоянно улучшать менеджмент непрерывности информационных и коммуникационных технологий путем применения предупреждающих и корректирующих действий. Эти действия должны соответствовать потенциальному воздействию проблем, выявленных в процессе анализа воздействия на бизнес организации, а также уровню приемлемости риска для организации.

Результаты предупреждающих и корректирующих действий должны быть отражены, учтены в соответствующей документации по менеджменту непрерывности информационных и коммуникационных технологий.

3.7 Постоянное улучшение

Организация должна постоянно повышать результативность менеджмента непрерывности информационных и коммуникационных технологий путем анализа политики и целей, результатов аудита, предупреждающих и корректирующих действий, а также анализа со стороны руководства.

4 Анализ требований к обеспечению непрерывности информационных и коммуникационных технологий



Цель:

Определение требований к непрерывности услуг информационных и коммуникационных технологий, необходимых для выполнения требований к общему менеджменту непрерывности бизнеса организации, проведение анализа текущей конфигурации (физической и логической) услуг информационных и коммуникационных технологий; и определение разницы между имеющейся способностью к обеспечению непрерывности информационных и коммуникационных технологий и требованиями непрерывности бизнеса для каждого критического вида услуг информационных и коммуникационных технологий

4.1 Определение требований к непрерывности информационных и коммуникационных технологий для выполнения требований непрерывности бизнеса

4.1.1 В соответствии с программой МНБ организация должна расставить приоритеты в действиях по восстановлению и определить минимальный уровень функционирования после возобновления работ для каждого критического вида деятельности.

Требования непрерывности бизнеса должны быть согласованы с высшим руководством организации. В результате должно быть документально оформлено и утверждено для каждого критического вида деятельности целевое время восстановления и минимальный уровень функционирования после возобновления работ. Критические виды деятельности могут включать в себя предоставление услуг информационных и коммуникационных технологий, таких как служба технической поддержки.

4.1.2 Организация должна определить и документировать услуги информационных и коммуникационных технологий. Описание услуг информационных и коммуникационных технологий должно быть доступно и однозначно для понимания персоналом организации. Для каждой из определенных услуг информационных и коммуникационных технологий может быть создано краткое описание, так как персонал организации и специалисты по информационным и коммуникационным технологиям иногда используют различные наименования для одной и той же услуги или по-разному излагают ее содержание. Для каждой из определенных услуг информационных и коммуникационных технологий должен быть установлен перечень поддерживаемых продукции или услуг организации.

4.1.3 Организация должна определить и документировать услуги информационных и коммуникационных технологий, которые необходимы для выполнения требований непрерывности бизнеса. Необходимо установить минимальные требования к производительности в области услуг информационных и коммуникационных технологий, необходимой для выполнения действий по восстановлению критических видов деятельности организации.

Примечание — Целевое время восстановления услуг информационных и коммуникационных технологий обычно меньше, чем целевое время восстановления критического вида деятельности, которую она поддерживает.

(Если стратегия непрерывности бизнеса требует применения временных мер, таких как переход на процедуры с ручным управлением вместо применения автоматизированных услуг информационных и коммуникационных технологий, то целевое время восстановления услуг информационных и коммуникационных технологий может превышать целевое время восстановления критического вида деятельности).

4.1.4 Перечень критических видов услуг информационных и коммуникационных технологий (4.1.2) и соответствующие требования к непрерывности информационных и коммуникационных технологий (4.1.3) должны быть утверждены высшим руководством.

4.2 Анализ критических видов услуг информационных и коммуникационных технологий

4.2.1 Для каждого критического вида услуг информационных и коммуникационных технологий в соответствии с перечнем, утвержденным высшим руководством, необходимо описать и задокументировать все компоненты услуги, в том числе должны быть установлены конфигурация услуги и ее взаимосвязь с другими компонентами, необходимыми для предоставления каждой услуги. Следует документировать конфигурацию нормальной среды предоставления услуги информационных и коммуникационных технологий и конфигурацию среды предоставления услуги, направленной на обеспечение непрерывности информационных и коммуникационных технологий.

4.2.2 Для каждого критического вида услуг информационных и коммуникационных технологий необходимо провести анализ текущей способности организации к обеспечению непрерывности, направленной на предупреждение инцидентов и оценку опасностей, связанных с приостановкой и/или ухудшением качества услуги, например, следует идентифицировать единичные отказы. Организация должна исследовать возможности повышения жизнеспособности услуг информационных и коммуникационных технологий, чтобы снизить вероятность и/или последствия приостановки предоставления услуги. Это позволит обеспечить более раннее обнаружение и реагирование на приостановку предоставления услуги информационных и коммуникационных технологий. На основе полученных данных организация может принять обоснованное решение о необходимости инвестиций в выявленные возможности повышения жизнеспособности услуги. Подобная оценка опасностей для каждой услуги дает возможность экономического обоснования для улучшения способности к восстановлению услуг информационных и коммуникационных технологий.

4.3 Идентификация расхождения между способностью организации к обеспечению непрерывности критических видов информационных и коммуникационных технологий и требованиями непрерывности бизнеса

4.3.1 Для каждого критического вида услуг информационных и коммуникационных технологий необходимо сравнить способность обеспечения непрерывности информационных и коммуникационных технологий в организации с требованиями по обеспечению непрерывности бизнеса. Выявленные расхождения должны быть документированы.

4.3.2 Высшее руководство должно быть проинформировано обо всех расхождениях способности к обеспечению непрерывности критических видов услуг информационных и коммуникационных технологий и требований по обеспечению непрерывности бизнеса. Такие расхождения могут указывать на потенциальные опасности и потребность в формировании ресурсов жизнеспособности и восстановления услуги, таких как:

a) персонал, включая его численность, навыки и знания;

b) производственные площади, на которых размещено оборудование информационных и коммуникационных технологий, например, компьютерный зал;

c) вспомогательные технологии, здания, оборудование и информационно-коммуникационные сети;

d) информационное программное обеспечение и базы данных;

e) внешние услуги и поставщики (поставки).

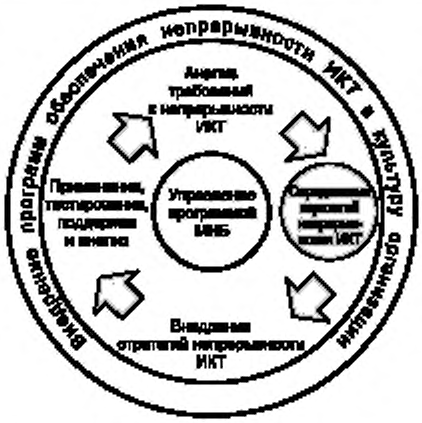
Подобные дополнительные ресурсы жизнеспособности и восстановления услуг могут потребовать дополнительного финансирования со стороны организации.

4.4 Утверждение

Высшее руководство должно утвердить наименования и определения услуг информационных и коммуникационных технологий, документально оформленный перечень критических видов услуг информационных и коммуникационных технологий и опасностей, связанных с выявленными

расхождениями способности к обеспечению непрерывности критических видов услуг информационных и коммуникационных технологий и требованиями по обеспечению непрерывности бизнеса, включая утверждение идентифицированных видов риска (см. 4.2.2). Должны быть разработаны способы устранения идентифицированных расхождений и снижения риска путем определения стратегий менеджмента непрерывности информационных и коммуникационных технологий.

5 Определение стратегий обеспечения непрерывности информационных и коммуникационных технологий



Цель:

Оценка и представление на утверждение высшим руководством общей стратегии менеджмента непрерывности информационных и коммуникационных технологий и стратегии менеджмента непрерывности информационных и коммуникационных технологий, включающей внедрение услуг информационных и коммуникационных технологий, обеспечивающих устранение расхождений между способностью к непрерывности бизнеса информационных и коммуникационных технологий и требованиями непрерывности бизнеса

5.1 Общие положения

В стратегии менеджмента непрерывности информационных и коммуникационных технологий необходимо определять подход к достижению необходимого уровня жизнеспособности услуг и внедрению процессов защиты и восстановления услуг организации.

Организация должна классифицировать все способы обеспечения менеджмента непрерывности информационных и коммуникационных технологий. Выбранные стратегии обеспечения непрерывности информационных и коммуникационных технологий должны поддерживать требования по обеспечению непрерывности бизнеса организации. При разработке стратегии организация должна учесть специфику ее внедрения и требования к постоянным ресурсам. Организация может привлечь внешних поставщиков для предоставления специализированных услуг и навыков, играющих важную роль в поддержке стратегии.

Стратегия менеджмента непрерывности информационных и коммуникационных технологий должна быть достаточно гибкой и учитывать различные бизнес-стратегии на различных рынках. Содержание стратегии должно учитывать внутренние ограничения и факторы, такие как:

- бюджет;
- доступность ресурсов;
- потенциальные затраты и доходы;
- технологические ограничения;
- склонность организации к рискам;
- существующую стратегию информационных и коммуникационных технологий организации.

5.2 Выбор стратегии обеспечения непрерывности информационных и коммуникационных технологий

Организация должна проанализировать способы обеспечения непрерывности предоставления услуг информационных и коммуникационных технологий. Эти способы обеспечения непрерывности должны предусматривать повышение уровня защищенности и жизнеспособности услуг, резервирование на случай восстановления при возникновении незапланированного сбоя, а также могут включать в себя подготовку к сбоям собственными силами организации и/или привлечение для этих работ услуг сторонних организаций.

Необходимо учитывать различные компоненты, необходимые для обеспечения непрерывности и восстановления услуг информационных и коммуникационных технологий. Непрерывность может быть достигнута разными способами, которые учитывают:

- навыки и знания;
- производственные площади;
- технологии;
- информацию;
- запасы.

5.3 Навыки и знания

Организация должна идентифицировать соответствующие стратегии поддержки основных навыков и знаний персонала в области информационных и коммуникационных технологий. Данные стратегии должны охватывать не только персонал организации, но и подрядчиков и другие причастные стороны, обладающие специальными навыками и знаниями в области информационных и коммуникационных технологий.

Стратегии по сохранению или обеспечению таких навыков могут включать в себя:

a) документирование способов функционирования критических видов услуг информационных и коммуникационных технологий;

b) обучение специальным навыкам в области информационных и коммуникационных технологий персонала и подрядчиков;

c) разделение ключевых навыков, направленное на снижение концентрации опасных событий (это может привести к территориальному разделению штата, обладающего ключевыми навыками, либо обучение ключевым навыкам не одного, а нескольких сотрудников);

d) сохранение и управление знаниями.

5.4 Производственные площади

Организация должна разработать стратегии снижения воздействия такого показателя, как отсутствие соответствующих производственных площадей (помещения) для обеспечения информационных и коммуникационных технологий. Стратегия может включать в себя одну или несколько мер:

a) наличие альтернативного помещения (места) в организации, включая вариант перемещения других видов деятельности;

b) наличие альтернативного помещения, предоставляемого при необходимости другими организациями;

c) наличие альтернативного помещения, предоставляемого при необходимости сторонними специалистами;

d) организация работы на дому или в других удаленных местах;

e) наличие иного, заранее согласованного, пригодного рабочего помещения;

f) использование альтернативной рабочей силы в установленном месте;

g) использование альтернативного мобильного рабочего помещения, которое может быть доставлено на участок, где произошел сбой, и использовано для обеспечения прямой замены некоторых из вовлеченных производственных активов.

При исследовании возможности использования альтернативного помещения необходимо учитывать следующее:

- безопасность места расположения;
- доступность для персонала;
- близкое расположение к производственным площадям (помещениям).

Примечание 1 — Существуют различные стратегии выбора производственных площадей (помещений) для информационных и коммуникационных технологий. Различные типы инцидентов или угроз могут требовать применения различных или многочисленных стратегий. Адекватность стратегии частично может зависеть от размера организации, сферы и масштаба деятельности, причастных сторон, географического месторасположения, применяемых технологий и других ключевых ограничений.

Примечание 2 — Организация должна исследовать способы обмена информацией, сетевые возможности и защитные меры, необходимые для выполнения специализированных функций информационных технологий.

5.5 Технология

Примечание — Предоставление технологических решений для удовлетворения требований непрерывности информационных и коммуникационных технологий зависит от особенностей используемых информационных и коммуникационных технологий, поддерживающих их критические виды деятельности, сроки и уровень обслуживания, необходимые для восстановления.

Организация должна установить стратегии непрерывности информационных и коммуникационных технологий, обеспечивающих доступность услуг информационных и коммуникационных технологий, которые поддерживают восстановление критических видов деятельности в рамках целевого времени восстановления, определенного в процессе анализа воздействия на бизнес.

Критические виды деятельности могут зависеть от предоставления актуализированных данных. Решения по обеспечению непрерывности предоставления данных должны быть разработаны в соответствии с целевыми сроками восстановления, установленными в организации.

Технологии, поддерживающие услуги информационных и коммуникационных технологий, требуют дополнительного применения комплексных мер по обеспечению непрерывности. Следовательно, при выборе стратегии информационных и коммуникационных технологий необходимо учитывать:

- целевое время и целевой срок восстановления услуг информационных и коммуникационных технологий, поддерживающих ключевые виды деятельности, идентифицированные в программе МНБ;
- местоположение и расстояние между технологическими объектами;
- количество технологических объектов;
- удаленный доступ к системам;
- требования к системе кондиционирования;
- требования к электроснабжению;
- использование необслуживаемых объектов;
- возможность подключения телекоммуникаций и дублирующей маршрутизации;
- характер «восстановления конфигурации» (необходимо ли ручное вмешательство для активации резервных информационных и коммуникационных технологий, или активация должна быть автоматической);
- необходимый уровень автоматизации;
- устаревание технологий;
- возможность подключения внешних поставщиков услуг и прочие внешние связи.

5.6 Информация

Выбранные способы обеспечения непрерывности должны обеспечивать непрерывную конфиденциальность, целостность, доступность и актуальность критической информации и данных, поддерживающих критические виды деятельности (см. ИСО/МЭК 27001 и ИСО/МЭК 27002).

Стратегии хранения и непрерывности информации и данных должны соответствовать требованиям непрерывности бизнеса организации и учитывать:

- требования к целевому сроку восстановления;
- способы организации надежного хранения данных, например дисков, кассет или оптических носителей информации; необходимо обеспечивать меры по резервному копированию и восстановлению данных, направленные на обеспечение защиты данных и их нахождение в безопасных условиях;
- места хранения информации, способы ее транспортировки или передачи, расстояние, местоположение, сетевые соединения и т.д. (хранение внутри помещений организации, вне помещений организации или у третьих лиц) и ожидаемые сроки извлечения резервных носителей;
- сроки восстановления, которые зависят от объема данных, способов их хранения, сложности процесса технического восстановления, требований пользователей услуг и требований организации к обеспечению непрерывности деятельности.

Примечание — Понимание «сквозного» использования данных во всей организации, включая информационные потоки и обмен информацией с третьими лицами, является критически важным для разработки стратегии менеджмента непрерывности информационных и коммуникационных технологий. Характер, актуальность и значимость данных могут отличаться в различных подразделениях организации.

5.7 Запасы

Организация должна идентифицировать и документировать уровень зависимости от услуг внешних поставщиков, поддерживающих предоставление услуг информационных и коммуникационных технологий, а также обеспечивать поставки критически важного оборудования и услуг в заранее установленные и согласованные сроки. Подобная зависимость может существовать для аппаратных средств, программного обеспечения, телекоммуникаций, прикладных приложений, сторонних услуг хостинга, коммунальных услуг и обеспечения соответствующей производственной среды с такими показателями как кондиционирование воздуха, мониторинг окружающей среды и обеспечение средствами пожаротушения.

Стратегии для данных услуг могут включать в себя:

- хранение дополнительного оборудования и копий программного обеспечения вне производственных площадей организации;
- заключение соглашений с поставщиками по поставке оборудования для замены в короткие сроки;
- ремонт и/или замена в минимально короткие сроки дефектных частей в случае сбоя в работе оборудования;
- дублирование поставки коммунальных услуг, таких как электроэнергия и телекоммуникации;
- обеспечение наличия аварийного генераторного оборудования;
- определение альтернативных/замещающих поставщиков.

Организация должна включать требования менеджмента непрерывности информационных и коммуникационных технологий и бизнеса в договора со своими партнерами и поставщиками услуг. Положения договоров должны включать ссылку на обязательства каждой из сторон, согласованные уровни предоставления услуг, ответные меры в случае серьезных инцидентов, распределение затрат, частоту проведения учений и корректирующие меры.

5.8 Утверждение

Способы обеспечения непрерывности информационных и коммуникационных технологий должны быть представлены высшему руководству вместе с рекомендациями по принятию решения, основанными на потенциальных затратах и приемлемости риска для организации.

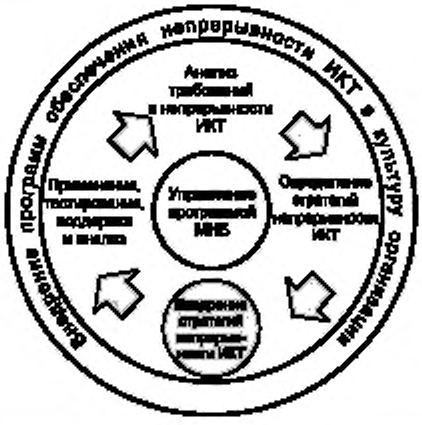
Необходимо довести до сведения высшего руководства реальную ситуацию по обеспечению непрерывности информационных и коммуникационных технологий, информацию о способности организации обеспечить выполнение требований непрерывности бизнеса в этой области, а также о существующих возможностях повысить степень выполнения этих требований.

Высшее руководство должно выбрать из представленных возможностей и утвердить стратегии обеспечения непрерывности информационных и коммуникационных технологий, что подтверждает соответствие выбранных стратегий обеспечения непрерывности общим требованиям непрерывности бизнеса организации.

При выборе стратегии менеджмента непрерывности информационных и коммуникационных технологий необходимо учитывать:

- вероятные опасности и последствия сбоев в работе;
- степень их интегрирования с общей стратегией непрерывности бизнеса организации;
- соответствие уровню приемлемого риска и общим целям организации.

6 Внедрение стратегий обеспечения непрерывности информационных и коммуникационных технологий



Цель:

Внедрение выбранной стратегии менеджмента непрерывности информационных и коммуникационных технологий организации, в том числе соответствующих структуры, планов и процедур, обеспечивающих внедрение

6.1 Внедрение стратегий менеджмента непрерывности информационных и коммуникационных технологий

Внедрение стратегии менеджмента непрерывности информационных и коммуникационных технологий необходимо начинать после утверждения этой стратегии высшим руководством организации.

Внедрение стратегии должно быть частью существующих проектов (жизненного цикла) организации, при этом необходимо использовать установленные средства управления проектами, процесс управления изменениями и управление программой МНБ, чтобы обеспечить полную прозрачность менеджмента и соответствующую отчетность.

6.2 Навыки и знания

Успешное внедрение может включать в себя:

- документирование процессов и процедур;
- документирование знаний, связанных с информационными и коммуникационными технологиями,
- перекрестное обучение в целях минимизации пробелов в навыках/знаниях;
- планирование преемственности;
- избегание концентрации квалифицированного персонала в одном месте.

6.3 Процессы

Процессы обеспечения непрерывности и восстановления должны быть документированы, четко сформулированы и иметь степень детализации, достаточную для их выполнения компетентным персоналом (эти процессы могут отличаться от бизнес-процессов).

Документированные процессы могут включать в себя процедуры, реализуемые в альтернативных условиях, а не на обычных рабочих местах. На практике такие процедуры должны быть адаптированы к конкретным обстоятельствам, сопутствующим сбоям в работе (например, уровень потерь или ущерба), приоритетам в работе организации и требованиям внешних причастных сторон.

6.4 Технология

Технологические стратегии информационных и коммуникационных технологий могут включать в себя:

- «горячее резервирование», при котором инфраструктура информационных и коммуникационных технологий размещается в двух разных местах;
- «теплое резервирование», при котором восстановление инфраструктуры производится на дополнительном месте размещения, где заранее частично подготовлена инфраструктура информационных и коммуникационных технологий;

- «холодное резервирование», при котором создание и конфигурация инфраструктуры осуществляется с нуля в альтернативном месте;
- соглашения о поставках аппаратных средств внешними поставщиками услуг;
- комбинация предыдущих стратегий: подход «выбор и перемешивание».

6.5 Данные

Меры по обеспечению доступности данных должны быть согласованы с требованиями, установленными в стратегии менеджмента непрерывности информационных и коммуникационных технологий, и могут включать в себя:

- дополнительное хранение данных в формате, обеспечивающем их доступность в сроки, установленные программой непрерывности бизнеса;
- альтернативные места хранения данных, которые могут быть физическими или виртуальными, при условии обеспечения безопасности и конфиденциальности данных; должны быть установлены соответствующие процедуры доступа и, если хранение такой информации организовано с привлечением третьих лиц, владельцы информации должны убедиться в наличии соответствующих средств управления.

6.6 Реагирование на инциденты информационных и коммуникационных технологий

Для всех инцидентов информационных и коммуникационных технологий должна быть установлена процедура реагирования для:

- подтверждения характера и масштаба инцидента;
- установления контроля над ситуацией;
- сдерживания эскалации инцидента;
- обмена информацией с причастными сторонами.

Принятые ответные меры на инцидент должны инициировать соответствующие действия в рамках процесса менеджмента непрерывности информационных и коммуникационных технологий. Ответные меры должны быть интегрированы в общий процесс управления в условиях инцидентов МНБ. Они могут осуществляться группой управления в условиях инцидента или отдельным сотрудником, ответственным за управление в условиях инцидента и непрерывностью бизнеса, в зависимости от размера организации.

В более крупных организациях может быть использован многоуровневый подход и созданы группы, специализирующиеся на выполнении различных функций. В рамках информационных и коммуникационных технологий такое разделение функций может быть основано на технических или обслуживающих задачах.

Примечание — В некоторых случаях потенциальное воздействие сбоя на услуги информационных и коммуникационных технологий может потребовать более обширных ответных мер на инцидент в соответствии с планом обеспечения непрерывности бизнеса организации, а также дополнительных действий, таких как обмен информацией со СМИ и управление социальным обеспечением.

Сотрудники, ответственные за управление в условиях инцидента, должны иметь планы активации, функционирования, координации и обмена информацией в рамках ответных мер на инцидент.

6.7 Планы

6.7.1 Общие положения

Организация должна установить планы управления в условиях инцидента, при реализации которых может произойти сбой в работе. Эти планы должны обеспечить непрерывность информационных и коммуникационных технологий и восстановление критичной деятельности.

Планы организации по управлению в условиях инцидента информационных и коммуникационных технологий, непрерывности бизнеса и техническому восстановлению могут быть активированы последовательно или параллельно.

Организация может разработать специальные планы по восстановлению услуг информационных и коммуникационных технологий и/или их возврату к нормальному ходу деятельности. При этом необходимо учитывать, что зачастую невозможно осуществить планы восстановления немедленно после инцидента.

Организация должна обеспечить использование планов обеспечения непрерывности информационных и коммуникационных технологий для обеспечения непрерывности бизнеса в течение более

продолжительного времени, устанавливая дополнительные сроки для разработки планов по восстановлению.

6.7.2 Содержание планов

Некоторые организации могут иметь один план, охватывающий всю деятельность по восстановлению услуг информационных и коммуникационных технологий для всех операций. В крупных организациях может существовать несколько планов, каждый из которых подробно описывает восстановление определенного элемента услуги информационных и коммуникационных технологий.

Все планы, такие как планы управления в условиях инцидента или планы обеспечения непрерывности информационных и коммуникационных технологий, должны быть точными и доступными для понимания сотрудниками, вовлеченными в их выполнение. Планы должны содержать следующие элементы:

a) Цели и область применения

Организация должна установить и согласовать с высшим руководством цели и область применения каждого конкретного плана. Они должны быть понятны сотрудникам, вовлеченным в их выполнение. Все связи с другими планами или документами организации, особенно с планами обеспечения непрерывности бизнеса, должны быть определены и сделаны соответствующие ссылки, способ получения и доступа к этим планам должен быть документирован. Каждый план должен точно установить существующие ограничения при его выполнении.

Каждый план управления в условиях инцидента и план обеспечения непрерывности информационных и коммуникационных технологий должен определять приоритетные цели с учетом:

- восстановления критических видов услуг информационных и коммуникационных технологий;
- сроков их восстановления;
- уровней восстановления каждого вида критических услуг информационных и коммуникационных технологий;
- ситуации активации каждого плана.

Планы могут также содержать процедуры и опросные листы, поддерживающие процесс анализа после инцидента.

b) Функции и обязанности

Организация должна документировать функции и обязанности уполномоченных лиц и групп (с точки зрения принятия решений и полномочий на расходование средств) во время и после инцидента.

c) Инициирование плана

Примечание — Невозможно вернуть потерянное время. Всегда лучше своевременно инициировать ответные меры на инцидент информационных и коммуникационных технологий и остановить его эскалацию, чем упустить возможность сдерживания инцидента на раннем этапе его развития.

Организации должны использовать протоколы эскалации и инициирования управления в условиях инцидента, установленные в детализированных планах управления в условиях инцидента системы обеспечения непрерывности бизнеса, чтобы создать основу для устранения потенциальных сбоев в работе, связанных с услугами информационных и коммуникационных технологий.

Метод инициирования плана обеспечения непрерывности информационных и коммуникационных технологий должен быть документирован. Данный процесс должен позволять инициировать соответствующие планы или их части в кратчайшие сроки либо перед событием, которое может привести к сбою в работе, либо немедленно после возникновения подобного события.

План должен включать точное описание:

- способов мобилизации группы менеджмента непрерывности информационных и коммуникационных технологий;
- мест сбора группы;
- мест проведения последующих собраний группы и детализированного определения всех альтернативных мест встречи (в крупных организациях данные места сбора могут называться «центры управления»);
- обстоятельств, при которых организация не инициирует ответные меры на сбой в области информационных и коммуникационных технологий (например, незначительные ошибки и небольшое по срокам отключение электричества, затрагивающие критические виды услуг информационных и коммуникационных технологий, которые можно регулировать в рамках оперативного управления организацией).

Организация должна документировать процесс завершения деятельности группы (или групп) менеджмента непрерывности информационных и коммуникационных технологий сразу после окончания инцидента и возврата к нормальному ходу деятельности.

d) Владелец и ответственный за ведение плана

Организация должна назначить основного владельца плана, а также идентифицировать и документировать перечень лиц, ответственных за регулярный пересмотр, корректировку и обновление плана.

Необходимо использовать систему управления версиями документов, при этом все изменения должны быть формально доведены до сведения всех заинтересованных сторон, а записи о распространении плана — зарегистрированы.

e) Контактная информация

Примечание — Контактная информация может включать в себя данные о способах связи с ответственными лицами в нерабочее время. Если планы содержат конфиденциальные данные частных лиц, то следует обеспечить необходимый уровень защиты этих данных.

Каждый план должен содержать основные контактные данные о ключевых причастных сторонах или ссылку на эти данные.

6.7.3 План обеспечения непрерывности информационных и коммуникационных технологий

Цель:

Обеспечение управляемости инцидентов информационных и коммуникационных технологий в организации.

План обеспечения непрерывности информационных и коммуникационных технологий должен:

1) быть гибким, выполнимым и реалистичным;

2) быть доступным для прочтения и понимания;

3) создавать основу управления серьезными проблемами организации, для которых могут быть применены меры по обеспечению непрерывности информационных и коммуникационных технологий (например, в случае серьезного сбоя в работе).

План обеспечения непрерывности информационных и коммуникационных технологий должен установить общую структуру, включающую планы восстановления деятельности, охватывающие:

- общую стратегию;
- критические виды услуг (для которых установлены целевое время восстановления и целевой срок восстановления);
- сроки восстановления;
- группы восстановления и распределение их обязанностей.

Планы восстановления должны быть документированы таким образом, чтобы компетентный персонал мог воспользоваться ими в случае инцидента. Планы восстановления должны включать в себя:

a) цели: краткое описание целей плана;

b) содержание, включающее (со ссылкой на результаты анализа воздействия на бизнес) следующие элементы:

- критичность услуг: описание соответствующих услуг и идентификацию их критичности для организации;
- технология: краткий обзор основных технологий, поддерживающих услуги, включая место ее размещения;
- организация: краткий обзор организационных структур (подразделения, ключевые сотрудники и процедуры), управляющих поддерживающими технологиями;
- документация: краткий обзор основной документации по поддерживающим технологиям, включая места (вне объекта или вне организации) хранения данной документации;

c) требования доступности: бизнес-требования к доступности услуг и поддерживающих технологий;

d) процедуры восстановления технологий: описание процедур, используемых для восстановления услуг информационных и коммуникационных технологий, включая следующее:

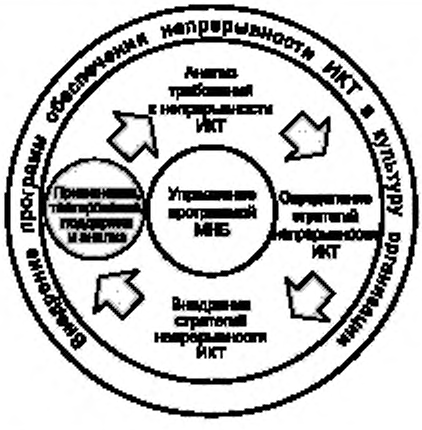
- перечень видов деятельности, например, техническая поддержка пользователей и восстановление контактной информации;
- перечень видов деятельности по восстановлению сети, систем, приложений, баз данных и т. д. до установленного уровня в альтернативном месте размещения с учетом изменений в производственной среде (например, может быть снижена пропускная способность каналов связи, нарушены коммуникации между различными системами и т. п.);

- перечень видов деятельности по восстановлению базовой функциональности, такой как безопасность, маршрутизация и ведение журналов;
- способы координации прикладных программ или связи между ними, синхронизации данных и возможного применения автоматизированных процедур для обработки накопившейся задолженности по информации;
- процессы, необходимые для восстановления услуг информационных и коммуникационных технологий и начала их функционирования в режиме восстановления;
- процедуры резервного копирования данных;
- способы и места получения персоналом дополнительной информации, инструкций и т. п., например, номеров телефонов «горячей линии»;
- шаги по возврату в нормальный режим работы.

e) Приложения:
- реестры информационных систем, приложений и баз данных;
- описание инфраструктуры сети и наименований услуг;
- реестры аппаратных средств и системного программного обеспечения;
- договоры и соглашения об уровне услуг.

f) Ключевые поставщики информационных и коммуникационных технологий:
- поставщики при обычном ходе деятельности;
- поставщики услуг при режиме восстановления.

7 Проведение учений и тестов



Цель:

Обеспечение соответствия стратегий и планов заданному уровню функционирования и повышение уровня осведомленности бизнеса путем наработки знаний, если необходимо

7.1 Проведение учений по отдельным элементам услуг информационных и коммуникационных технологий

Примечание — Планы обеспечения непрерывности информационных и коммуникационных технологий организации нельзя считать надежными до их опробования в процессе проведения учений. Программа учений может включать в себя проведение различных упражнений и тестов, которые, в совокупности, подтверждают жизнеспособность организации и ее способность к восстановлению услуг информационных и коммуникационных технологий, поддерживающих общую непрерывность деятельности организации.

Организация должна проводить учения не только по восстановлению услуг информационных и коммуникационных технологий, но также по элементам обеспечения жизнеспособности, чтобы определить:

a) способность защищать, поддерживать и/или восстанавливать услуги независимо от уровня серьезности инцидента;

b) способность применяемых методов менеджмента непрерывности информационных и коммуникационных технологий минимизировать воздействие инцидентов на бизнес;

c) выполнимость процедур возврата к нормальному ходу деятельности.

7.2 Учения

7.2.1 Программа учений

Примечание — В учения должен быть вовлечен весь персонала организации, а не только подразделение информационных и коммуникационных технологий. В учениях могут участвовать поставщики и иные третьи лица. Подразделение информационных и коммуникационных технологий играет в учениях важную роль, включая участие в планировании учений и их проведении, однако ведущую роль в учениях необходимо отводить всему персоналу организации.

Часто невозможно подтвердить способность организации к полному восстановлению информационных и коммуникационных технологий после проведения одного учения. Для моделирования реального инцидента целесообразно применять сокращенный режим проведения учений. Программа учений должна включать в себя различные уровни проведения учений, начиная с ознакомительного тестирования планов и заканчивая учениями по поддержанию жизнеспособности компьютерного зала, как показано на рисунке 2 (см. 7.2.2), и учитывать все аспекты непрерывного предоставления услуг информационных и коммуникационных технологий.

Необходимо понимать риск, связанный с проведением учений. Программа учений не должна приводить к неприемлемому уровню риска для организации. Она должна быть утверждена высшим руководством, документирована и включать подробное описание опасностей и риска, связанных с проведением учений.

Цели программы учений по обеспечению непрерывности информационных и коммуникационных технологий должны соответствовать области применения и целям менеджмента непрерывности бизнеса и быть интегрированными в общую программу учений по непрерывности бизнеса организации. Проведение каждого учения должно выполняться в соответствии с целями бизнеса (даже если прямое участие со стороны бизнеса отсутствует) и определенными целями тестирования или валидации отдельных элементов стратегии восстановления и жизнеспособности.

Проведение учений по отдельным элементам дополняет проверку систем в целом.

В программе учений по обеспечению непрерывности информационных и коммуникационных технологий необходимо определить регулярность, область и формат каждого учения. Ниже приведены примеры областей применения учений:

- восстановление данных: восстановление одного файла или базы данных после повреждения;
- восстановление одной услуги (включая полное восстановление услуги);
- восстановление прикладного приложения (оно может состоять из нескольких услуг, вспомогательных приложений и инфраструктуры);
- восстановление после отказа услуг, размещенных на платформе высокой доступности (например, кластеризация: моделирование потери одного сервера в кластере);
- восстановление данных из резервной копии (восстановление одиночных файлов или набора файлов из ленточного хранилища, находящегося за пределами организации/объекта);
- тестирование сети;
- тестирование восстановления после отказа коммуникационной инфраструктуры.

Учения должны быть проведены с использованием современных технологий и включать тесты взаимосвязанных систем и соответствующие группы конечных пользователей.

7.2.2 Область применения учений

Целью учений являются:

- создание уверенности в том, что способность организации к восстановлению и стратегия восстановления соответствуют требованиям бизнеса;
- демонстрация способности поддержки и восстановления услуг на согласованном уровне предоставления услуг и/или целей восстановления вне зависимости от типа инцидента;
- демонстрация способности услуги к восстановлению на заранее установленном уровне в случае инцидента в месте восстановления;
- обеспечение ознакомления персонала с процессом восстановления;
- идентификация возможностей для улучшений, которые необходимо внести в стратегию, архитектуру или процессы восстановления;
- обеспечение основы для ведения журналов аудита (следов) и компетентности персонала организации.

Учения должны быть применены к среде информационных и коммуникационных технологий и всем компонентам, обеспечивающим предоставление услуги от компьютерного центра до рабочего стола конечного пользователя или по любому другому каналу предоставления услуг.

7.2.3 Элементы восстановления услуг

Организация должна проводить учения по всем элементам восстановления услуг информационных и коммуникационных технологий, направленные на проверку их соответствия установленному размеру и сложности, а также области применения менеджмента непрерывности бизнеса.

Учения не должны фокусироваться исключительно на операциях восстановления и возобновления услуги, они должны включать в себя проверку надежности механизмов системного мониторинга, обеспечения способности к восстановлению, а также управлению в аварийной ситуации.

Организация должна проводить учения по отдельным компонентам вплоть до полного тестирования всей системы в месте ее расположения, что необходимо для достижения высокой надежности и отказоустойчивости системы (см. рисунок 2).

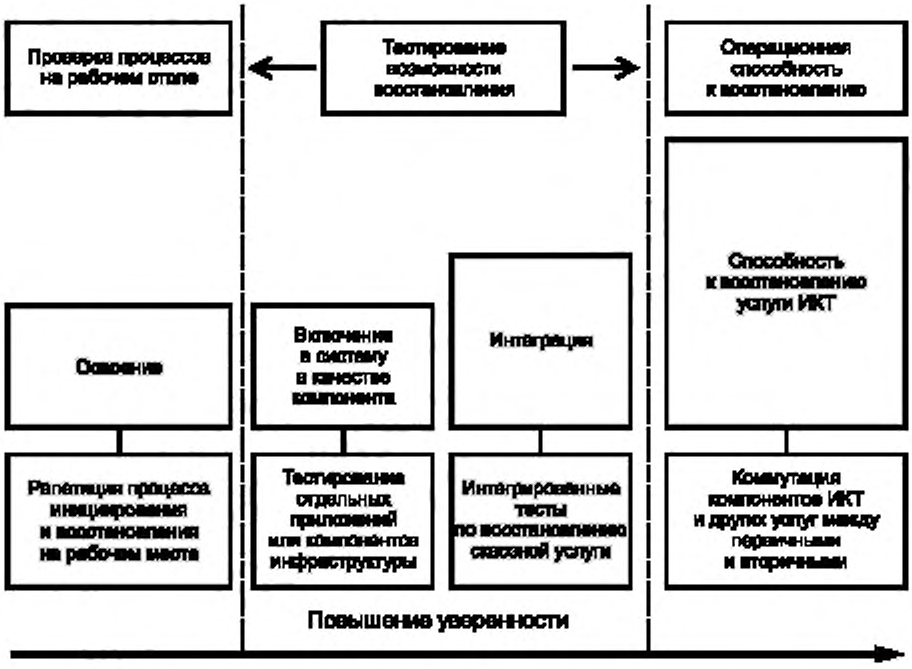


Рисунок 2 — Элементы восстановления услуг информационных и коммуникационных технологий

Необходимо тестирование следующих элементов:

- компьютерный зал, в том числе системы обеспечения физической безопасности, обнаружения возгорания, водоснабжения, электроснабжения, отопления, охранной сигнализации, вентиляции, кондиционирования воздуха и мониторинга окружающей среды;
- инфраструктура, включая общую способность к восстановлению сетевых соединений, диверсификацию и безопасность сети, включая антивирусную защиту, системы обнаружения и предотвращения вторжений (см. ИСО/МЭК 27001);
- аппаратные средства, включая серверы, телекоммуникационное оборудование, средства хранения и сменные носители;
- программное обеспечение;
- данные;
- услуги.

7.3 Планирование

Для обеспечения в период учений непрерывной доступности услуг и предотвращения инцидентов учебные мероприятия должны быть тщательно спланированы, что способствует минимизации риска возникновения инцидента в результате проведения учений и тестов.

Менеджмент риска должен соответствовать уровню проводимых учений и тестов (отдельный компонент или компьютерный зал) и может включать:

- обеспечение резервного копирования всех данных непосредственно перед учением;
- проведение упражнений и тестов в изолированной среде;
- планирование проведения учений во внерабочее время или в неактивное время бизнес-цикла с уведомлением конечных пользователей.

Учения должны быть близкими к реальным условиям, тщательно спланированными и согласованными с причастными сторонами, чтобы свести к минимуму риск нарушения бизнес-процессов. Учения не должны проводиться во время инцидентов.

Масштаб и сложность учений должны соответствовать целям восстановления деятельности организации.

Каждая проверка должна иметь согласованное и утвержденное инициатором учений «техническое задание», которое может включать следующие разделы:

- описание;
- цели;
- область применения;
- допущения и предположения;
- ограничения;
- опасности и связанный с ними риск;
- критерии достижения положительного результата;
- ресурсы;
- функции и обязанности;
- график проведения учений;
- сбор данных для учений;
- ведение журнала учений/инцидентов;
- подведение итогов;
- действия по результатам учений (последующий контроль и отчетность).

Планирование учений должно позволить организации достичь установленных критериев.

7.4 Управление учениями

Организация должна разработать четкую структуру управления учениями с распределением функций и ответственности между лицами, вовлеченными в проведение учений.

Структура управления учениями может включать в себя:

- приказ о проведении учений;
- обмен информацией об учениях;
- подтверждение наличия достаточного количества персонала для безопасного проведения учений;
- достаточное количество наблюдателей и/или участников для регистрации данных о ходе учений и возникающих проблемах;
- ключевые этапы учений;
- протокол, составляемый по окончании учений;
- протоколы об аварийной остановке учений.

Учения должны проводиться в рамках общей структуры управления учениями для обеспечения:

- достижения целей и ключевых этапов учений;
- назначения соответствующих уровней конфиденциальности по всем материалам и действиям в период учений;
- мониторинга и снижения текущего риска;
- регистрации всех посетителей и наблюдателей;
- последовательной регистрации хода учений;
- доведения результатов учений до всех участников и получения обратной связи.

7.5 Анализ, отчетность и последующий контроль

По окончании учений необходимо провести анализ полученных результатов и внедрить соответствующие корректирующие действия, включая:

- сбор данных о полученных результатах и выявленных проблемах;
- анализ полученных результатов на соответствие целям учений и критериям достижения положительного результата;
- идентификацию имеющихся пробелов;
- определение графика реализации корректирующих действий;
- создание отчета по результатам учений для рассмотрения инициаторами учений;
- объединение данных и последующий контроль над действиями, предпринимаемыми на основе отчета по результатам учений.

8 Поддержка, анализ и улучшение



Цель:

Обеспечение постоянной жизнеспособности стратегии менеджмента непрерывности информационных и коммуникационных технологий и способности к адаптации в динамичной рабочей среде

8.1 Управление изменениями

8.1.1 Работа с изменениями

Изменения обычно приводят к появлению дополнительных видов риска, не только риска отказа, но и риска дестабилизации существующих политик и стратегий. Организация должна обеспечить жизнеспособность и способность к адаптации стратегии менеджмента непрерывности информационных и коммуникационных технологий.

Внесение изменений в услуги информационных и коммуникационных технологий должно проводиться только после оценки и анализа технических и экономических последствий.

Для обеспечения постоянного соответствия стратегии и планов менеджмента непрерывности информационных и коммуникационных технологий политике и целям организации необходимо следующее:

a) высшее руководство должно обеспечить постоянное соответствие стратегии менеджмента непрерывности информационных и коммуникационных технологий требованиям МНБ организации;

b) в процессе управления изменениями (в том числе их разработка и внедрение) должны участвовать те же специалисты, которые были ответственными за разработку стратегии менеджмента непрерывности услуг информационных и коммуникационных технологий;

c) процесс разработки новых услуг информационных и коммуникационных технологий должен включать в себя требование к непрерывности работы существующих услуг;

d) комплексная проверка деятельности по объединению и/или поглощению в области информационных и коммуникационных услуг должна включать в себя оценку степени их направленности на устойчивое развитие организации;

e) вывод из эксплуатации компонента информационных и коммуникационных технологий должен проводиться в соответствии с процедурами менеджмента непрерывности информационных и коммуникационных технологий.

8.1.2 Управление записями по менеджменту непрерывности информационных и коммуникационных технологий

Должны быть созданы средства управления записями по менеджменту непрерывности информационных и коммуникационных технологий, направленные на обеспечение:

a) идентификации, читаемости записей и доступа к ним;

b) идентификации, хранения, защиты и извлечения записей.

8.1.3 Управление документами по менеджменту непрерывности информационных и коммуникационных технологий

Организация должна установить средства управления документацией по менеджменту непрерывности информационных и коммуникационных технологий для обеспечения следующих процедур:

a) одобрение и утверждение соответствия документов требованиям МНБ до их опубликования;

b) пересмотр, обновление и повторное утверждение документов по мере необходимости;

c) идентификация изменений и установление статуса текущей версии документов,

d) доступность в местах использования соответствующих версий применяемых документов;

e) идентификация внешних документов и управление их распространением;

f) принятие соответствующих мер по предупреждению непреднамеренного использования устаревших документов, их идентификация в случае их хранения для нужд организации.

8.2 Анализ менеджмента непрерывности информационных и коммуникационных технологий

8.2.1 Сроки и область анализа

Высшее руководство должно обеспечивать проведение регулярного анализа системы менеджмента непрерывности информационных и коммуникационных технологий. Этот анализ может проводиться в виде самооценки, внутренних или внешних аудитов.

Анализ должен включать в себя оценку возможностей для улучшения и необходимости внесения изменений в систему менеджмента непрерывности информационных и коммуникационных технологий, включая политику и цели менеджмента непрерывности информационных и коммуникационных технологий.

Результаты анализа должны быть документированы, необходимо вести записи в процессе анализа.

8.2.2 Входные данные для анализа со стороны руководства

Входные данные для анализа со стороны руководства должны содержать информацию о следующем:

a) уровнях предоставления внутренних услуг;

b) способности внешних поставщиков услуг обеспечивать соответствующий уровень предоставления услуг;

c) результатах предшествующих и аналогичных аудитов;

d) обратной связи с заинтересованными лицами, включая независимых наблюдателей;

e) статусе предупреждающих и корректирующих действий;

f) уровнях остаточного и приемлемого риска;

g) контроле выполнения мер и рекомендаций по результатам предыдущего анализа со стороны руководства;

h) опыте, полученном в ходе учений, инцидентов и при проведении программ обучения и повышения осведомленности;

i) передовом опыте и наилучшей практике других организаций.

8.2.3 Результаты анализа

Результаты анализа должны быть утверждены высшим руководством и включать в себя:

a) изменение области применения менеджмента непрерывности информационных и коммуникационных технологий;

b) повышение эффективности менеджмента непрерывности информационных и коммуникационных технологий;

c) изменение стратегии и процедур менеджмента непрерывности информационных и коммуникационных технологий (если применимо), необходимых для улучшения качества ответных мер на внутренние и/или внешние опасные события, которые могут повлиять на услуги информационных и коммуникационных технологий, включая внесение изменений в:

1) требования бизнеса;

2) требования к жизнеспособности;
3) уровни риска и/или уровни принятия риска;
d) необходимые ресурсы;
e) требования по финансированию и бюджетированию.

8.3 Улучшение менеджмента непрерывности информационных и коммуникационных технологий путем применения предупреждающих и корректирующих действий

8.3.1 Общие положения

Организация должна совершенствовать менеджмент непрерывности информационных и коммуникационных технологий путем применения предупреждающих и корректирующих действий, которые соответствуют потенциальным воздействиям, определяемым в ходе анализа воздействия на бизнес, и склонности организации к рискам.

Изменения, возникающие в результате таких предупреждающих и корректирующих действий, должны быть отражены в документации по менеджменту непрерывности информационных и коммуникационных технологий.

8.3.2 Предупреждающие действия

Организация должна выявить уязвимости в услугах информационных и коммуникационных технологий и установить документированную процедуру для:

a) идентификации потенциальных сбоев;
b) идентификации причин сбоев;
c) определения и внедрения необходимых предупреждающих действий;
d) анализа и регистрации результатов предпринятых мер;
e) информирования соответствующих лиц или подразделений о потенциальных сбоях и предпринятых предупреждающих действиях.

8.3.3 Корректирующие действия

Организация должна принять меры для устранения всех фактических сбоев в услугах информационных и коммуникационных технологий. В документированной процедуре по корректирующим действиям должны быть установлены требования к:

a) идентификации сбоев;
b) идентификации причин сбоев;
c) оценке необходимости принятия мер для предупреждения повторного сбоя;
d) определению и внедрению необходимых корректирующих действий;
e) регистрации результатов принятых мер;
f) анализу предпринятых корректирующих действий.

Приложение А
(справочное)

Основные этапы менеджмента непрерывности информационных и коммуникационных технологий

На рисунке А.1 приведены основные этапы менеджмента непрерывности информационных и коммуникационных технологий, которые расположены по оси времени. Этапы начинаются с нулевого времени, когда происходит сбой предоставления услуги информационных и коммуникационных технологий.

Целевой срок восстановления показывает объем потери данных, ожидаемый после сбоя, с учетом применения стратегии восстановления услуг информационных и коммуникационных технологий. Директивный срок восстановления представлен на оси времени как промежуток между временем последнего успешного резервного копирования и временем сбоя в работе.

Первым этапом после сбоя выполнения услуги информационных и коммуникационных технологий является обнаружение приостановления предоставления услуги (или ухудшения ее качества). Этот этап длится с момента времени обнаружения проблемы до времени получения уведомления. В некоторых случаях уведомление может быть получено в виде телефонного звонка пользователя в службу ИТ-поддержки.

Далее может пройти время, в течение которого проводится исследование, анализ сбоя предоставления услуги информационных и коммуникационных технологий, а также обмен информацией о сбое со всеми вовлеченными сторонами, и принимается решение об инициировании процессов обеспечения непрерывности информационных и коммуникационных технологий. Организации может потребоваться некоторое время с момента сбоя предоставления услуги информационных и коммуникационных технологий до принятия решения об инициировании процессов обеспечения непрерывности информационных и коммуникационных технологий с учетом времени, затрачиваемого на обмен информацией и принятие решений. В некоторых ситуациях решение об инициировании может потребовать более глубокого анализа, например, если предоставление услуги не было полностью остановлено, или существует большая вероятность самостоятельного восстановления услуги, поскольку инициирование процессов обеспечения непрерывности информационных и коммуникационных технологий часто влияет на обычный ход деятельности.

После инициирования начинается процесс восстановления услуг информационных и коммуникационных технологий. Он может быть разделен на восстановление инфраструктуры (сеть, аппаратные средства, операционная система, программное обеспечение резервного копирования и т.д.) и приложений (база данных, приложение, пакетные задания, интерфейсы и т.д.). Если услуги информационных и коммуникационных технологий восстановлены и персоналом информационных и коммуникационных технологий проведено тестирование систем, то услуга может быть предоставлена пользователям для тестирования с целью его использования в операциях по обеспечению непрерывности бизнеса.

В системе менеджмента непрерывности бизнеса для каждой продукции, услуги или вида деятельности должно быть установлено целевое время восстановления. Данное целевое время восстановления начинается с момента возникновения сбоя и продолжается до тех пор, пока продукция, услуга или вид деятельности не будут полностью восстановлены. Для этого необходимо применение набора услуг информационных и коммуникационных технологий, каждая из которых обычно включает в себя набор систем или приложений информационных и коммуникационных технологий. Каждый из этих компонентов систем или приложений информационных и коммуникационных технологий имеет свое целевое время восстановления, как подмножество целевого времени восстановления комплексной услуги информационных и коммуникационных технологий. Это целевое время восстановления должно быть меньше, чем целевое время восстановления непрерывности бизнеса, и учитывать время обнаружения и принятия решения, а также время, необходимое для проведения пользователем тестирования (если обеспечение непрерывности поставки продукции, предоставления услуги или выполнения вида деятельности невозможно без использования информационных и коммуникационных технологий, то в течение некоторого периода времени пользователь может использовать иные ИТ средства, например, ручные процедуры).

Восстановленные услуги информационных и коммуникационных технологий, как правило, работают в течение некоторого периода времени, поддерживая непрерывность бизнеса. Если это длительный период, то может потребоваться увеличение способности восстановленных услуг информационных и коммуникационных технологий к поддержанию увеличивающегося объема деятельности потенциально до того момента времени, когда продукция, услуга или деятельность будут полностью восстановлены до нормального хода деятельности.

Через некоторое время организация может принять решение перейти из режима непрерывности бизнеса к нормальному функционированию. Персонал информационных и коммуникационных технологий может спланировать данное изменение режима и использовать время естественного спада в операциях, однако необходимо учитывать, что это достаточно сложная задача. Возврат к нормальному режиму деятельности лучше назвать возвратом к новому нормальному режиму деятельности, так как сбой обычно приводит к значительным изменениям в бизнесе.

Стрелки в верхней части рисунка А.1 показывают, как принципы обеспечения непрерывности информационных и коммуникационных технологий, описанные в настоящем стандарте, согласуются с осью времени нарушения нормального хода деятельности.

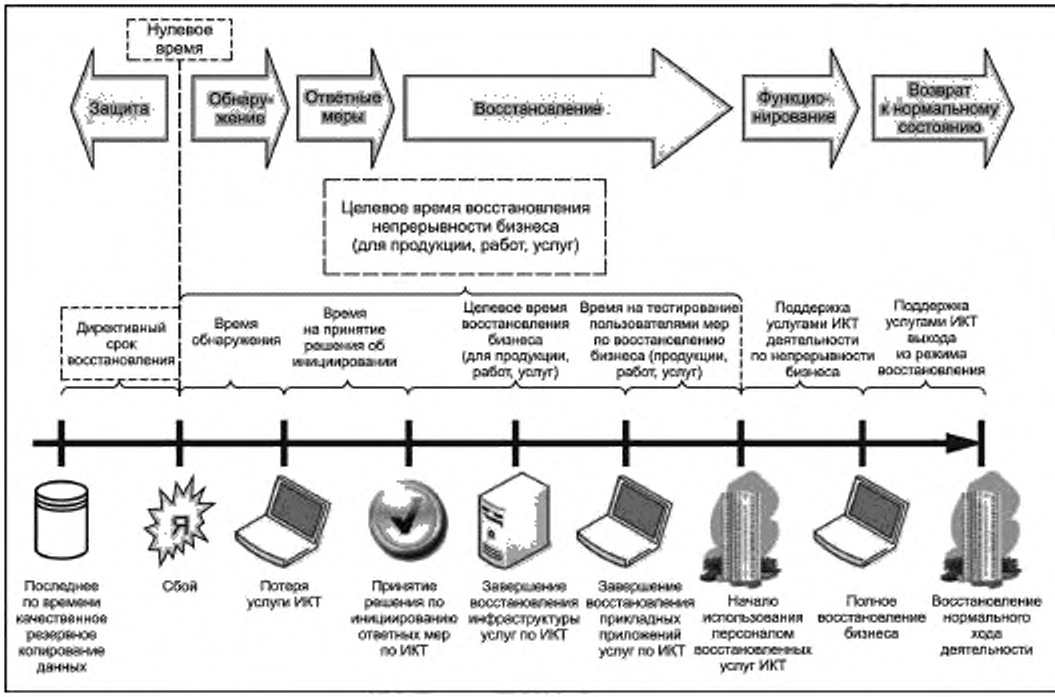


Рисунок А.1 — Основные этапы менеджмента непрерывности информационных и коммуникационных технологий

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документа, указанных в библиографии настоящего стандарта, национальным и межгосударственному стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта и документа	Степень соответствия	Обозначение и наименование соответствующего национального и межгосударственного стандарта
BS 25999-1*	IDT	ГОСТ Р 53647.1—2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство»
BS 25999-2*	IDT	ГОСТ Р 53647.2—2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования»
ISO 9000:2005**	IDT	ГОСТ ISO 9000—2011 «Системы менеджмента качества. Основные положения и словарь»
ISO/IEC 20000-1	IDT	ГОСТ Р ИСО/МЭК 20000-1—2013 «Информационная технология. Управление услугами. Часть 1. Требования к системе управления услугами»
ISO/IEC 20000-2	IDT	ГОСТ Р ИСО/МЭК 20000-2—2010 «Информационная технология. Менеджмент услуг. Часть 2. Кодекс практической деятельности»
ISO/IEC 27001	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ISO/IEC 27002	IDT	ГОСТ Р ИСО/МЭК 27002—2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичные стандарты.		

* Заменены на BS ISO 22301:2012.

** Заменен на ISO 9000:2015.

Библиография

[1] BS 25999, Business continuity management

[2] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary

[3] ISO/IEC 20000-1, Information technology — Service management — Part 1: Specification

[4] ISO/IEC 20000-2, Information technology — Service management — Part 2: Code of practice

[5] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[6] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security management

УДК 658:562.014:006.354 ОКС 03.100.01

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

Редактор переиздания *Е.В. Яковлева*
Технический редактор *И.Е. Черепкова*
Корректор *М.В. Бучная*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 26.06.2020. Подписано в печать 26.08.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,35.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru