ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 53131 — 2008 (ИСО/МЭК ТО 24762:2008)

Защита информации

РЕКОМЕНДАЦИИ ПО УСЛУГАМ ВОССТАНОВЛЕНИЯ ПОСЛЕ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ФУНКЦИЙ И МЕХАНИЗМОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Общие положения

ISO/IEC TR 24762:2008
Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services
(MOD)

Издание официальное

Москва
Стандартинформ
2011

gost.e-ecolog.ru

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») и Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России») на основе аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации № 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 533-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК ТО 24762—2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по услугам по восстановлению информационно-коммуникационных технологий после бедствий» (ISO/IEC TR 24762:2008 «Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services») путем введения дополнительных положений и изменения его структуры, обоснование которых приведено во введении к настоящему стандарту

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

6 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемом информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2011

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины, определения и сокращения . . . 2
4 Восстановление и обеспечение информационной безопасности информационных и телекоммуникационных систем организации при чрезвычайной ситуации и обеспечение непрерывности деятельности организации . . . 6
4.1 Общая информация . . . 6
4.2 Аспекты обеспечения условий непрерывности в информационной сфере организации . . . 7
4.3 Роль совета директоров и исполнительных органов организации . . . 8
4.4 Идентификация недостатков . . . 9
4.5 Непрерывность сервисов в изменяющейся среде и обеспечение информационной безопасности информационных и телекоммуникационных систем . . . 9
5 Понимание рисков непрерывности и их влияния на цели деятельности организации и восстановление защитных мер обеспечения информационной безопасности информационных и телекоммуникационных систем . . . 9
6 Восстановление после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий . . . 11
6.1 Организационная основа . . . 11
6.2 Вопросы системы менеджмента информационной безопасности организации и менеджмента непрерывности бизнеса . . . 12
6.3 Восстановление и обеспечение функционирования процессов системы менеджмента информационной безопасности организации и защитных мер информационной безопасности при чрезвычайных ситуациях . . . 13
Приложение А (обязательное) Восстановление информационно-коммуникационных технологий после чрезвычайной ситуации . . . 16
Приложение В (обязательное) Средства восстановления информационно-коммуникационных технологий после чрезвычайной ситуации . . . 23
Приложение С (обязательное) Выбор площадок для восстановления . . . 42
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте . . . 43
Приложение ДБ (справочное) Терминологические статьи международного стандарта ИСО/МЭК ТО 24762, которые применены в настоящем стандарте с модификацией их содержания . . . 44
Приложение ДВ (справочное) Сопоставление структуры настоящего стандарта со структурой международного стандарта ИСО/МЭК ТО 24762 . . . 45
Библиография . . . 47

Введение

Основное конкурентное преимущество любого современного бизнеса лежит в его информационной сфере. Конкурентное преимущество имеет тот, кто быстрее, точнее и на более длительный срок прогнозирует развитие тех или иных направлений деятельности или возможных проблем и рисков, потребностей бизнеса; кто быстрее и адекватнее реагирует на значимые для деятельности организации события и способен извлекать пользу (преимущества) даже из неблагоприятных ситуаций.

Для реализации вышеупомянутых условий обеспечения конкурентного преимущества требуется высокоорганизованная, высокотехнологичная и автоматизированная информационная сфера, в которой должны поддерживаться эффективные процессы. Такая информационная сфера, основанная только на глобальных данных (ранее — преимущественно на локальных), будет более уязвимой. Однако с точки зрения бизнеса основной причиной уязвимости информационной сферы является неопределенность состояния ее информационной базы, создающая иногда значительную стохастическую составляющую (риски) бизнеса. Понесенные потери могут иметь естественные причины, не связанные с нарушениями безопасности.

Подразделение организации, обеспечивающее ее безопасность, не может и не должно отвечать за все. Такой «привилегией» обладает только высшее руководство организации, и все ошибки — организационные, управленческие, ошибки в результате неадекватной и неэффективной деятельности — являются ошибками системы корпоративного управления организаций. Все остальные подразделения организации разделяют общую ответственность в объеме определенной им конкретной деятельности, в том числе и в части обеспечения безопасности. Область ответственности подразделения безопасности организации — злонамеренная активность, негативно влияющая на цели бизнеса, а самая сложная ее задача — противодействие злонамеренному использованию стохастичности бизнеса, то есть противодействие скрытому, невидимому злоумышленнику.

Одна из важнейших задач подразделения безопасности — формализация собственной деятельности в рамках организации (корпорации), т. е. определение совместно с высшим руководством организации роли и ответственности подразделения безопасности в организации. Роль подразделения безопасности должна определяться совокупностью процессов, которые это подразделение будет поддерживать, и механизмов включения этих процессов в общее корпоративное управление, поддержки этих процессов правами (каналами влияния на объект и степенью влияния), ресурсами и ответственностью.

В связи с усилением зависимости деятельности организации от непрерывности ее информационных процессов, доступности и готовности компонентов информационной сферы в разряд критических переходят аспекты, связанные с обеспечением непрерывности бизнеса. Руководство организаций все чаще ощущает зависимость их деятельности от сбоев, в том числе связанных с рисковыми событиями в информационной сфере.

В настоящем стандарте представлены рекомендации по планированию деятельности, связанной с восстановлением функций и механизмов безопасности информационных и телекоммуникационных технологий после чрезвычайных ситуаций в контексте общего процесса обеспечения непрерывности деятельности организации.

Основаниями разработки национального стандарта, модифицированного по отношению к международному стандарту, являются:

- различия в объектах стандартизации национального и международного стандартов, обусловленные потребностями в обеспечении информационной безопасности субъектов российской экономики и поддержке деятельности специализированных подразделений организаций;

- международный стандарт не учитывает государственные интересы и направлен на удовлетворение потребностей бизнеса (организаций, провайдеров услуг, групп организаций, связанных взаимными соглашениями, которые используют услуги аутсорсинга электронной обработки данных) в части восстановления информационных и коммуникационных технологий (ИКТ) после чрезвычайных ситуаций.

Объект стандартизации международного стандарта — услуги по восстановлению ИКТ после чрезвычайных ситуаций, в то время как объектом стандартизации гармонизированного модифицированного национального стандарта являются услуги по восстановлению после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий, а предметом стандартизации — общие положения.

Изменения, введенные в настоящий стандарт по отношению к международному стандарту, обусловлены необходимостью наиболее полного достижения целей национальной стандартизации в области защиты информации.

Структура настоящего стандарта по отношению к международному стандарту ИСО/МЭК ТО 24762 изменена в целях обеспечения ее соответствия правилам, установленным в разделе 3 ГОСТ Р 1.5 в части объекта и аспекта стандартизации.

Разделы 5, 6 и 8 международного стандарта ИСО/МЭК ТО 24762, как содержащие вспомогательную информацию относительно объекта и аспекта стандартизации настоящего стандарта, приведены в приложениях А, В и С настоящего стандарта с учетом сохранения перекрестных ссылок, имеющихся в указанных разделах. Отдельные слова в тексте данных приложений стандарта, измененные в целях учета аспекта стандартизации настоящего стандарта и для сохранения перекрестных ссылок, выделены курсивом.

Раздел 7 и приложение А международного стандарта ИСО/МЭК ТО 24762 исключены, как не имеющие непосредственного отношения к объекту и аспекту стандартизации настоящего стандарта.

Настоящий стандарт дополнен разделами 4, 5 и подразделом 6.1, содержащими положения, устанавливающие требования к объекту и аспекту стандартизации настоящего стандарта.

Положения подразделов 6.2 и 6.3 настоящего стандарта, устанавливающие требования к системе менеджмента информационной безопасности организации, замещают положения раздела 9 международного стандарта ИСО/МЭК ТО 24762, не отвечающие объекту и аспекту стандартизации настоящего стандарта.

Положения введенных разделов и подразделов выделены путем заключения их в рамки из тонких линий.

Для выделения разделов 1 и 2, модифицированных по отношению к тексту ИСО/МЭК ТО 24762, использована одиночная вертикальная полужирная линия, которая расположена на полях соответственно слева (четные страницы) и справа (нечетные страницы) от текста.

Сопоставление структуры настоящего стандарта со структурой примененной в нем части международного стандарта ИСО/МЭК ТО 24762 приведено в таблице ДВ.1 (приложение ДВ).

В настоящем стандарте некоторые терминологические статьи приведены в иной редакции, чем в ИСО/МЭК ТО 24762. Для выделения этих статей использована одиночная вертикальная полужирная линия, которая расположена на полях соответственно слева (четные страницы) и справа (нечетные страницы) от текста, модифицированного по отношению к соответствующему тексту ИСО/МЭК ТО 24762. Исходные по отношению к указанным терминологические статьи ИСО/МЭК ТО 24762 приведены в приложении ДБ настоящего стандарта.

В настоящий стандарт включен ряд дополнительных статей с терминами. Эти статьи заключены в рамки из тонких линий.

В целях идентификации терминологических статей настоящего стандарта, гармонизированных со статьями ИСО/МЭК ТО 24762, для этих статей в скобках (справа) приведены номер соответствующей статьи ИСО/МЭК ТО 24762 и условное обозначение степени их соответствия.

- IDT — идентичные статьи,
- MOD — модифицированные статьи.

Установленные настоящим стандартом термины расположены в систематизированном порядке, отражающем систему понятий в области стандартизации.

Для каждого понятия установлен один стандартизованный термин.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина. При этом не входящая в круглые скобки часть термина образует его краткую форму.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два или более термина, имеющие общие элементы.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, — светлым.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защита информации

РЕКОМЕНДАЦИИ ПО УСЛУГАМ ВОССТАНОВЛЕНИЯ ПОСЛЕ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ФУНКЦИЙ И МЕХАНИЗМОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Общие положения

Information protection. Guidelines for disaster recovery services of information and communications technology security functions and mechanisms. General

Дата введения — 2009 — 10 — 01

1 Область применения

Настоящий стандарт устанавливает общие требования в части поддержания (и восстановления) функционирования защитных мер (функций и механизмов) обеспечения информационной безопасности (ИБ) информационно-телекоммуникационных систем (ИТС) организации в условиях чрезвычайной ситуации в контексте роли и места защитных мер ИБ ИТС в обеспечении непрерывности деятельности организации.

Настоящий стандарт распространяется на процессы (услуги) по обеспечению (и восстановлению) информационной безопасности организации в условиях возникшей чрезвычайной ситуации.

Настоящий стандарт предназначен для персонала (служб безопасности) организации, а также для внутренних и внешних провайдеров (поставщиков) услуг, участвующих в обеспечении информационной безопасности организации.

Положения настоящего стандарта необходимо использовать в контексте общих требований к системам менеджмента информационной безопасности организаций, установленных в ГОСТ Р ИСО/МЭК 27001.

Положения настоящего стандарта следует использовать в соответствии с требованиями нормативных правовых актов Российской Федерации о безопасности, о защите населения и регионов от чрезвычайных ситуаций природного и техногенного характера и требованиями единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, а также с требованиями нормативных правовых актов Российской Федерации, устанавливающих нормы по защите информации и информационной безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью

ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Издание официальное

ГОСТ Р ИСО/МЭК ТО 18044—2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться заменяющим (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1.1 **вычислительное и взаимосвязанное оборудование** (computing and related equipment): Компьютерное, сетевое, телекоммуникационное и периферийное оборудование, которое поддерживает мероприятия организации по обработке информации. (3.1, IDT)

3.1.2 **системы ИКТ** (ICT systems): Аппаратные, программные и программно-аппаратные средства компьютеров, телекоммуникационное и сетевое оборудование или другие электронные системы обработки информации и взаимосвязанное оборудование. (3.2, IDT)

Примечание — Системы ИКТ включают любое оборудование или взаимосвязанные системы, или подсистемы оборудования, которые используют при приобретении, хранении, манипулировании, управлении, перемещении, контроле, отображении, коммутации, обмене, передаче или приеме данных/информации.

3.1.3 **информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки. (3.3, MOD)

[ГОСТ Р ИСО/МЭК 13335-1—2006, пункт 2.14], [1]

3.1.4

информационная безопасность организации (information security of organization): Состояние защищенности интересов (целей) организации в условиях угроз в информационной сфере.

Примечания

1 Защищенность достигается обеспечением совокупности свойств информационной безопасности — конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры. Приоритетность свойств информационной безопасности может быть определена значимостью информационных активов для интересов (целей) организации.

2 Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

3.1.5 **инфраструктура** (infrastructure): Мощности и оборудование, делающие возможными услуги восстановления ИКТ после *чрезвычайной ситуации*, включающие энергоснабжение, телекоммуникационные соединения и средства контроля влияния внешней среды (перечень может быть расширен). (3.4, IDT)

3.1.6 **организация** (organization): Юридическое лицо, которое имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде, а также имеющее самостоятельный баланс или смету и зарегистрированное в установленном порядке. (3.5, MOD)

[ГОСТ Р 1.4—2004, пункт 3.3], [2]

3.1.7

чрезвычайная ситуация; ЧС: Обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей.

Примечание — Чрезвычайные ситуации различают по характеру источника (природные, техногенные, биолого-социальные, военные) и по масштабам (локальные, местные, территориальные, региональные, федеральные, трансграничные).

[ГОСТ Р 22.0.02—94, статья 2.1.1], [3]

3.1.8

чрезвычайная ситуация (в организации): Внезапное, незапланированное катастрофическое событие, которое не позволяет организации выполнять критичные бизнес-процессы в требуемом для бизнеса объеме.

3.1.9

непредвиденная ситуация: Рисковое событие, связанное с неблагоприятными внешними событиями природного и техногенного характера, а также с действиями субъектов (групп субъектов), приводящими к невозможности функционирования организации или ее служб/подразделений в обычном, регламентируемом соответствующими стандартами режиме.

3.1.10

событие информационной безопасности: Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

[ГОСТ Р ИСО/МЭК 27001—2006, пункт 3.5]

3.1.11

инцидент информационной безопасности: Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание — Инцидентами информационной безопасности являются:
- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

[ГОСТ Р ИСО/МЭК 27001—2006, пункт 3.6]

3.1.12

система менеджмента информационной безопасности; СМИБ: Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Примечание — Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределению ответственности, практическую деятельность, процедуры, процессы и ресурсы.

[ГОСТ Р ИСО/МЭК 27001—2006, пункт 3.7]

3.1.13

защитная мера: Сложившаяся практика, процедура или механизм обработки риска.

Примечание — Следует заметить, что понятие «защитная мера» может служить синонимом понятия «контроль».

[ГОСТ Р ИСО/МЭК 13335-1—2006, пункт 2.24], [1]

3.1.14

восстановление (защитных мер обеспечения ИБ ИТС): Процесс перевода защитных мер обеспечения ИБ ИТС в штатное состояние после восстановления деятельности организации при условии наличия (новой) карты рисков ИБ деятельности организации.

Примечание — Восстановление включает идентификацию карты рисков ИБ деятельности организации, настройку или замену защитных мер ИБ, регулирование и контроль состояния защитных мер ИБ, контроль работоспособности объекта и его рисков ИБ, имеющего указанные защитные меры ИБ.

3.1.15

риск: Влияние неопределенности на цели организации.

Примечания

1 Влияние неопределенности подразумевает отклонение от ожидаемого результата.

2 Цели организации могут иметь различные аспекты (финансовые аспекты, аспекты, связанные с охраной здоровья, безопасностью и внешней средой) и могут применяться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта или процесса.

3 Риск часто характеризуют ссылкой на потенциальные события, их последствия или их комбинацию, а также на то, как они могут влиять на достижение целей организации.

4 Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и связанной с ними вероятностью их возникновения.

3.1.16

владелец риска: Физическое лицо или сущность (логический объект), обладающие обязанностями и полномочиями для осуществления менеджмента риска и любой связанной с ним деятельности и обработки риска.

3.1.17

менеджмент риска: Скоординированные действия по руководству и управлению, осуществляемые организацией в отношении риска.

3.1.18

ИТ-сервис (ИТ-услуга): Совокупность функциональных возможностей информационных и, возможно, неинформационных технологий, предоставляемая конечным пользователям в качестве услуги (сервиса) [4].

Примечание — Примерами ИТ-сервисов (ИТ-услуг) могут служить передача сообщений, бизнес-приложения, сервисы файлов и услуги печати, сетевые сервисы (услуги) и т. д.

3.1.19

критичный компонент (информационно-телекоммуникационной системы): Компонент информационно-телекоммуникационной системы, нарушение непрерывности функционирования которого может нанести значительный ущерб организации.

3.1.20

организационная мера (по обеспечению ИБ): Совокупность действий, определяемых нормативно-правовой документацией организации, по обеспечению ИБ без применения технических средств защиты.

3.1.21

технические средства защиты ИБ: Оборудование, используемое для защиты ИБ организации.

Примечание — Такое оборудование может быть представлено техническими и программно-техническими средствами.

3.1.22

лицо, ответственное за информационную безопасность: Лицо, отвечающее за внедрение и поддержку программы обеспечения информационной безопасности.

[ГОСТ Р ИСО/МЭК ТО 13569—2007, пункт 3.37], [5]

3.1.23

доступность информации [ресурсов информационной системы]: Состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут беспрепятственно их реализовывать.

Примечание — К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также право на изменение, использование, уничтожение ресурсов.

[Р 50.1.056—2005, статья 3.1.8], [6]

3.1.24

целостность (информации [ресурсов автоматизированной информационной системы]): Состояние информации [ресурсов автоматизированной информационной системы], при котором ее [их] изменение осуществляется преднамеренно только субъектами, имеющими на него право.

[Р 50.1.053—2005, статья 3.1.8], [7]

3.1.25 **привлеченные провайдеры услуг** (outsourced service providers): Внешние провайдеры услуг по восстановлению ИКТ после *чрезвычайной ситуации*. (3.6, IDT)

3.1.26 **провайдеры услуг** (service providers): Внутренние группы или внешние стороны, предоставляющие организациям услуги по восстановлению ИКТ после *чрезвычайной ситуации*. (3.7, IDT)

3.1.27 **соглашение об уровне сервиса** (service level agreement): Письменное соглашение между провайдером услуг и организацией, документирующее услуги и согласованные уровни обслуживания. (3.8, IDT)

Примечание — В случае привлеченных провайдеров услуг соглашение об уровне сервиса является письменным соглашением, имеющим обязательную договорную силу.

3.1.28 **обязательство по уровню обслуживания** (service level commitment): Обязательство провайдера услуг (обычно внутреннего провайдера услуг) перед организацией, которое определяет услуги и согласованные уровни обслуживания. (3.9, IDT)

3.2 В настоящем стандарте применены следующие сокращения:

ИБ — информационная безопасность;

ИКТ — информационно-коммуникационные технологии;

ИТ — информационные технологии;

ИТС — информационно-телекоммуникационные системы;

СМИБ — система менеджмента информационной безопасности;

ЧС — чрезвычайная ситуация.

4 Восстановление и обеспечение информационной безопасности информационных и телекоммуникационных систем организации при чрезвычайной ситуации и обеспечение непрерывности деятельности организации

4.1 Общая информация

4.1.1 Одним из основных условий, определяющих надежность и устойчивость деятельности организации, является обеспечение ею непрерывности своего бизнеса, т. е. способности выполнять процессы своей деятельности и поддерживать их непрерывное и согласованное взаимодействие в условиях проявления (в отношении организации) различных деструктивных воздействий, определяемых нестабильностью и (или) недружественностью внешней и внутренней среды организации.

Таким образом, непрерывность бизнеса организации предусматривает обеспечение двух взаимосвязанных слагаемых — непрерывности бизнес-процессов и качественного (адекватного и непрерывного) управления ими.

4.1.2 Основными причинами (источниками риска) возможного нарушения непрерывности бизнес-деятельности организации могут быть:

- неприемлемое для бизнеса состояние технологической среды и информационно-технологического обеспечения организации, включающего ИТС, связанное с нарушением функционирования или некачественным функционированием их компонентов из-за отсутствия и (или) недоступности качественных (и в необходимом объеме) ресурсов и услуг, требуемых для выполнения бизнес-процессов и процессов управления;

- действия (случайные или преднамеренные) субъектов (организованных групп субъектов) — собственных работников организации или сторонних лиц, противоречащие интересам организации и способные нарушить реализацию процессов основной, вспомогательной и управленческой деятельности;

- недостаточное качество самих бизнес-процессов и несовершенство общекорпоративного менеджмента, выражаемое, например, в неудовлетворительной организации деятельности, несовершенстве организационной структуры, ошибках управления;

- внешние обстоятельства — события, явления и процессы во внешней среде организации, неблагоприятным образом влияющие на ее деятельность.

4.1.3 Информационная составляющая деятельности организации и процессов ее управления, представляемая совокупностью информации и информационных процессов (технологий), которые обеспечивают каждый процесс деятельности организации и (или) являются его частью, в значительной степени подвержена воздействию различных деструктивных факторов внешней и внутренней среды организации.

Это означает, что значительная часть рисков организации, включая риск прерывания ее деловой деятельности, связана с информацией, а уровень и условия проявления этих рисков во многом определены качеством информации и информационных услуг (сервисов ИТ по подготовке, обработке, передаче, хранению и отображению информации), которые могут быть предоставлены бизнесу информационно-технологическим комплексом организации и (или) сторонними организациями (провайдерами услуг).

4.1.4 К свойствам ИБ организации, нарушение которых способно привести к неприемлемому для бизнеса снижению качества и безопасности услуг ИТС и, как следствие, к прерыванию деятельности организации, следует отнести:

- для информации — полезность (адекватность), конфиденциальность, доступность, целостность (достоверность и полноту), объективность, актуальность, согласованность,

- для технических и программных средств — функциональность, доступность и целостность;

- для ИТС и информационных процессов — функциональность, доступность, целостность и подотчетность.

Перечень приведенных свойств может быть расширен и уточнен в зависимости от конкретных потребностей бизнеса организации.

4.1.5 Для поддержания своей деятельности в ЧС организация должна:

- решить в первую очередь производственные проблемы, возникшие в результате ЧС;
- срочно задействовать утвержденные процедуры необходимых изменений в эксплуатационной среде, включая информационную сферу организации;
- инструктировать персонал, задействованный в локализации (ликвидации) ЧС, и документировать все реализованные изменения;
- пересмотреть все реально выполненные изменения при ЧС с точки зрения целей деятельности организации, включая переоценку рисков деятельности и рисков ИБ.

4.2 Аспекты обеспечения условий непрерывности в информационной сфере организации

4.2.1 Обеспечение непрерывности в информационной сфере организаций представляет собой совокупность политик, процессов деятельности и инструментальных средств, с помощью которых организации повышают не только свою потенциальную возможность реагирования на крупномасштабные отказы функционирующих систем, но также и устойчивость к крупным инцидентам ИБ в целях избежания отказа критических систем и сервисов.

4.2.2 Данная деятельность связана с решением ряда задач в рамках корпоративного управления и должна быть реализована в полном соответствии с принятыми в организации политиками, стандартами, процессами деятельности для обеспечения:

- требований системы менеджмента непрерывности бизнеса организации;
- поддержки менеджмента серьезных инцидентов ИБ и антикризисного менеджмента;
- корпоративного управления и менеджмента риска;
- менеджмента информационных технологий в организации;
- менеджмента информационной безопасности организации.

4.2.3 Менеджмент непрерывности в информационной сфере организации должен установить требования к стратегии применения ИТ в организации в целях идентификации информационных систем и сервисов, нуждающихся в обеспечении устойчивости, доступности и возможностях высокого уровня.

4.2.4 Менеджмент непрерывности в информационной сфере организации должен учитывать риски, способные оказать возможное или ожидаемое серьезное воздействие (иметь негативное последствие), которое может создать угрозу непрерывности бизнеса.

К таким рискам относят:

- потерю, ущерб или отказ в предоставлении доступа к ключевым сервисам инфраструктуры;
- потерю или искажение информации;
- саботаж, вымогательство или коммерческий шпионаж;
- преднамеренное проникновение или атаку на критические информационные системы.

4.2.5 Непрерывность бизнеса организации может быть достигнута управлением рисками организации в целях оценки и обеспечения уверенности в том, что в любое время организация сможет продолжать работу по крайней мере на заранее определенном минимальном уровне. Процесс менеджмента непрерывности бизнеса включает снижение риска до приемлемого уровня и планирование восстановления бизнес-процессов в случае реализации факторов риска и нарушения штатной деятельности организации.

Менеджмент непрерывности в информационной сфере организации должен быть частью общего плана обеспечения непрерывности деятельности организации, а не отдельным самодостаточным процессом.

Деятельность, включая услуги по восстановлению после ЧС защитных мер (функций и механизмов) безопасности информационных и телекоммуникационных технологий, следует планировать в рамках менеджмента непрерывности в информационной сфере организации с учетом влияния факторов рисков информационной природы на деятельность организации в процессе восстановления ее деятельности и работы в новых условиях.

4.2.6 При разработке стратегии менеджмента непрерывности в информационной сфере организации рекомендуется учитывать следующие четыре отдельных, но взаимосвязанных этапа в менеджменте серьезных инцидентов ИБ, имеющие отношение к обеспечению ИБ организации:

1) начальное (первичное) реагирование — охватывает начальные действия, требуемые для обеспечения безопасности и благополучия людей, затронутых инцидентом (ЧС) ИБ, в целях активизации соответствующих групп менеджмента инцидентов и определения уровня реагирования, адекватного инциденту ИБ;

2) восстановление сервисов (услуг) информационной сферы организации — можно осуществлять на нескольких этапах в зависимости от потребностей и масштаба организации. Особенность этапа заключается в восстановлении всех требуемых сервисов в приоритетном порядке до заранее согласованных (возможно, ухудшившихся) уровней сервиса;

3) предоставление услуг по врéменной (промежуточной) схеме деятельности — в случае, если организация будет не готова и не способна возобновить операции штатного обслуживания; в этом случае будет востребовано предоставление необходимых услуг на заранее согласованных уровнях обслуживания, пока обстоятельства не позволят перевести эти нештатные услуги снова в режим обычного функционирования бизнеса или аннулировать их;

4) возобновление штатных (нормальных) услуг — как в случае с восстановлением сервисов, может иметь место на этапах, соответствующих потребностям и приоритетам организации, когда каждый сервис был проверен и было подтверждено его соответствие требованиям штатного функционирования. Все временные дополнительные сервисы должны быть выведены из эксплуатации. Завершением данного этапа является восстановление до штатных (нормальных) уровней услуг всех информационных процессов организации.

4.2.7 Стратегию менеджмента непрерывности в информационной сфере организации необходимо строить на четком понимании потребности организации в согласованных уровнях услуг ИТС и их безопасности с учетом:

- приоритетов ключевых бизнес-подразделений в конкретные периоды времени;
- пиковых нагрузок на бизнес;
- стратегически важных периодов ведения бизнеса, например, периодов отчетности, предельных сроков изготовления и т. п.;
- соответствия с планами и целями менеджмента непрерывности бизнеса;
- воздействия отказа или потери;
- требований ко времени восстановления;
- приемлемых уровней простоя и функционирования;
- изменений и обновлений систем;
- новых проектов;
- взаимозависимости уровней услуг ИТС и их безопасности;
- соблюдения законодательства;
- соблюдения предельных сроков;
- имитации ЧС и обучения действиям при ЧС согласно планам восстановления функций и механизмов безопасности ИКТ после ЧС;
- защиты критически важных данных.

4.2.8 На этапах начального (первичного) реагирования, восстановления сервисов (услуг) информационной сферы организации, а также предоставления услуг по временной (промежуточной) схеме деятельности менеджмент непрерывности в информационной сфере организации должен включать рассмотрение реализации соответствующих мер обеспечения ИБ ИТС. Все решения об использовании (неиспользовании) мер обеспечения ИБ ИТС применительно к идентифицированным факторам рисков ИБ должны быть санкционированы высшим руководством организации.

На этапе возобновления штатных (нормальных) услуг информационной сферы организации необходимые меры обеспечения ИБ ИТС должны функционировать в штатном режиме, а их эффективность — оцениваться в рамках СМИБ организации.

4.3 Роль совета директоров и исполнительных органов организации

4.3.1 Приоритеты бизнеса должны быть установлены на уровне совета директоров или высшего исполнительного органа организации с учетом договорных обязательств, требований к срокам и порядку финансовой и иной отчетности и т. д.

Данная система приоритетов должна быть основой планирования в рамках менеджмента непрерывности в информационной сфере организации, а также основой установления приоритетов при восстановлении после ЧС функций и механизмов безопасности ИКТ.

4.3.2 Лицо, ответственное за обеспечение ИБ организации, должно совместно с руководителем отдела информатизации определить, от каких информационных процессов и автоматизированных систем зависят ключевые приоритетные виды деятельности организации.

Это лицо должно инициировать процесс определения потребностей в мерах обеспечения ИБ ИТС с участием владельцев риска и лиц, ответственных за ключевые приоритетные виды деятельности орга-

низации. Лицо, ответственное за обеспечение ИБ организации, должно довести до сведения руководителя отдела информатизации порядок реализации мер обеспечения ИБ ИТС и согласовать с ним порядок соответствующих действий.

4.3.3 Совет директоров (или равный ему по значимости орган) должен санкционировать порядок реализации мер обеспечения ИБ ИТС в условиях ЧС и в периоды восстановления деятельности организации.

4.4 Идентификация недостатков

4.4.1 Основа стратегии менеджмента непрерывности в информационной сфере организации — обеспечение стабильности деятельности в границах всей информационной инфраструктуры организации. Необходимо проводить внутренние проверки всех возможных недостатков от отдельных точек прерываний до избыточности, зависимости от каналов поставки и общих процессов, связанных со вспомогательными служебными операциями в информационной сфере, такими, как технологии безопасного резервирования и восстановления.

4.4.2 Необходимо планировать, проверять и оценивать улучшение информационной инфраструктуры организации. Для этого должны быть разработаны четкие планы работ в условиях ЧС и определена потребность в использовании конкретных мер безопасности в условиях восстановления после ЧС.

Необходимо достичь соглашения об уровнях инвестиций и приоритетах, связанных с затратами на обеспечение непрерывности в информационной сфере и конкретными затратами на обеспечение ИБ ИТ, на уровне совета директоров или высшего исполнительного органа.

4.5 Непрерывность сервисов в изменяющейся среде и обеспечение информационной безопасности информационных и телекоммуникационных систем

Ключевые факторы, которые должны быть рассмотрены для обеспечения уверенности в том, что стратегия менеджмента непрерывности в информационной сфере организации и планы восстановления деятельности остаются актуальными и эффективными для организации по мере внесения изменений в деятельность организации и ее среду, включают:

- ответственность и подотчетность на уровне совета директоров за стратегию менеджмента непрерывности в информационной сфере эксплуатационной среды организации в целях оценки ее актуальности при изменениях, развитии и росте организации;
- лиц, ответственных за стратегию менеджмента непрерывности в информационной сфере эксплуатационной среды организации. Никакое внесение изменений в информационную инфраструктуру не должно рассматриваться до тех пор, пока последствия изменения не будут оценены и поняты, а планы работ в ЧС не будут проверены;
- обеспечение процесса сопровождения приобретения новых систем проверкой отсутствия компрометации непрерывности в информационной сфере организации;
- учет последствий деятельности, связанной со слияниями и поглощениями организаций. Зачастую деятельность, связанная со слияниями и поглощениями организаций, может обеспечить ощутимые преимущества, выражающиеся в экономии денежных средств. С другой стороны, слияние и поглощение организаций может снизить способности организации по обеспечению требуемой непрерывности в информационной сфере вследствие утраты резервных узлов, дублирующих систем и создаваемой ими избыточности;
- оценку способности поставщиков поддерживать соответствующие уровни услуг;
- внутренний/внешний аудит планов организации.

5 Понимание рисков непрерывности и их влияния на цели деятельности организации и восстановление защитных мер обеспечения информационной безопасности информационных и телекоммуникационных систем

5.1 Виды риска, которые необходимо идентифицировать в контексте обеспечения непрерывности в информационной сфере организации, должны учитывать изменения:

- бизнес-процесса или деятельности организации, включая риски в пределах от катастрофического отказа до незначительного нарушения;
- зависимостей, включая риски, последствия которых колеблются в пределах от потери основного поставщика товаров или провайдера услуг до временного сбоя информационного потока от другого бизнес-процесса;

- оборудования;
- строений или среды;
- информационной технологии или системы;
- процессов менеджмента и защитных мер ИБ, включая обеспечение таких характеристик, как конфиденциальность, целостность и доступность;
- проектов (планов).

Все идентифицированные риски должны быть указаны в плане обеспечения непрерывности в информационной сфере организации.

5.2 Для каждого риска, который идентифицирован как значимый, может быть разработан документированный профиль риска, определяющий:

- характер риска и источники его происхождения (природа риска);
- правдоподобность/вероятность возникновения риска, включая подробности о любых обстоятельствах, в которых правдоподобность/вероятность риска может меняться;
- описание потенциального воздействия риска на бизнес, включая оценки расходов для бизнеса от непринятия мер для предотвращения или уменьшения этого воздействия;
- подробности о возможных признаках возникновения риска и о способах обнаружения этих признаков;
- оценку возможности/вероятности обнаружения риска и меры, которые могут быть приняты для повышения степени этой вероятности;
- подробности о существующих защитных мерах, предназначенных для мониторинга признаков и условий наступления рискового события, предотвращения его возникновения или снижения его воздействия, включая оценки расходов на реализацию и поддержание защитных мер;
- предложения, касающиеся дополнительных защитных мер или изменений существующих защитных мер для предотвращения возникновения рискового события и уменьшения его воздействия, включая подробности о необходимых средствах, оборудовании и персонале, оценке времени, усилий и расходов, необходимых для реализации и поддержания дополнительных защитных мер;
- предполагаемую экономию, получаемую вследствие реализации предложенных защитных мер в случае возникновения рискового события.

Формализация профиля рисков обеспечивает основу для анализа затрат и выгод, которая может служить основанием для принятия решений о том, какие действия следует предпринять в рамках мониторинга риска, модификации риска, передачи риска и мероприятий, связанных с планированием обеспечения непрерывности бизнеса.

5.3 В целом обеспечение непрерывности в информационной сфере организации должно быть основано на понимании потенциальных рисков и их влияния на достижение целей деятельности организации. На этапах восстановления штатной деятельности после ЧС организация может пойти на существенные риски, не компенсированные мерами обеспечения ИБ ИТС в случаях, если последствия невозможности восстановления той или иной деятельности сопряжены с существенными потерями для организации.

Потери в информационной сфере (в части персонала, управления или компонентов инфраструктуры) обычно ведут к утрате возможности эксплуатации и управления информационной инфраструктурой организации с последующим ухудшением или утратой критических информационных сервисов/приложений и данных. Степень воздействия этой потери на организацию зависит от вида деятельности организации.

5.4 Необходимо установить требования ко времени восстановления информационных сервисов и мер обеспечения ИБ ИТС, значимых для реализации критических видов деятельности организации.

5.5 Необходимо установить требования к актуальности данных, используемых при восстановлении информационных сервисов и мер обеспечения ИБ ИТС. Требования к актуальности данных, используемых при восстановлении мер обеспечения ИБ ИТС, должны содержать порядок определения важности информации о конфигурации системы и используемых мерах обеспечения ИБ ИТС.

Невозможность получения актуальной информации о конфигурации и используемых мерах обеспечения ИБ ИТС может создать риски прерывания деятельности организации. Указанные факторы рисков должны быть учтены в рамках менеджмента непрерывности в информационной сфере организации.

Вопросы получения актуальной информации о конфигурации и используемых мерах обеспечения ИБ ИТС должны быть рассмотрены в контексте:

- требований к устойчивости и доступности ИТС;
- основных поставщиков и привлекаемых сторон;

- аппаратных и программных активов;
- хранения;
- режимов резервирования;
- обучения персонала;
- размещения зданий, резервных площадок (помещений) и производственного оборудования;
- передачи данных;
- архивирования.

6 Восстановление после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий

6.1 Организационная основа

6.1.1 Задачи восстановления процессов (функций) и механизмов обеспечения ИБ ИТС организации необходимо решать на трех уровнях ее менеджмента:

1) уровень руководства организации, на котором должны решаться общие вопросы восстановления СМИБ, требующие обязательного участия руководства организации либо являющиеся исключительно его прерогативой,

2) уровень служб/подразделений организации, на котором необходимо решать входящие в их компетенцию вопросы восстановления ИБ, включающие вопросы их взаимодействия при ЧС, в том числе определяемые планами обеспечения непрерывности восстановления ИБ;

3) уровень исполнителей функциональных ролей в подразделениях организации, на котором вопросы восстановления ИБ решают сотрудники (ответственные исполнители) организации в рамках их должностных обязанностей и возложенных на них функций.

6.1.2 На уровне руководства организации исходя из целей бизнеса и на основе результатов оценки рисков необходимо:

- определить бизнес-процессы ИТС, критичные для целей деятельности организации и наиболее чувствительные к нарушению ИБ;
- определить виды информации и элементы ИТС (информационные системы, их компоненты, ИТ-сервисы и т. д.), нарушение ИБ которых влияет на непрерывность процессов деятельности организации (см. ГОСТ Р ИСО/МЭК 27001, приложение А, пункт А.14.1.2);
- установить допустимые границы (пределы) изменчивости свойств (характеристик) ИБ (конфиденциальности, доступности, целостности и др.) ИТС для бизнес-процессов организации при возникновении ЧС (т. е. критерии принятия риска и приемлемые уровни риска);
- утвердить с учетом требований 4.3.2 приоритеты (последовательность) и сроки восстановления (допустимую продолжительность нарушения) средств защиты свойств ИБ элементов ИТС при ЧС;
- обеспечить ресурсы (материальные/технические, людские, финансовые и др.), требуемые для обеспечения и восстановления работоспособности средств и механизмов защиты ИБ при ЧС;
- утвердить обязанности и ответственность в отношении восстановления процессов и механизмов обеспечения ИБ элементов ИТС бизнес-процессов организации при ЧС;
- обеспечить четкое управление и координацию деятельности служб/подразделений организации по восстановлению средств и механизмов обеспечения ИБ элементов ИТС организации при возникновении ЧС.

6.1.3 На уровне служб/подразделений организации необходимо:

- осуществлять оценку и обработку рисков, связанных с нарушением функционирования процессов и механизмов обеспечения ИБ ИТС организации (результаты оценки рисков, связанных с ИБ и влияющих на критичные бизнес-процессы, должны быть доведены до сведения владельцев риска и руководства организации);
- сформировать (разработать) планы и регламенты (процедуры) действий по восстановлению процессов и механизмов обеспечения ИБ при возникновении ЧС;
- определить требования к персоналу (службам) организации на период восстановления процессов и механизмов обеспечения ИБ, нарушенных при возникновении ЧС;
- осуществлять контроль деятельности персонала и служб/подразделений организации по восстановлению процессов и механизмов обеспечения ИБ в рамках возложенных на них ролей;

- отслеживать изменения внешней и внутренней среды организации, а также изменения, вносимые в архитектуру ИТС организации с учетом требований 4.5, и оценивать возможное влияние вносимых изменений на ИБ организации и процессы восстановления средств защиты ИБ.

6.1.4 На уровне исполнителей (в их зонах ответственности, определенных должностными обязанностями/инструкциями) необходимо обеспечивать обслуживание технических средств по обеспечению ИБ и реализацию мероприятий, определенных в соответствующих планах и регламентах, по восстановлению процессов и механизмов обеспечения ИБ, нарушенных при возникновении ЧС.

6.2 Вопросы системы менеджмента информационной безопасности организации и менеджмента непрерывности бизнеса

6.2.1 Положения настоящего стандарта дополняют требования ГОСТ Р ИСО/МЭК 27001 (приложение А, раздел А.14), определяющие следующие цели и меры ИБ организации в контексте обеспечения непрерывности бизнеса:

- включение ИБ в процесс менеджмента непрерывности бизнеса: следует разработать и поддерживать управляемый процесс для обеспечения непрерывности бизнеса во всей организации, который учитывает требования ИБ, необходимые для непрерывности бизнеса организации (см. ГОСТ Р ИСО/МЭК 27001, приложение А, пункт А.14.1.1);
- непрерывность бизнеса и оценка риска: события, которые могут стать причиной прерывания бизнес-процессов, следует идентифицировать наряду с вероятностью и воздействием таких прерываний, а также с их последствиями для ИБ (см. ГОСТ Р ИСО/МЭК 27001, приложение А, пункт А.14.1.2);
- разработка и внедрение планов непрерывности, включая ИБ: следует разработать и внедрить планы для поддержания или восстановления работы и для обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критичных бизнес-процессов (см. ГОСТ Р ИСО/МЭК 27001, приложение А, пункт А.14.1.3);
- структура плана непрерывности бизнеса: следует поддерживать единую структуру планов непрерывности бизнеса для обеспечения непротиворечивости всех планов, последовательного учета в них требований ИБ и идентификации приоритетов для тестирования и поддержки (см. ГОСТ Р ИСО/МЭК 27001, приложение А, пункт А.14.1.4);
- тестирование, поддержка и пересмотр планов непрерывности бизнеса: планы непрерывности бизнеса должны регулярно тестироваться и обновляться для того, чтобы обеспечить их актуальность и эффективность (см. ГОСТ Р ИСО/МЭК 27001, приложение А, пункт А.14.1.5).

6.2.2 Рекомендации по организации деятельности по обеспечению услуг по восстановлению ИКТ и ИТС после ЧС, приведенные в приложении А настоящего стандарта, включают рассмотрение следующих основных областей:

- факторы стабильности внешней среды;
- управление активами, включая информационные активы организации;
- близость площадки, задействованной в восстановлении деятельности организации;
- управление отношениями с поставщиками;
- соглашения о привлечении внешних дополнительных ресурсов;
- обеспечение ИБ;
- активизация и прекращение использования плана восстановления после ЧС;
- обучение и подготовка;
- тестирование систем ИКТ в соответствии с планами непрерывности бизнеса;
- планирование обеспечения непрерывности бизнеса для провайдеров услуг (привлекаемых организаций) по восстановлению ИКТ организации после ЧС;
- документирование задач восстановления ИКТ и ИТС после ЧС и периодический пересмотр документации.

6.2.3 Основные средства восстановления ИКТ и ИТС после ЧС, рассмотренные в приложении В настоящего стандарта, включают:

- площадки для восстановления и их размещение;
- средства физического контроля доступа;
- физическая безопасность помещений;
- специально выделенные зоны;
- средства контроля влияния внешней среды;
- телекоммуникации;

- энергоснабжение;
- управление кабельной системой;
- противопожарную защиту;
- центр работы в чрезвычайной ситуации;
- помещения с ограниченным доступом;
- санитарно-гигиенические нормы и услуги, обеспечивающие жизнедеятельность человека;
- физические мощности и жизненный цикл вспомогательного оборудования;
- тестирование.

Для планирования непрерывности бизнеса в части обеспечения ИБ необходимо рассмотреть факторы риска ИБ в деятельности организаций с учетом положений разделов 4 и 5. При выборе перечисленных и (или) иных средств восстановления ИКТ и ИТС после ЧС необходимо оценивать потребность в реконфигурации используемых или использовании дополнительных мер ИБ (функций и механизмов обеспечения ИБ ИТС организаций), определенных требованиями:

- национальных стандартов в области защиты информации;
- ГОСТ Р ИСО/МЭК 27001 (приложение А), ГОСТ Р ИСО/МЭК 17799 (приложение А), ГОСТ Р ИСО/МЭК 15408-1, ГОСТ Р ИСО/МЭК 15408-2, ГОСТ Р ИСО/МЭК 15408-3;
- стандартов организаций, включая стандарты Центрального банка России [8], ОАО «РЖД», ОАО «Газпром», Ассоциации российских банков и других организаций;
- иных нормативных документов, содержащих своды правил (практик) и требования к мерам ИБ (функциям и механизмам обеспечения ИБ ИТС организаций).

При принятии решения организацией по использованию в своей деятельности документированных профилей риска (см. 5.2) рекомендуется разделы профилей риска, содержащие описание существующих и дополнительных защитных мер, сопровождать комментарием по их соответствию стандартизированным требованиям.

6.2.4 При реализации процедур восстановления ИКТ и ИТС после ЧС необходимо рассмотреть факторы рисков, связанные с выбором резервных площадок для восстановления.

Общие требования к процессу выбора резервной площадки для восстановления изложены в приложении С настоящего стандарта.

6.3 Восстановление и обеспечение функционирования процессов системы менеджмента информационной безопасности организации и защитных мер информационной безопасности при чрезвычайных ситуациях

6.3.1 В целях обеспечения управления ИБ в случае возникновения ЧС в планах обеспечения непрерывности бизнеса организации должны быть предусмотрены мероприятия по восстановлению нарушенных операций, процессов менеджмента ИБ (мероприятия по восстановлению штатного функционирования системы менеджмента ИБ организации).

6.3.2 Разработка и принятие организацией критериев и уровней управляемого снижения эффективности СМИБ организации, означающих предельные возможности по обеспечению ИБ организации в данных условиях, может стать важным положительным фактором. Разработка и принятие организацией критериев и уровней управляемого снижения эффективности СМИБ организации может быть основой для эффективного восстановления процессов деятельности в рамках СМИБ организации (предопределение точек регламентированного возврата в штатное состояние).

Критерии управляемого снижения эффективности должны быть соотнесены с установленными в Российской Федерации категориями ЧС и категориями возможных последствий для организации.

6.3.3 Необходимо рассмотреть следующие мероприятия, связанные с восстановлением процессов деятельности в рамках СМИБ организации:

- защита критичных информационных активов организации;
- эксплуатация защитных мер ИБ (функций и механизмов обеспечения ИБ ИТС организации);
- контроль (мониторинг) факторов рисков ИБ деятельности организации;
- менеджмент инцидентов ИБ организации;
- мониторинг ИБ критичных объектов эксплуатационной среды организации, а также используемых и подключаемых в режиме ЧС дополнительных мер ИБ организации;
- контроль соответствия установленным в организации нормам деятельности в рамках обеспечения ИБ организации в соответствии с требованиями планов по восстановлению штатного функционирования.

6.3.4 Основными задачами системы менеджмента ИБ организации в случае возникновения ЧС являются усиление контроля за соблюдением требований ИБ, установленных в стандартах и нормативных

правовых документах федеральных органов исполнительной власти и внутренних документах организации, и восстановление в кратчайшие сроки нарушенных процессов и механизмов обеспечения ИБ (средств защиты) организации.

Необходимо исключить возможность негативного влияния вторичных рисков деятельности организации, вследствие частичной или полной утраты функциональных возможностей обеспечения ИБ ИТС организации, на процессы восстановления основной деятельности организации. Данные задачи следует решать в плоскости контроля системы менеджмента ИБ организации.

На период восстановления нарушенных процессов и механизмов обеспечения ИБ (средств защиты) менеджмент ИБ организации должен быть направлен (сосредоточен) на усиление организационных мер по обеспечению ИБ.

6.3.5 При возникновении ЧС должны особо соблюдаться требования:

- контроля доступа к информационным активам организации (в особенности лиц сторонних организаций, доминирующие полномочия которых могут быть определены их отношением к государственной системе предупреждения и ликвидации ЧС);

- физической безопасности и сохранности информационных активов организации (защита от повреждений и выноса/хищения);

- обязательной регистрации в журналах действий с критически важными информационными активами организации и сервисами ИТС, осуществляемых персоналом организации и представителями сторонних организаций.

Порядок реализации данных видов деятельности в условиях ЧС необходимо отражать во внутренних нормативных документах ИБ организации (политиках, положениях, регламентах, инструкциях для персонала). Должен быть установлен порядок проверки (проведения учений) готовности организации к выполнению данных требований в условиях ЧС.

6.3.6 В случае повреждения (в результате ЧС) механизмов системы контроля (удаленного) доступа менеджментом ИБ организации должны быть приняты меры по приостановке/запрету (на период восстановления) удаленного доступа к информационным активам организации. В этом случае может быть временно прекращен (запрещен) выход в Интернет, а также ограничен или запрещен для определенных компонентов ИТС обмен по телекоммуникационной сети организации.

6.3.7 При повреждении механизмов криптографической защиты и (или) их ключевой системы на период их восстановления необходимо рассмотреть меры по работе в особых условиях. Менеджмент организации должен рассмотреть риски и принять решение об исключении из режима работы в особых условиях механизмов криптографической защиты информации либо приостановить эксплуатацию компонентов ИТС организации, использующих поврежденные средства криптографии.

6.3.8 Должны быть установлены обязанности персонала для проведения комплекса мероприятий по восстановлению штатного функционирования СМИБ организации исходя из потребностей организации, в обязательном порядке включенные в должностные инструкции персонала организации, привлекаемого к восстановлению СМИБ организации и (или) отвечающего за него.

Должны быть назначены дублеры для основных исполнителей, привлекаемых и (или) отвечающих за восстановление СМИБ организации.

Вопросы привлечения персонала организации или иных лиц к мероприятиям, связанным с восстановлением штатного функционирования системы менеджмента ИБ организации, необходимо планировать в порядке первоочередности с учетом следующих условий:

- наличие персонала для работы в условиях ЧС и восстановление деятельности организации в границах основной или резервной площадки;

- необходимость участия персонала в восстановлении критически важной деятельности (основной, управленческой и т. д.) организации;

- компетенция и навыки персонала;

- предельный срок участия в деятельности по восстановлению штатного функционирования СМИБ организации.

Действия исполнителей ролей по восстановлению СМИБ организации и механизмов обеспечения ИБ (технических средств защиты) должны документироваться (например, в регистрационном журнале, закрепленном за каждым рабочим местом ИТС организации и критичным компонентом ИТС).

6.3.9 В организации должен быть определен и документирован порядок восстановления средств защиты компонентов ИБ ИТС организации, определяющий процедуры и последовательность восстановления.

Восстановление функций и механизмов обеспечения ИБ (средств защиты), нарушенных при аварии и (или) ЧС, необходимо начать с компонентов ИТС, обеспечивающих функционирование критичных (значимых для деятельности организации) бизнес-процессов.

Степень критичности бизнес-процессов и поддерживающих их компонентов ИТС следует устанавливать исходя из особенностей бизнеса организации и приемлемых рисков прерывания ее деятельности, связанных с нарушением ИБ.

6.3.10 Последовательность (приоритетность) восстановления средств защиты конфиденциальности, доступности, целостности и других свойств безопасности для критичных компонентов ИТС каждого бизнес-процесса организации должна быть определена исходя из рисков прерывания деятельности организации, связанных с нарушением данных свойств ИБ.

6.3.11 Последовательность (приоритетность) восстановления средств защиты может быть определена установленной в организации приоритетностью обеспечения защиты свойств ИБ применительно к восстанавливаемым критичным компонентам ИТС каждого бизнес-процесса организации.

6.3.12 Время восстановления всех нарушенных функций и (или) механизмов обеспечения ИБ (средств защиты), необходимых для безопасного функционирования компонентов ИТС бизнес-процесса, не должно превышать допустимой для бизнеса организации продолжительности нарушения непрерывности ИТС бизнес-процесса.

При невозможности выполнения данного условия в организации может быть рассмотрен вопрос о временном прекращении использования защитных мер.

6.3.13 Процесс восстановления нарушенной функции и (или) механизмов обеспечения ИБ (средств защиты) в организации должен быть обеспечен соответствующими ресурсами.

Резервные (запасные) части аппаратного обеспечения и копии инсталляционных носителей программ, необходимые для восстановления элементов аппаратного и программного обеспечения для средств защиты соответственно, должны быть доступны в требуемые для восстановления сроки и защищены от повреждения одновременно с восстанавливаемым средством защиты.

6.3.14 Особенности восстановления средства защиты сервисов ИТ, предоставляемых сторонними организациями (приоритетность восстановления средств защиты и сроки восстановления, непрерывность сервисов ИТ на период восстановления и др.), должны быть отражены в соответствующих соглашениях с конкретными организациями.

Приложение А
(обязательное)

Восстановление информационно-коммуникационных технологий после *чрезвычайной ситуации*

А.1 Общая информация

Предоставление услуг по восстановлению ИКТ после *чрезвычайной ситуации* независимо от того, обеспечивается ли оно внутренними силами организации или осуществляется с привлечением внешних ресурсов, должно соответствовать рекомендациям, описанным в последующих пунктах. Следование рекомендациям гарантирует, что услуги по восстановлению ИКТ после *ЧС* были реализованы после должного рассмотрения непредвиденных событий, могущих оказывать влияние на способность выполнения обязательств по обслуживанию, и взаимосвязанного уменьшения риска посредством предварительных соглашений с другими провайдерами услуг в данной области деятельности.

Следует отметить, что:

a) эти рекомендации будут в различной степени применимы к провайдерам услуг по восстановлению ИКТ после *ЧС*. Провайдеры услуг по восстановлению ИКТ после *ЧС* должны интерпретировать смысл этих рекомендаций в контексте конкретных мощностей и услуг, которые они предлагают или намерены предлагать;

b) когда провайдеры услуг по восстановлению ИКТ после *ЧС* заключают договор или оговаривают соглашения об уровне сервиса с организациями, необходимо учитывать вопрос близости площадки.

А.2 Стабильность внешней среды

Стабильность внешней среды важна для непосредственного функционирования центра по восстановлению, а также для безопасности и благополучия персонала при поездках. Коммунальные услуги, необходимые для функционирования центра по восстановлению, такие, как энергоснабжение и телекоммуникации, могут быть затронуты нестабильностью внешней среды. Безопасность персонала при поездках в центр по восстановлению и из него может зависеть от нарушений в работе транспортной системы. Благополучие персонала и общественная деятельность после работы также могут быть ограничены ненадежной внешней средой. Частое возникновение в крупном масштабе следующих видов действий будет указывать на лежащую в их основе нестабильность внешней среды:

a) забастовки;
b) демонстрации;
c) нарушения общественного порядка;
d) насильственные преступления;
e) природные бедствия;
f) пандемии;
g) намеренные атаки (например, террористические акты, биологические атаки).

А.3 Менеджмент активов

А.3.1 Общая информация

Провайдеры услуг должны обеспечивать, чтобы активы, размещенные в их помещениях для восстановления ИКТ после *ЧС*, могли быть точно идентифицированы, установлены и своевременно извлечены, когда они потребуются организациям. Помимо вычислительного и взаимосвязанного оборудования активы включают прикладные программы, важнейшие записи, хранящиеся на носителях данных (магнитных или иных), и необходимую операционную документацию, которые размещают в операционных помещениях провайдеров услуг для восстановления ИКТ после *ЧС и (или) аварии*.

А.3.2 Права собственности и привилегии организации

Провайдеры услуг должны подробно документировать и актуализировать список активов, размещенных в их помещениях для восстановления ИКТ после *ЧС*. В случае привлечения провайдеров услуг список активов должен быть включен в договоры о предоставлении услуг, в которых должны быть соответствующие пункты для идентификации их прав собственности и привилегий.

А.3.3 Защита активов

Для всех активов, размещенных в помещениях для восстановления ИКТ после *ЧС*, провайдеры услуг должны обеспечивать выполнение следующего:

a) список активов поддерживается (это может быть осуществлено за счет использования менеджмента конфигурации систем и взаимосвязанных процессов, поддерживающих детали текущих версий документации, программных средств и всех остальных активов (ИСО/МЭК 20000 [9], [10] предоставляет руководство по учреждению менеджмента конфигурации));

b) все активы помечаются/маркируются способом, уникально идентифицирующим право собственности;

c) в случае предоставления услуг по восстановлению ИКТ после *ЧС* с привлечением внешних ресурсов организации и привлеченные провайдеры услуг не должны демонстрировать точные названия организаций в

ярлыках/маркировке активов, чтобы не подвергать риску безопасность. Например, на оборудовании, размещенном на коллективно используемых стеллажах, ярлыки/маркировка не должны включать точные названия организаций.

Провайдеры услуг должны установить «системы»[1)] для защиты, поддержки, установления местонахождения, извлечения и возврата всех помеченных/промаркированных активов организации, размещенных в их помещениях, и обеспечить, чтобы активы организации для восстановления ИКТ после *ЧС*:

a) размещали и хранили в безопасной среде;

b) поддерживали в хорошем рабочем состоянии с помощью установки соответствующих средств контроля влияния внешней среды;

c) не использовали или не перебрасывали для других целей, кроме установленных в договоре;

и чтобы местоположение активов организации для восстановления ИКТ после *ЧС* было возможно точно отследить для извлечения.

В случае предоставления услуг по восстановлению ИКТ после *ЧС* с привлечением внешних ресурсов привлеченные провайдеры услуг должны обеспечивать, чтобы:

a) организации были проинформированы в случае перемещения их активов;

b) активы организации извлекали и возвращали в заранее определенные и согласованные временные интервалы, когда приходит запрос от организаций;

c) организации заранее предупреждались и их активы возвращались им в соответствии с надлежащими установленными и согласованными процедурами до начала любой конфискации или прекращения работы.

Организации должны рассмотреть следствия хранения данных для восстановления после *ЧС* и других активов за национальными границами и обеспечить соответствие всем необходимым в данном случае правовым и нормативным требованиям.

А.3.4 Доступность документации

Провайдеры услуг (если этого требуют их соглашения об уровне сервиса) и организации должны поддерживать резервные копии планов, процедур на случай *ЧС*/аварии и другой важной документации для осуществления менеджмента аварий и *ЧС*, включая подробности того, как связаться с персоналом, и о точках доступа для аварийных услуг. Такие резервные планы, процедуры и другую важную информацию необходимо хранить во внешних легкодоступных местах.

А.4 Близость площадки

Площадки для восстановления после *ЧС* должны находиться в таких географических регионах, которые вряд ли будут затронуты той же *ЧС*/аварией, что и основные площадки организаций. Вопрос близости площадок и соответствующих рисков следует принимать во внимание, когда провайдеры услуг по восстановлению ИКТ после *ЧС* заключают договор и обговаривают соглашения об уровне сервиса с организациями.

А.5 Менеджмент отношений с поставщиками

А.5.1 Общая информация

Провайдеры услуг должны оценивать соответствующие риски, а затем принимать адекватные меры для обеспечения того, чтобы критически важное оборудование и услуги могли быть предоставлены их поставщиками в заранее определенные и согласованные временные интервалы. Такими поставщиками могут быть исходные производители оборудования и (или) фирмы-поставщики.

Приведенные ниже рекомендации применяют только к оборудованию, предоставляемому провайдерами услуг. Организациям, разместившим свое оборудование на площадке для восстановления, следует оформить собственные договоренности со своими производителями или поставщиками оборудования.

А.5.2 Поддержка критически важного оборудования

Провайдеры услуг должны установить процедуры для обеспечения специальной поддержки критически важного оборудования его поставщиками, например процедуры для обеспечения замены и поставки критических компонентов ИКТ в заранее определенные и согласованные сроки.

А.5.3 Система поставки

Провайдеры услуг должны обеспечить, чтобы была разработана система поставки, управляющая поставкой оборудования, как новых приобретений, так и замены. Система должна охватывать следующие аспекты:

a) формы поставки и время выполнения заказа на оборудование и запасные части;

b) гарантийный период в случае любых возникающих дефектов;

c) соответствующую предлагаемую поддержку с точки зрения установки, введения в строй и обучения при необходимости;

d) для каждого критически важного компонента ИКТ предоставление дополнительной информации, включая:

1) описание — название, номер устройства и дату приобретения;

2) производителей;

3) поставщиков;

[1)] «Системы» формируются из интегрированных и взаимодействующих компонентов процессов, ресурсов и реализованных элементов (таких, как техническая реализация средств контроля или практических приемов) для достижения заявленной цели.

4) наличие;

5) сроки поставки и установки.

А.5.4 Оборудование, предоставляемое третьей стороной

Провайдеры услуг должны обеспечить, чтобы в случае, когда оборудование может быть предоставлено третьей стороной в аренду или в наем, договоры с такими поставщиками включали следующие положения:

a) ремонт и замена неисправных частей в случае неправильного срабатывания оборудования;

b) идентификация оборудования, не покрывающегося страховкой;

c) сроки и условия возвращения поставщикам арендованного оборудования.

А.5.5 Персонал, предоставляемый третьей стороной

Провайдеры услуг должны установить процедуры для обеспечения квалификации и надежности персонала поставщика, непосредственно вовлеченного в поддержку их услуг по восстановлению. Это должно охватывать персонал, предоставляемый поставщиками для:

a) технического обслуживания и ремонта средств и оборудования на месте и вне места эксплуатации;

b) обеспечения постоянной поддержки услуг в помещениях провайдера услуг в качестве работающего по договору персонала для провайдеров услуг. Эти договоры должны охватывать:

1) предоставление замены в заранее определенные и согласованные сроки, если предоставляемый и работающий по договору персонал недоступен или не способен выполнять порученные задачи по восстановлению ИКТ после ЧС;

2) подтверждение любых необходимых проверок надежности работающего по договору персонала.

А.6 Соглашения о привлечении внешних ресурсов

А.6.1 Общая информация

Провайдеры услуг могут оформлять соглашения о привлечении внешних ресурсов со своими поставщиками на временной или постоянной основе. В отличие от менеджмента отношений с поставщиками третьей стороны, связанного с оборудованием и услугами, предоставляемыми поставщиками, провайдер услуг может обладать меньшей степенью контроля в любом соглашении о привлечении внешних ресурсов. Поэтому выбору и менеджменту отношений с привлеченными поставщиками следует уделять больше внимания. Это включает обеспечение понимания поставщиком специфики деловых потребностей провайдера услуг, более строгие договорные соглашения, более тщательные периодические проверки соглашений о привлечении внешних ресурсов, внимательную проверку средств контроля безопасности поставщика, а также квалификации и надежности персонала поставщика.

Такие соглашения о привлечении внешних ресурсов не должны оказывать влияния на способность провайдеров услуг оказывать услуги организациям. Кроме того, основная ответственность за оказание услуг по-прежнему лежит на провайдерах услуг и не может быть возложена на третью сторону.

А.6.2 Информированность поставщиков

Провайдеры услуг должны обеспечить, чтобы все внешние стороны, вовлеченные в механизм привлечения внешних ресурсов, включая субподрядчиков, сознавали свои обязанности и обязательства по поддержке услуг провайдера услуг. Например, следует проводить периодические информационные совещания для всех привлеченных поставщиков.

А.6.3 Договорное соглашение

Провайдеры услуг должны обеспечить, чтобы обязанности и обязательства привлеченных поставщиков, включая их субподрядчиков, были зафиксированы в договорных соглашениях. Например, привлеченные поставщики должны пополнять ресурсы в заранее определенный и согласованный период времени.

А.6.4 Периодическая проверка

Провайдеры услуг должны проверять риски привлечения внешних ресурсов поставщиков по крайней мере ежегодно. В ходе проверок необходимо изучать:

a) финансовое благополучие и жизнеспособность поставщиков;

b) новые возможности альтернативных поставок.

А.6.5 Средства контроля безопасности поставщиков

Провайдеры услуг должны обеспечить, чтобы всеми сторонами, вовлеченными в соглашения о привлечении внешних ресурсов, был принят идентичный уровень физических, логических и других средств контроля безопасности для ограничения и защиты доступа к функциям провайдера услуг, осуществляемым с привлечением внешних ресурсов. Это должно охватывать все взаимосвязанное оборудование, программные и аппаратные средства и помещения.

Провайдеры услуг должны также обеспечить проведение ими регулярных аудитов всех физических, логических и других необходимых средств контроля безопасности, устанавливаемых привлеченными сторонами.

А.6.6 Качество персонала поставщика

Провайдеры услуг должны обеспечить, чтобы у всех привлеченных поставщиков были формальные политики и процедуры в отношении найма персонала для предоставления услуг. Эти политики и процедуры должны быть частью договорного соглашения с привлеченными поставщиками и включать:

a) требования к квалификации и опыту персонала;

b) необходимость проверки (проверок) надежности персонала поставщика, когда это нужно;

c) политики, касающиеся, например, этики, поведения, полового или расового притеснения;

d) политики и процедуры, связанные с мониторингом функционирования;

e) политики и процедуры, касающиеся замены персонала.

А.7 Информационная безопасность

А.7.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы ИБ организаций не подвергалась риску, а для этого им может потребоваться инвестировать дополнительные ресурсы для выделения и поддержки ИБ организаций.

Провайдеры услуг должны сообщать о физических, логических и других механизмах обеспечения безопасности (включая менеджмент инцидентов (и слабых мест) ИБ) организациям и согласовывать с организациями применимость механизмов обеспечения безопасности при активации плана на случай *ЧС*. Помещения и оборудование для восстановления после *ЧС* необходимо подвергнуть оценке, чтобы убедиться, что они соответствуют требованиям организаций к защите.

Для обеспечения выполнения соответствующих требований безопасности провайдеры услуг должны придерживаться требований ИСО/МЭК 27001 [11] и ИСО/МЭК 27002 [12].

А.7.2 Изолирование систем информационно-коммуникационных технологий

Провайдеры услуг должны обеспечить, чтобы информация системы ИКТ одной организации не была доступна или не стала известна системе ИКТ другой организации, если только это не разрешено. Провайдеры услуг должны создать средства для идентификации и физического и логического изолирования размещенных в их помещениях различных систем ИКТ, которые:

a) поддерживают и сопровождают различные внешние поставщики;

b) абонированы разными организациями.

А.7.3 Ограничение и разделение персонала

Провайдеры услуг в своих помещениях для восстановления при необходимости должны создать средство для идентификации и ограничения доступа различного персонала к системам ИКТ и информации для обеспечения того, чтобы:

a) существовали ограничения физического доступа к помещениям, вмещающим системы ИКТ. Например, системы ИКТ с разными требованиями защиты должны быть размещены в разных сооружениях или участках/помещениях, чтобы могли быть надлежащим образом реализованы средства физического контроля доступа;

b) рабочие участки, используемые персоналом провайдера услуг, организации и поставщика, были спланированы и спроектированы с учетом конфиденциальности и секретности информации, которые в этом случае являются главными требованиями при проектировании, например, применительно к сооружениям и (или) выделенным отдельным участкам/помещениям для использования персоналом различной принадлежности.

А.7.4 Передача данных

Провайдеры услуг должны обеспечить поддержку целостности и конфиденциальности данных организации для восстановления после *ЧС* во время передачи (электронным или физическим способом) на площадку для восстановления после *ЧС* и с нее с учетом договорных обязательств перед организациями.

А.7.5 Менеджмент инцидентов информационной безопасности

Провайдеры услуг должны обеспечить, чтобы обо всех инцидентах ИБ и слабых местах безопасности быстро сообщалось соответствующим органам и принимались необходимые меры. Должна существовать полностью совместимая с ГОСТ Р ИСО/МЭК ТО 18044 схема менеджмента инцидентов ИБ.

А.7.5.1 Процедуры

Должна быть установлена формальная совокупность процедур для разрешения вопроса инцидентов (и слабых мест) ИБ (включая физические). Она должна охватывать:

a) обнаружение всех инцидентов (и слабых мест) ИБ и взаимосвязанные процедуры и пути их распространения;

b) сообщение обо всех инцидентах (и слабых местах) ИБ и их регистрацию;

c) регистрацию реагирования, принятых предупредительных и корректирующих мер;

d) периодическую оценку всех инцидентов (и слабых мест) ИБ;

e) извлечение уроков из проверок инцидентов (и слабых мест) ИБ и внесение усовершенствований в обеспечение безопасности и схему менеджмента инцидентов (и слабых мест) ИБ.

А.7.5.2 Критерии оценки

Все инциденты (и слабые места) ИБ необходимо оценивать, когда нужно, путем изучения журналов регистрации. Должны быть созданы критерии оценки инцидентов (и слабых мест) ИБ и (или) реагирования персонала на основе:

a) обнаружения: Как был обнаружен инцидент (или слабое место) ИБ? Могут ли параметры обнаружения быть улучшены с помощью технических мер или иным способом?

b) уведомления: Как было сообщено об инциденте (или слабом месте) ИБ соответствующему персоналу? Были ли проинформированы о сложившейся ситуации все затронутые стороны? Существуют ли альтернативные и более эффективные каналы оповещения и предупреждения?

c) реагирования: Как принимались решения и осуществлялось реагирование? Могут ли быть сделаны дальнейшие усовершенствования для улучшения процесса принятия решений?

d) эффективности: Были ли надлежащими оценки инцидентов (или слабых мест) ИБ и (или) взаимосвязанного ущерба? Было ли эффективным реагирование, например, с точки зрения сдерживания или предотвращения дальнейших инцидентов (или слабых мест) ИБ и (или) взаимосвязанного ущерба?

А.8 Активация и дезактивация плана восстановления после *чрезвычайной ситуации*

А.8.1 Общая информация

Провайдеры услуг должны вместе с организациями установить условия и процедуры активации и дезактивации услуг по восстановлению после *ЧС*.

Организации вместе со своими провайдерами услуг (с учетом договорных обязательств провайдера услуг перед организацией) должны поддерживать резервные копии планов, процедур на случай *ЧС*/аварии и другой важной информации (такой, как списки контактных данных или «дерево звонков») для осуществления менеджмента *ЧС* и аварий.

А.8.2 Предварительные соглашения

Для предотвращения путаницы и разногласий провайдеры услуг должны обеспечить, чтобы между ними и организациями были установлены предварительные соглашения, в обязательном порядке задокументированные и доведенные до уполномоченного персонала. Они должны включать:

a) список уполномоченных представителей организации, которые могут активировать или дезактивировать абонированные услуги;

b) принятые между представителями провайдера услуг и организации средства связи для уведомления, подтверждения, активации и дезактивации абонированных услуг;

c) условия, в силу которых организация может активировать или дезактивировать абонированные услуги;

d) протокол уведомления любой стороны об уходе или изменениях в составе основного персонала (чтобы принять меры предосторожности против неправомерной активации и т. д.);

e) список персонала организации, которому разрешен доступ к помещению для восстановления ИКТ после *ЧС* после активации плана.

А.8.3 Уведомление

Провайдеры услуг должны обеспечить, чтобы заключаемые с организациями соглашения включали при необходимости приведенные ниже процедуры уведомления:

a) первоначальное уведомление представителями организации представителей провайдера услуг;

b) подтверждение со стороны представителей провайдера услуг представителям организации;

c) уведомление персонала провайдера услуг, непосредственно вовлеченного в предоставление абонированных услуг, в целях достижения его готовности;

d) уведомление внешних поставщиков провайдера услуг, вовлеченных в предоставление абонированных услуг, в целях достижения их готовности;

e) консультацию с представителями организации по вопросу одной из следующих линий действий:

1) продолжать оставаться в состоянии готовности;

2) прекратить уведомление;

3) активировать абонированные услуги в течение заранее определенного периода времени.

Вся связь между представителями провайдера услуг и организации на этапе уведомления должна осуществляться посредством заранее согласованных между провайдерами услуг и организациями средств связи.

А.8.4 Инициирование услуг

Провайдеры услуг должны обеспечить, чтобы заключаемые с организациями соглашения включали при необходимости приведенные ниже процедуры активации абонированных услуг:

a) информирование руководства провайдера услуг об активации услуг организацией;

b) получение необходимых записей из безопасного хранилища (с учетом договорных обязательств перед организациями);

c) приведение в действие персонала провайдера услуг, непосредственно вовлеченного в предоставление абонированных услуг;

d) приведение в действие внешних поставщиков провайдера услуг, вовлеченных в предоставление абонированных услуг;

e) подготовку абонированных услуг, например площадки для восстановления, для передачи занимающемуся восстановлением персоналу организации;

f) передачу абонированных услуг, например площадки для восстановления и оборудования, провайдерами услуг занимающемуся восстановлением персоналу организации.

Время реагирования для каждой из приведенных выше процедур тоже должно быть включено в соглашение с каждой организацией.

А.8.5 Завершение оказания услуг

Провайдеры услуг должны обеспечить, чтобы заключаемые с организациями соглашения включали процедуры, упорядочивающие передачу организациями помещений и оборудования провайдерам услуг, когда услуги предоставлены.

А.9 Обучение и образование

А.9.1 Общая информация

Провайдеры услуг и организации должны обеспечить, чтобы обучение восстановлению ИКТ после *ЧС* предоставлялось всему персоналу провайдера услуг и привлеченному персоналу организации, в особенности, чтобы весь новый персонал был соответствующим образом обучен, мог принимать на себя и компетентным образом выполнять свои рабочие обязанности. Члены персонала должны быть признаны компетентными, прежде чем им

будут поручены рабочие обязанности. Обучение можно проводить при помощи собственного персонала или привлекать третьи стороны. Вводное обучение восстановлению после *ЧС* должно быть предоставлено всему персоналу, а специальное обучение — персоналу, которому поручены основные обязанности по восстановлению после *ЧС*.

А.9.2 Обучение персонала провайдера услуг

Провайдеры услуг должны обеспечить «систему», гарантирующую, что весь персонал, непосредственным образом вовлеченный в предоставление услуг организациям по восстановлению ИКТ после *ЧС*, включая персонал, управляющий физическими мощностями, соответствующим образом обучен и аттестован, а именно:

a) все члены персонала провайдера услуг проходят формальное обучение по восстановлению ИКТ после *ЧС* и получают образование, соответствующее их ролям в восстановлении организации. Персонал, управляющий физическими мощностями, должен пройти формальное обучение и получить подготовку, соответствующую операционным ролям. Для персонала, выполняющего основные обязанности, необходимо проводить аттестацию обучаемых во время и (или) в конце каждого курса обучения;

b) все учебные занятия необходимо документировать, фиксировать результаты и принимать меры для рассмотрения вопросов, касающихся выявленных недостатков.

А.9.3 Обучение персонала организации

Организации должны установить программы для обучения своего персонала, которому будут поручены обязанности во время аварии или *ЧС* (например, администраторы баз данных, старший персонал в сфере разработки приложений, администраторы средств связи, работники, оказывающие первую помощь, начальники пожарной службы и, возможно, часть старшего персонала из числа пользователей), чтобы обеспечить удовлетворительные результаты во время *ЧС*/аварии. По аналогичным причинам вовлеченный персонал организации должен также участвовать в учениях, связанных с планами восстановления после *ЧС*.

Организации также должны обеспечить, чтобы заместители основного персонала были обучены и участвовали в учениях, связанных с планами восстановления после *ЧС*, на случай, если основной персонал будет недоступен, когда это потребуется.

Проводимое организацией тестирование, включая имитацию *ЧС*/аварии, хотя и является ценным, не должно быть единственным элементом формального обучения. Это мероприятие дает практический опыт, но не обеспечивает систематического и тщательного обучения.

А.9.4 Виды обучения

Провайдеры услуг и организации должны обеспечить, чтобы виды предоставляемого для персонала обучения были соразмерны порученным задачам и обязанностям. Виды обучения включают:

a) вводное обучение — для обеспечения базового понимания и осознания;

b) обучение повышенного уровня — для усвоения персоналом специальных знаний и навыков для выполнения порученных задач;

c) постоянное обучение — для поддержки знаний персонала на уровне, отвечающем современным требованиям, и обеспечения его компетентности при выполнении порученных задач;

d) тренинг — для поддержки компетентности и готовности персонала.

А.9.5 Объем и частота обучения

Провайдеры услуг и организации должны составить график соответствующего обучения для всего персонала и поддерживать запись предоставленного обучения, охватывающего:

a) вводное обучение при занятии своей должности — для всего нового персонала;

b) обучение повышенного уровня для подготовки персонала к выполнению ключевых задач — для специального персонала.

Для персонала, выполняющего основные обязанности, обучение необходимо проводить по крайней мере раз в год, а для всего персонала — по мере необходимости, после существенных изменений средств и услуг, которые могут оказывать влияние на предлагаемые организациям услуги.

А.9.6 Оценка

Провайдеры услуг и организации должны обеспечить проведение оценки всего обучения. Оценку персонала необходимо проводить по одному или более из приведенных ниже элементов:

a) понимание и интерпретация персоналом политик, процедур и работы оборудования и мощностей, например отмены физического доступа при увольнении персонала;

b) реагирование персонала на конкретные события (например, на физическое вторжение).

А.10 Тестирование систем ИКТ

Провайдеры услуг должны обеспечить регулярное тестирование всех систем ИКТ, необходимых для восстановления после *ЧС*, чтобы гарантировать их постоянную возможность поддержки планов восстановления после *ЧС*.

Тестирование также необходимо проводить в случае каких-либо существенных изменений требований организации и (или) изменений мощностей и возможностей провайдера услуг, влияющих на предоставляемые организациям услуги. Примеры таких изменений включают перебазирование площадок для восстановления после *ЧС*, существенные модернизации систем ИКТ или подготовку новых систем ИКТ.

А.11 Планирование обеспечения непрерывности бизнеса для провайдеров услуг по восстановлению ИКТ после *чрезвычайной ситуации*

Конечным результатом этой работы провайдеров услуг должны быть создание, тестирование, поддержка и обновление планов обеспечения непрерывности бизнеса, охватывающих все деловые функции. Однако провайдеры услуг не должны переходить непосредственно к созданию планов без соответствующей важной предварительной работы. Провайдеры услуг должны сначала идентифицировать свои деловые приоритеты, а затем верную и наиболее рентабельную стратегию обеспечения непрерывности бизнеса, соответствующую их деловой среде. Только когда у провайдеров услуг будут согласованные стратегии обеспечения непрерывности бизнеса и, таким образом, понимание наилучшего пути вперед, они должны создавать, тестировать и использовать планы обеспечения непрерывности бизнеса, а также осуществлять менеджмент рисков, чтобы и далее снижать вероятность необходимости активации планов и (или) уменьшать влияние *ЧС* или аварии, если таковые произойдут. Общий подход, которому рекомендуется следовать при планировании обеспечения непрерывности бизнеса, приведен на рисунке А.1.

Рекомендуемый подход состоит из ряда отдельных этапов, вместе направленных на достижение обстоятельного и жизнеспособного плана обеспечения непрерывности бизнеса, который будет полностью отвечать требованиям бизнеса провайдеров услуг в случае *ЧС* или аварии. Эти этапы таковы:

a) установление требований, временной шкалы и приоритетов восстановления бизнеса (включая первоначальное проведение анализа влияния на бизнес и оценки риска);

b) формулировка стратегии обеспечения непрерывности бизнеса;

c) создание плана обеспечения непрерывности бизнеса;

d) тестирование плана обеспечения непрерывности бизнеса;

e) осознание всем персоналом обеспечения непрерывности бизнеса;

f) постоянная поддержка плана обеспечения непрерывности бизнеса;

g) снижение риска.

Первые пять этапов являются последовательными. Когда план впервые создается и тестируется, мероприятия шестого этапа осуществляют через какое-то время, проводят через регулярные интервалы, а также после существенных изменений, которые могут оказать влияние на действенность планов, возвращаясь к любому другому этапу в целях корректировки при необходимости. Седьмой этап проводят параллельно другим этапам.

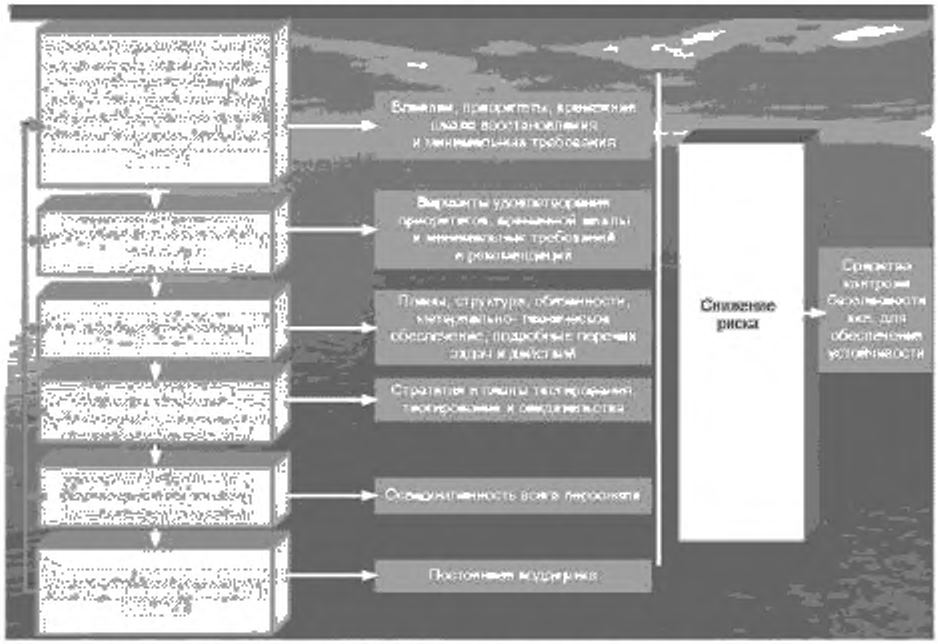


Рисунок А.1 — Подход к планированию обеспечения непрерывности бизнеса

А.12 Документация и периодический пересмотр

Все созданные политики, планы и положения должны быть задокументированы. Персоналу соответствующего уровня должно быть поручено обеспечение периодического пересмотра и обновление каждого документа. Система менеджмента конфигурации должна быть использована для поддержки текущих версий документов, а также, например, для создания инвентаризационных описей активов и программного обеспечения.

Приложение В
(обязательное)

Средства восстановления информационно-коммуникационных технологий после *чрезвычайной ситуации*

В.1 Общая информация

Провайдеры услуг по восстановлению ИКТ после *ЧС* должны удовлетворять основным требованиям, чтобы они могли обеспечивать безопасную физическую рабочую среду для содействия усилиям организации по восстановлению. В дополнение к охвату основных требований к физическим мощностям должны быть также рассмотрены требования к средствам контроля влияния внешней среды, телекоммуникациям, постоянному энергоснабжению и не относящимся к восстановлению удобствам, таким, как парковка и доступность питания и воды. Для провайдеров услуг со многими площадками для восстановления руководство должно в равной степени относиться к каждой и ко всем площадкам.

В.2 Местоположение площадок для восстановления

В.2.1 Общая информация

Местоположение площадок для восстановления может иметь нежелательные уязвимые места, вследствие которых на наилучшим образом спроектированной и оборудованной площадке для восстановления существуют остаточные риски, которые не могут быть уменьшены. Примеры таких потенциальных угроз описаны ниже.

В.2.2 Опасности природного характера

Площадки для восстановления не следует размещать в районах, подверженных опасностям природного характера, или следует оценить и уменьшить или же принять риски. Эти опасности природного характера включают (перечень может быть расширен):

a) вулканы и землетрясения;

b) тайфуны, ураганы и бури;

c) нахождение на низменных участках рядом с реками, подверженными разливу после дождя;

d) грозовые разряды.

В.2.3 Метеорологические изменения

Экстремальные и внезапные изменения внешней среды могут оказывать влияние на физические мощности и доступность площадок для восстановления. Площадки для восстановления следует выбирать на основе оценки степени и скорости метеорологических изменений и вероятного влияния на:

a) физические мощности (например, внезапное изменение температуры внешней среды может вызвать разрыв водопроводной трубы и затопление подвала);

b) доступность (например, сильные ливни могут оказывать влияние на значительные сегменты транспортной системы и ограничивать доступность площадок для восстановления).

В.2.4 Промышленные и коммерческие опасности

Площадки для восстановления не следует размещать вблизи мест с потенциальными промышленными или коммерческими опасностями, включая, например:

a) расположенные поблизости предприятия, обрабатывающие химические или взрывчатые вещества;

b) авиалинию прямо над площадкой для восстановления;

c) расположенные поблизости постоянно заполненные больницы, особенно те, которые имеют дело с определенными заболеваниями (такими, как пандемии, например, птичьего гриппа, атипичной пневмонии), с результирующим скоплением транспорта;

d) строения или участки, где осуществляется коммерческая деятельность, могущие стать объектом для общественных демонстраций или других угроз.

В.2.5 Доступность

Площадки для восстановления следует размещать в районах с хорошей доступностью. Должна быть возможность перемещения на площадки для восстановления персонала и оборудования организации без чрезмерной задержки. Доступность следует измерять:

a) надежными воздушными связями (от международных до местных аэропортов при необходимости);

b) качественным железнодорожным сообщением;

c) обширной дорожной сетью;

d) удобным сообщением от аэропортов и железнодорожных станций до площадок для восстановления;

e) удобным сообщением от гостиниц до площадок для восстановления;

f) простотой зарубежного или транснационального въезда при необходимости.

Основные площадки организации и площадки для восстановления должны размещаться как можно дальше друг от друга, однако с учетом того условия, что если от персонала организации потребуют реализации планов восстановления после *ЧС* на площадках для восстановления, то время восстановления должно быть выдержано.

В.2.6 Альтернативные маршруты

Необходимы альтернативные маршруты доступа к площадкам для восстановления, если на обычных маршрутах доступа к площадкам для восстановления возникают неожиданный затор, остановка или блокирование движения, а обходной доступ невозможен без чрезмерных трудностей для персонала и оборудования. Например, площадка для восстановления, доступ к которой возможен только через мост, может пострадать от физической изоляции, если мост будет поврежден. В таком случае необходим альтернативный маршрут доступа, обходящий мост.

В.2.7 Коллективно используемые помещения

Провайдерам услуг следует уделять особое внимание площадкам для восстановления, расположенным в коллективно используемых помещениях, из-за больших рисков нахождения в непосредственной близости других организаций и их персонала по сравнению с использованием специальных помещений для индивидуального использования. Провайдеры услуг должны обеспечить, чтобы:

a) формальные проверки оценки риска и уменьшения риска для коллективно используемых помещений проводились:

1) периодически, по крайней мере ежегодно;

2) когда происходят существенные изменения, связанные с коллективно используемыми помещениями (например, появление новых арендаторов и изменение назначения помещений существующими арендаторами);

b) подробности об остаточных рисках, которые не могут быть уменьшены, были предоставлены организациям для рассмотрения.

В.2.8 Коммунальные предприятия

Площадки для восстановления не следует размещать вблизи предприятий, предоставляющих коммунальные или иные услуги, так как площадки уязвимы к воздействиям, которые могут затрагивать операции. Такие коммунальные предприятия могут создавать вибрацию, помехи или стать объектом вредительства. Примеры таких предприятий:

a) электростанции;

b) сооружения связи башенного типа;

c) подземные и наземные железнодорожные линии.

В.2.9 Кабельная инфраструктура

Телекоммуникационные и силовые кабели от поставщиков к площадкам для восстановления не должны быть чрезмерно подвержены риску внешнего физического повреждения. Например, кабельная система, подвешенная на столбах, по сравнению с подземной кабельной системой подвержена большему риску физического повреждения, которого следует избегать.

В.2.9.1 Уменьшение риска

Для площадок для восстановления, подвергающихся потенциальным рискам, которые нельзя устранить, должны существовать соответствующие процедуры уменьшения риска и должны быть предприняты усилия для минимизации этих рисков до соответствующего уровня. Пример таких потенциальных рисков — строительство нового предприятия по обработке опасных веществ поблизости.

В.3 Средства физического контроля доступа

В.3.1 Общая информация

Средства физического контроля доступа представляют собой ключевые элементы в обеспечении защиты площадок для восстановления, и крайне важно, чтобы такие средства контроля существовали и функционировали во всех точках входа и выхода зданий. После входа персонал организации должен иметь доступ ко всем выделенным ему помещениям, без навязывания дополнительного контроля доступа при перемещении персонала из одной части абонированных помещений для восстановления в другую (если только это не является абсолютно необходимым).

Поэтому провайдеры услуг должны обеспечить, чтобы были установлены, задокументированы и реализованы средства, политики и процедуры физического контроля доступа, соразмерные оцененным рискам и предоставляемым организациям услугам, для осуществления контроля и мониторинга физического доступа в помещения провайдера услуг, из них и внутри их.

В.3.2 Классификация кадровой безопасности

Должна быть установлена формальная система классификации кадровой безопасности, учитывающая следующие категории персонала:

a) персонал провайдера услуг;

b) служащие организации;

c) поставщики и подрядчики;

d) посетители.

В.3.3 Охраняемые зоны

В помещениях провайдера услуг должны быть идентифицированы и установлены отдельные зоны, имеющие физическую защиту, с:

a) мощностями с ограниченным доступом — зоны/помещения, вмещающие основное оборудование и мощности, такие, как серверы и другое компьютерное оборудование, коммутаторы связи и другое взаимосвязанное

оборудование, а также кабельная система, архивы носителей данных, оборудование для кондиционирования воздуха и основные распределительные стойки для энергоснабжения;

b) общедоступными мощностями — зоны/помещения, используемые всем персоналом и не подвергающиеся каким-либо внутренним ограничениям, связанным с безопасностью, например приемные, конференц-залы, кафетерии, туалеты.

Должна быть установлена формальная система контроля доступа персонала в каждую из охраняемых зон на основе классификации кадровой безопасности, которая должна действовать в течение всего времени проведения работ по восстановлению.

В.3.4 Персонал

Должны быть установлены формальные процедуры для рассмотрения вопроса, касающегося персонала, присоединенного к провайдерам услуг или уходящего от провайдеров услуг. Они должны охватывать:

a) новый персонал, присоединенный к провайдеру услуг, — для определения применимого уровня санкционированного доступа и последующей выдачи соответствующих идентификационных карточек/нагрудных визиток для физического контроля доступа;

b) персонал, подлежащий увольнению, — для немедленного уведомления службы безопасности об увольнении членов персонала с отменой всех соответствующих санкционирований доступа и возвратом идентификационных карточек/нагрудных визиток для физического контроля доступа.

В.3.5 Контроль доступа

Должны быть установлены формальные политики и процедуры для контроля входа в помещения провайдера услуг для обеспечения того, чтобы весь проход происходил в специальных точках входа и чтобы личность всех членов персонала, включая посетителей, проверялась при входе.

В.3.6 Лица, не относящиеся к персоналу

Должны быть установлены формальные политики и процедуры для контроля прохода и перемещения лиц, не относящихся к персоналу провайдера услуг, в помещениях провайдера услуг для обеспечения того, чтобы:

a) запросы на вход в помещения провайдера услуг и доступ к оборудованию были заранее определены и организованы, например, разрешение может быть получено посредством предшествующего электронного письма и беседы (если подающее запрос лицо хорошо известно соответствующему персоналу провайдера услуг, который подтверждает санкционирование занимающемуся обеспечением безопасности персоналу) или представления формальной подписанной формы санкционирования;

b) занимающийся обеспечением безопасности персонал на входе осуществлял встречную проверку с привлечением имеющего к этому отношение персонала провайдера услуг;

c) посетители всегда оставались в вестибюле или сопровождались в специальные, находящиеся под надзором помещения для ожидания, пока они не будут приняты персоналом провайдера услуг;

d) проход подрядчиков, расположенных на площадке, для заранее определенной цели и в определенный период времени был ограничен зонами/помещениями, которые необходимы для выполнения их конкретных санкционированных задач. Это относится к уборщикам, поставщикам провизии и другому привлеченному обслуживающему персоналу;

e) всех посетителей, направляющихся в зоны с ограниченным доступом, в течение всего времени сопровождал персонал провайдера услуг;

f) персонал поставщика, занятый работами по техническому обслуживанию в зонах с ограниченным доступом, находился под физическим надзором, для недопущения получения им доступа к системам вне сферы его деятельности (если физическому контролю препятствуют ограничения, связанные с ресурсами, допустим также мониторинг с помощью замкнутой телевизионной системы);

g) идентификационные карточки выдавались всем посторонним лицам, проходящим в помещения провайдера услуг, включая постоянных подрядчиков, таких, как уборщики и работники кафетерия. В *В.4.8* описано использование идентификационных карточек для контроля перемещения персонала в помещениях;

h) поддерживался журнал регистрации прохода посторонних лиц в помещения провайдера услуг, включая постоянных подрядчиков. В журнале регистрации фиксируют:

1) личность посторонних лиц, включая фамилию и название организации;
2) цель посещения;
3) посещаемых сотрудников провайдера услуг;
4) время входа/выхода;
5) замечания;
6) подпись сотрудника в журнале регистрации.

В.3.7 Персонал организации

Должны быть установлены формальные политики и процедуры для регулирования доступа персонала организации к помещениям провайдера услуг, охватывающие:

a) обычное время, когда уполномоченному персоналу организации разрешено посещение площадки для восстановления в заранее согласованное время, как предусмотрено в договоре провайдера услуг с организацией, например в период тестирования;

b) время ЧС/аварии, когда персоналу организации предоставлен постоянный доступ к выделенным зонам/помещениям для проведения операций по восстановлению.

В.3.8 Поведение персонала в охраняемых зонах с ограниченным доступом

Должны быть установлены формальные политики и (или) принципы, регулирующие поведение персонала в помещениях с ограниченным доступом, таких, как серверные, вычислительные центры и архивы носителей данных. Эти политики должны включать:

a) запрет курения;

b) запрет приема пищи и употребления напитков;

c) условия использования устройств, генерирующих радиочастоту, например мобильных телефонов, вблизи чувствительного оборудования;

d) условия использования устройств хранения данных и фотоаппаратуры, например персональных цифровых секретарей, универсальной последовательной шины (USB) накопителей и мобильных телефонов со встроенной фотокамерой.

В.3.9 Функции и роли по обеспечению безопасности

Провайдеры услуг должны установить обязанности соответствующего персонала по поддержанию безопасности.

Они должны охватывать:

a) назначение конкретного персонала на выполнение обязанностей, связанных с физической безопасностью *персонала*, например для целей распространения/предоставления информации в случае инцидента ИБ;

b) назначение компетентных заместителей для выполнения критических обязанностей в случае, когда основные назначенные лица недоступны или иным образом не способны выполнять работу;

c) адекватное обучение всего назначенного персонала, прежде чем ему будет поручено обеспечение безопасности;

d) периодическое посещение всем назначенным персоналом курсов повышения квалификации по обеспечению безопасности, чтобы гарантировать, что назначенный персонал остается компетентным в выполнении своих задач;

e) установление процедур тестирования персонала, которому поручено обеспечение безопасности, чтобы гарантировать поддержку его готовности и знаний. Тестирование следует проводить периодически, например раз в год. Оценка реагирования персонала во время тестирования должна соответствовать критериям оценки, приведенным в *А.7.5.2 (приложение А)*.

В.3.10 Тестирование

Стратегия, цели, планы тестирования, само тестирование и результаты тестирования образуют неотъемлемую часть системы управления, поддерживающую ее целостность. Политики и процедуры, определяющие планирование, проведение, документирование, проверку и жизненный цикл тестирования, приведены в *В.15.4*.

В.3.11 Инциденты (и слабые места) физической безопасности

Обо всех инцидентах (и слабых местах) физической безопасности должно быть немедленно сообщено соответствующему органу и должны быть приняты соответствующие меры. Об урегулировании инцидентов (и слабых мест) информационной безопасности (включая физические) см. в *А.7.5 (приложение А)*.

В.3.12 Нерабочее время

Должны быть установлены политики и процедуры для регулирования доступа персонала к помещениям для восстановления во внерабочее время (например, доступ персонала во время праздников). Они должны включать:

a) процедуры санкционирования и уведомления;

b) порядок действий в чрезвычайных ситуациях, например во время восстановления после бедствия, на рабочих местах организации.

В.3.13 Санкционирование

Санкционирование всего физического доступа к помещениям провайдера услуг и находящимся в них мощностям с ограниченным доступом необходимо:

a) предоставлять на основе принципов «необходимого знания» и «необходимого сдерживания»;

b) пересматривать и обновлять на периодической основе.

В.3.14 Обеспечение непрерывности

Все реализованные средства, политики и процедуры должны действовать 24 часа в сутки и 365 дней в году.

В.4 Физическая безопасность помещений

В.4.1 Общая информация

В соответствии с результатами оценки риска должны существовать физические средства контроля безопасности и процедуры для защиты электронных информационных систем, строений, мощностей и оборудования провайдера услуг и организации от несанкционированного физического доступа, изменения и повреждения. Таким образом, все помещения, предоставляемые организациям провайдерами услуг, должны быть физически защищены и подвергаемы мониторингу, прежде всего в целях безопасности и охраны здоровья персонала.

В.4.2 Концепция защиты

Должна быть установлена единая концепция защиты для интеграции всей физической защиты безопасности и процедур. Эта концепция защиты должна формировать основу всей физической защиты безопасности и процедур, чтобы они могли объединяться и дополнять друг друга. Например, концепция защиты, базирующаяся только на высокой стене по периметру, будет неэффективна против других форм вторжения. Используемая концепция защиты должна быть основана на одном из следующих подходов:

a) многоуровневый — помещения делятся на уровни от внешнего периметра до внутреннего центра с соответствующим возрастанием накладываемых ограничений (например, требуется дополнительный допуск, отличающийся от разрешения для прохода через ворота, чтобы войти в серверную);

b) основанный на секторах — помещения делятся на отдельные секторы, например секторы А, Б, В и Г, и каждому сектору соответствуют разные критерии защиты доступа для ограничения прохождения из одного сектора в другой;

c) комбинированный — сочетание многоуровневого подхода и основанного на секторах: помещения делятся на отдельные секторы с возрастанием накладываемых ограничений от внешнего периметра до внутреннего центра для каждого сектора.

Концепция защиты должна реализовываться на основе надлежащего планирования, проектирования, сооружения и управления физическими помещениями.

В.4.3 Физическое строение

Физические строения, вмещающие площадки для восстановления, необходимо планировать, проектировать и строить с учетом обеспечения безопасности. В строениях, специально не предназначенных для этого (например, коллективно используемых помещениях), должны быть реализованы надлежащие средства контроля для уменьшения соответствующих рисков безопасности.

В.4.3.1 Внешние стороны

Периметры и внешние стороны всех строений с мощностями для восстановления должны быть физически защищены от вторжения и вандализма. Средства контроля безопасности должны включать:

a) прочную конструкцию внешних стен строений;

b) надлежащую защиту всех дверей и при необходимости окон от несанкционированного доступа, например, путем прочной конструкции и установки замков и сигнализации.

Кроме того, строения должны быть защищены от ударов молнии и наведенных скачков напряжения, которые могут повредить внутренность строения и (или) вызвать постоянную или временную неисправность размещенного в нем электрического и электронного оборудования. Примеры соответствующих средств контроля включают молниеотводы и устройства защиты от электрического перенапряжения для критически важного оборудования.

В.4.3.2 Внутренняя часть

Физические барьеры для помещений с ограниченным доступом внутри строений, например машинного зала, должны включать стены, простирающиеся от пола до потолка (т. е. плита к плите), для предотвращения несанкционированного прохода и загрязнения среды, например из-за дыма или огня. Если это невозможно, провайдеры услуг должны реализовать другие барьеры.

В.4.3.3 Инспектирование

Все строения с мощностями для восстановления необходимо периодически инспектировать, при этом инспектирование должно охватывать, как минимум:

a) все входы в помещения провайдера услуг и выходы из них;

b) зоны, непосредственно окружающие периметр помещений провайдера услуг;

c) заборы по периметру и (или) стены помещений провайдера услуг;

d) любые неиспользуемые боковые входы в строение (т. е. проверка того, что они всегда заперты);

e) грузовые лифты (т. е. проверка того, что они защищены посредством карточки доступа или других средств контроля безопасности, в том числе отключение во внерабочее время).

В.4.4 Физическое наблюдение за безопасностью

Должно быть установлено физическое наблюдение за безопасностью, чтобы осуществлять мониторинг перемещения персонала внутри и вокруг помещений провайдера услуг. Наблюдение за безопасностью должно быть установлено с использованием сочетания оборудования (такого, как замкнутая телевизионная система и детекторы движения) и охраны; оно должно действовать постоянно и быть полностью управляемым.

Должны быть разработаны процедуры для установки, технического обслуживания, ремонта и модернизации оборудования для физического наблюдения за безопасностью, чтобы гарантировать отсутствие упущений в обеспечении безопасности. Например, может быть поставлена охрана для наблюдения за затрагиваемыми площадками/помещениями во время этих мероприятий.

Персонал, отвечающий за физическое наблюдение за безопасностью, должен быть адекватным образом обучен и периодически подвергаться тестированию для проверки реагирования на физическое вторжение и нападение. Требования к обучению и взаимосвязанные критерии оценки приведены в *А.9 (приложение А)*.

Физические зоны, которые должны находиться под наблюдением, должны по возможности включать:

a) все входы в помещения провайдера услуг и выходы из них;

b) все входы в помещения с ограниченным доступом, например в машинный зал и хранилище носителей данных, и выходы из них;

c) зоны, непосредственно окружающие периметр помещений провайдера услуг;

d) заборы по периметру и (или) стены помещений провайдера услуг;

e) зоны между заборами по периметру и (или) стенами и сооружениями в пределах помещений провайдера услуг.

Провайдеры услуг могут привлекать внешние ресурсы (внешних поставщиков) для обеспечения физического наблюдения за безопасностью, например обеспечения безопасности и мониторинга, но с учетом рекомендаций, представленных в *А.6 (приложение А)*.

В.4.5 Системы обнаружения и сигнализации

В.4.5.1 Общая информация

Должны быть установлены системы физического обнаружения и сигнализации для обнаружения вторжений и нападений, а также, например, возгорания и затопления и обеспечения раннего предупреждения соответствующего персонала об их возникновении. Системы обнаружения и сигнализации должны соответствовать требованиям приведенных ниже пунктов.

В.4.5.2 Конструкция

Системы обнаружения и сигнализации должны быть реализованы путем использования одного из следующих подходов:

a) централизованного — все устройства обнаружения подключены к централизованному оборудованию, которое управляется 24 часа в сутки;

b) децентрализованного — все устройства обнаружения функционируют и управляются локально;

c) комбинированного — комбинация централизованного и децентрализованного подходов (например, использование централизованного оборудования для мониторинга сигналов тревоги в помещениях с ограниченным доступом и местного управления другой сигнализацией).

В идеале все сигнальные устройства должны быть также связаны с местными органами охраны правопорядка и пожарной службой.

В.4.5.3 Виды предупреждений

Системы обнаружения и сигнализации должны по возможности предупреждать по крайней мере о следующих угрозах:

a) задымление;

b) возгорание;

c) протечка воды;

d) вторжение.

В.4.5.4 Охватываемые помещения

Системами обнаружения и сигнализации должны быть охвачены зоны ограниченного доступа, на площадках/помещениях, вмещающих оборудование с ограниченным доступом, должны быть установлены соответствующие виды устройств обнаружения и сигнализации.

Помещения с ограниченным доступом должны включать:

a) серверные;

b) другие машинные залы;

c) помещения с архивами носителей данных;

d) помещения с оборудованием для контроля влияния внешней среды (вмещающие оборудование для кондиционирования);

e) помещения с основными коммутаторами связи;

f) помещения с системой бесперебойного питания;

g) аккумуляторные (если они не соединены с помещениями с системой бесперебойного питания);

h) помещения с силовым трансформатором или генераторной установкой;

i) помещение с главным распределительным щитом или для конференц-связи;

j) другие телекоммуникационные помещения (например, вмещающие распределительные коробки для проводки и штепсельных соединений).

В.4.6 Операции

Персонал провайдера услуг должен быть адекватным образом обучен и периодически проходить тестирование для проверки реагирования на предупреждения систем обнаружения и сигнализации. Критерии оценки реагирования персонала описаны в *А.7.5.2*, а информация об обучении, образовании и тестировании персонала приведена в *А.9 (приложение А)*.

В.4.7 Хранилища

Провайдеры услуг должны быть способны предоставлять организациям безопасные хранилища и принадлежности для хранения их важнейших записей, магнитных носителей и ресурсов. Для обеспечения безопасных условий хранения необходимо соблюдать:

a) установленную формальную совокупность процедур для управления и обеспечения безопасности сбора, транспортировки, приема, маркировки, хранения и извлечения важнейших записей, магнитных носителей и ресурсов — в помещения организаций и из них, во внутренние и внешние хранилища и на площадки для восстановления. Например, отправляемые магнитные ленты важнейших записей можно хранить в защищенном шкафу в экспедиции перед сбором и доставкой организациям;

b) наличие соответствующих средств контроля влияния внешней среды, чтобы поддерживать целостность записей организации во время транспортировки и хранения;

c) для хранилищ, не расположенных на площадках для восстановления:

- критерии выбора мест для хранилищ должны быть такими же, как для выбора местоположения площадок для восстановления. Например, хранилища необходимо размещать вдали от мест с опасностями природного характера, к ним должны быть простой доступ и альтернативные маршруты доступа;

- хранилищам следует обеспечивать такой же уровень физического контроля доступа и защиты от влияния внешней среды, как для площадок для восстановления;

d) доступность на площадках для восстановления безопасных шкафов с возможностью запирания для хранения важнейших записей, магнитных носителей и ресурсов организации.

Провайдеры услуг могут привлекать внешние ресурсы (внешних поставщиков) для обеспечения хранилищ, но с учетом принципов, представленных в *А.6 (приложение А)*.

В.4.8 Идентификационные карточки

Должна существовать определенная форма видимой идентификации по идентификационным карточкам в целях мониторинга и контроля перемещения персонала в помещениях провайдера услуг со следующими требованиями:

a) каждая идентификационная карточка должна уникальным образом идентифицировать данного человека;

b) идентификационные карточки должны быть такими, чтобы было затруднительно сделать их дубликаты или подделать их;

c) каждому человеку единовременно должна выдаваться только одна идентификационная карточка;

d) каждый человек должен отвечать за обеспечение безопасности и надлежащее использование выданной идентификационной карточки;

e) о потере идентификационной карточки следует немедленно сообщать;

f) при нахождении в помещениях провайдера услуг идентификационную карточку следует все время носить на видном месте;

g) идентификационные карточки персонала должны заметно отличаться от идентификационных карточек, выдаваемых посетителям;

h) идентификационные карточки, выдаваемые посетителям, должны быть возвращены, когда данные лица покидают помещения провайдера услуг;

i) идентификационные карточки должны быть возвращены в последний рабочий день членов персонала (это часть процедур обеспечения безопасности при завершении работы).

В.4.9 Ключи

Должно существовать централизованное управление всеми ключами (включая карты с магнитным кодом, смарт-карты и коды цифровой клавишной панели), дающими возможность физического доступа к строениям площадки для восстановления и зонам/помещениям, а также, например, к шкафам внутри них.

Менеджмент ключей должен определять следующие политики и процедуры:

a) обычный контроль за выдачей ключей персоналу, например выдача ключей новому персоналу и возврат ключей при увольнении;

b) особый контроль за выдачей ключей персоналу для важнейших помещений (например, выдача ключей для прохода в серверные должна строго ограничиваться только несколькими основными членами персонала);

c) хранение запасных ключей (например, в специально контролируемой коробке или шкафчике для ключей);

d) действия при потере ключей (например, обязательная замена соответствующих замков и выдача новых ключей).

В.4.10 Легковоспламеняющиеся материалы

Легковоспламеняющиеся материалы, такие, как топливо для зажигалок, недопустимо хранить в помещениях, вмещающих оборудование с ограниченным доступом.

В.4.11 Портативное оборудование

Портативное оборудование, такое, как ноутбуки, мобильные телефоны, персональные цифровые секретари, USB-накопители или другие портативные жесткие диски, нельзя приносить в зоны/помещения, вмещающие чувствительную аппаратуру, если только это портативное оборудование не находится под контролем уполномоченного персонала провайдера услуг и (или) организации. Вопрос о таком контроле может решаться в каждом конкретном случае.

В.4.12 Карты и справочники

Карты помещений, телефонные справочники и другие документы, которые могут вызвать ассоциацию или позволят идентифицировать помещения для обработки значимой информации, необходимо предоставлять только соответствующему уполномоченному персоналу.

В.4.13 Инспектирование поступающих и исходящих материалов

Все поступающие и исходящие материалы для помещений провайдера услуг необходимо инспектировать на предмет потенциальных опасностей и инцидентов безопасности.

В.4.14 Устранение носителей данных и документов

Провайдеры услуг должны предоставлять организациям на площадках для восстановления соответствующее оборудование и средства для устранения ненужных документов, носителей данных и других материалов. Примеры такого оборудования: бумагорезательные машины, которые могут обеспечивать надежное уничтоже-

ние ненужных распечаток; оборудование, обеспечивающее размагничивание магнитных лент; оборудование для измельчения (поперечной нарезки) компакт-дисков. Устранение следует производить таким образом, чтобы не могло быть сделано никаких выводов в отношении ранее хранившихся данных.

В.4.15 Обеспечение непрерывности

Все реализованные меры и процедуры физической безопасности должны действовать 24 часа в сутки и 365 дней в году.

В.4.16 Здоровье и безопасность персонала

Должны существовать процедуры для обеспечения соответствующего уровня безопасности и охраны здоровья персонала на площадках для восстановления. Это включает периодическое инспектирование надежности строения и пожаробезопасности, охватывающее такие сферы, как вентиляция, снижение возможности возгорания, незаблокированность маршрутов эвакуации и аварийное освещение.

В.5 Специально выделенные зоны

В.5.1 Общая информация

Должны быть приняты меры, чтобы оставить конкретные зоны/помещения в зданиях провайдера услуг для размещения оборудования организации и использования во время восстановления. Эти зоны/помещения нельзя использовать в иных целях в обычное время. Если зону/помещение используют в иных целях во время обычных операций, у провайдера услуг должен быть предусмотрен процесс немедленной трансформации/использования ее для целей, необходимых во время *ЧС* или аварии.

В.5.2 Территория для собраний

Провайдеры услуг должны предоставлять адекватные территории для собраний с системой громкой связи, чтобы дать возможность организациям собирать и инструктировать весь свой персонал, занятый восстановлением. Территории для собраний могут быть открытыми пространствами, залами или аудиториями, которые должны:

a) вместить ожидаемое большое количество членов персонала, занятого восстановлением, из различных групп по восстановлению;

b) быть действующими и удобными для персонала при любых погодных условиях;

c) отвечать требованиям конфиденциальности организаций, чтобы любой проводимый там инструктаж или беседу нельзя было подслушать в соседних помещениях.

В.5.3 Зоны *(временного)* хранения

Провайдеры услуг должны предоставить зоны *(временного)* хранения для погрузки, разгрузки и инспектирования компьютерного и взаимосвязанного оборудования организации.

Провайдеры услуг должны установить политики и процедуры для регулирования перемещения оборудования организации в зоны *(временного)* хранения, включая присутствие и надзор представителей организации и провайдера услуг при необходимости и процедуры для рассмотрения вопросов нарушений норм и исключительных ситуаций.

В.5.4 Наладочная зона

Провайдеры услуг должны предоставить наладочные зоны с адекватным энергоснабжением для тестирования компьютерного и взаимосвязанного оборудования. Энергоснабжение в наладочной зоне должно быть изолировано от энергоснабжения других частей помещений для восстановления, чтобы предотвратить влияние случайного отключения на энергоснабжение в других частях помещений для восстановления во время тестирования оборудования. Следует также уделить внимание изолированию сети в наладочной зоне, если там необходимо тестировать использование сети.

Провайдеры услуг должны установить политики и процедуры для регулирования перемещения и тестирования оборудования организации в наладочной зоне, включая присутствие и надзор представителей организации и провайдера услуг при необходимости и процедуры для рассмотрения вопросов нарушений норм и исключительных ситуаций.

В.5.5 Другие зоны

Провайдерами услуг должны быть приняты меры, чтобы дать возможность организациям размещать свое вычислительное и взаимосвязанное оборудование в защищенной среде, т. е. предотвращать несанкционированные физический доступ, изменение или удаление. Например, могут быть оставлены зоны/помещения для принтеров и факсов и защищенные шкафы для маршрутизаторов и модемов.

В.6 Средства контроля влияния внешней среды

В.6.1 Общая информация

Провайдеры услуг должны обеспечить существование политик и процедур для обеспечения защиты электронных информационных систем, оборудования и мощностей провайдера услуг и организаций от опасностей природного характера и (или) опасностей вредного воздействия внешней среды. Эти политики и процедуры должны охватывать разработку и предоставление организациям средств подходящей конструкции и принадлежностей для предотвращения ухудшения состояния носителей, используемых для хранения. Например, в помещении для хранения магнитных носителей данных необходимо средствами управления поддерживать надлежащие температуру и влажность

В.6.2 Персонал и оборудование

Должны существовать процедуры для достижения соответствующего уровня качества внешней среды для оборудования и персонала на площадках для восстановления. Эти процедуры должны обеспечивать средства контроля влияния внешней среды для:

a) температуры;

b) вентиляции;

c) влажности;

d) вибрации и шума.

Должны быть также установлены процедуры для обеспечения соответствующего мониторинга и контроля напряженности электромагнитного поля по возможности.

В.6.3 Помещения

Провайдеры услуг должны обеспечить, чтобы средства контроля влияния внешней среды были предоставлены для следующих помещений:

a) серверные;

b) другие машинные залы;

c) с архивами носителей данных;

d) с оборудованием для контроля влияния внешней среды (вмещающие оборудование для кондиционирования);

e) с основными коммутаторами связи;

f) с системой бесперебойного электропитания;

g) аккумуляторные (если они не соединены с помещениями с системой бесперебойного электропитания);

h) с силовым трансформатором или генераторной установкой;

i) с главным распределительным щитом или для конференц-связи;

j) другие телекоммуникационные помещения (например, вмещающие распределительные коробки для проводки и штепсельных соединений).

В.6.4 Избыточность

Провайдеры услуг должны обеспечивать, чтобы все оборудование, обеспечивающее контроль влияния внешней среды, устанавливалось с дополнительной избыточностью, чтобы быть приспособленным к техническому обслуживанию и (или) сбою и предотвращать неблагоприятное влияние на уровни обслуживания. Например, должны быть установлены дополнительные агрегаты для кондиционирования воздуха в целях дублирования во время технического обслуживания основной системы кондиционирования воздуха.

В.7 Телекоммуникации

В.7.1 Общая информация

Телекоммуникации обеспечивают необходимую связь между площадками для восстановления и внешним миром. Всю информацию (голосовая, данные и, возможно, видео) необходимо передавать своевременным, эффективным и продуктивным образом, а вся передача с площадок для восстановления и на них должна осуществляться без нарушений или ухудшения качества и без перехвата информации.

Приведенные ниже рекомендации относятся к линиям связи от точки физического входа в помещения провайдера услуг до стоек физического оборудования. (Линии связи вне помещений провайдера услуг и находящиеся под контролем поставщиков телекоммуникационных услуг не рассматриваются в настоящем стандарте.)

В.7.2 Поставщики

У провайдеров услуг должны существовать процедуры и ресурсы для содействия организациям в обсуждении условий и привлечении любых поставщиков телекоммуникационных услуг для соответствия минимальным стандартам избыточности, надежности, безопасности и качества.

В.7.3 Отказ телекоммуникаций вследствие отказа одного элемента

Провайдеры услуг должны обеспечить, чтобы отказ телекоммуникаций вследствие отказа одного элемента был сведен к минимуму посредством наличия альтернативных источников телекоммуникаций, что позволит осуществлять переключение в случае аварии. Любой альтернативный источник должен быть независимой, иной и не находящейся в коллективном использовании совокупностью телекоммуникационного оборудования и линий связи на площадке для восстановления провайдера услуг. Таким образом, провайдеры услуг должны обеспечить, чтобы не происходило отказа системы вследствие отказа одного элемента для сетевого оборудования и линий связи, входящих/выходящих с их площадок, и чтобы существовали альтернативные сетевые соединения, позволяющие осуществлять переключение в случае аварии, что может быть достигнуто посредством:

a) сетевого разнообразия;

b) разнообразия провайдеров телекоммуникационных услуг, которое может быть достигнуто либо путем предоставления линии связи с другим провайдером сетевых услуг, либо путем демонстрирования способности подключения к другому узлу, зданию или помещению, где есть по крайней мере еще один провайдер сетевых услуг.

В.7.4 Защита

Провайдеры услуг должны обеспечить, чтобы вся телекоммуникационная кабельная система, поддерживающая информационные и (или) голосовые и видеоуслуги в их помещениях, была защищена от вмешательства, перехвата или повреждения, включая обеспечение этого посредством:

a) разделения силовых и телекоммуникационных кабелей для предотвращения помех и возможного повреждения;

b) отделения телекоммуникационной кабельной системы с волоконно-оптическими кабелями от других кабелей;

c) избегания прокладки кабелей через общедоступные помещения, чтобы минимизировать возможность прослушивания;

d) обеспечения кабельных каналов и (или) кабельных лотков с соответствующей прочностью материала, чтобы защитить проходящие внутри кабели от физического повреждения.

(См. также *B.9.2.*)

B.7.5 Связность и пропускная способность

Провайдеры услуг должны обеспечить наличие линий связи с достаточной пропускной способностью и связностью, чтобы дать возможность организациям осуществлять международную связь и связь с основными поставщиками информационных услуг и информационной поддержки без излишних ограничений и задержки передачи.

B.7.6 Мобильная связь

Провайдеры услуг должны обеспечить, чтобы при нахождении членов персонала организации в их помещениях они имели возможность связаться с внешними сторонами, находящимися вне данных помещений, используя свои мобильные телефоны в заранее предназначенных для этого местах. Например, провайдеры услуг могут заключить соглашения с поставщиками, предоставляющими телекоммуникационные услуги, или владельцами участков/строений, вмещающих площадки для восстановления, в целях улучшения приема мобильной связи. Могут быть также заключены аналогичные соглашения по использованию технологии беспроводной сети в помещениях провайдера услуг.

Провайдеры услуг должны также обеспечить разнообразие поставщиков услуг сотовой связи, чтобы не зависеть от единственного поставщика.

Все аспекты, касающиеся мобильной связи, должны быть предметом договорных соглашений между провайдерами услуг и организациями.

B.8 Энергоснабжение

B.8.1 Общая информация

Все вычислительное оборудование зависит от постоянного и стабильного источника электропитания для выполнения обычных операций, а прерывание или нарушение энергоснабжения может привести к потере важной информации или затруднению работ по восстановлению. Поэтому провайдеры услуг должны обеспечить введение политик и процедур, способствующих обеспечению постоянной доступности адекватной подачи электроэнергии.

Приведенные ниже принципы относятся к линиям энергоснабжения от точки физического входа в помещения провайдера услуг до стоек физического оборудования. (Линии энергоснабжения вне площадок провайдера услуг и находящиеся под контролем поставщиков электроэнергии не рассматриваются в настоящем стандарте.)

B.8.2 Поставщики электроэнергии

Провайдеры услуг должны обеспечить наличие процедур, гарантирующих, что электроснабжение, предоставляемое поставщиками, отвечает минимальным стандартам избыточности, надежности, безопасности и качества, включая процедуры мониторинга поступающего электроснабжения и разрешения нерешенных проблем с поставщиками, если таковые возникают.

B.8.3 Отказ энергоснабжения вследствие отказа одного элемента

Провайдеры услуг должны обеспечить, чтобы отказ энергоснабжения вследствие отказа одного элемента был сведен к минимуму благодаря наличию альтернативных источников электропитания, что позволит осуществлять переключение в случае сбоя, включая:

a) генераторы (см. *B.8.5.2*);

b) средства и оборудование для источников бесперебойного питания (см. *B.8.5.3*).

Кроме того, по возможности у провайдеров услуг должно быть поступающее на площадки для восстановления энергоснабжение от независимых, иных и не находящихся в коллективном использовании мощностей и линий энергоснабжения, например энергоснабжение от других подстанций.

B.8.4 Защита

Провайдеры услуг должны создать процедуры и установить необходимое оборудование, чтобы изолировать и обеспечить защиту всего работающего в их помещениях оборудования организаций и собственного оборудования от повреждения из-за увеличения и (или) скачков напряжения, грозовых разрядов или других непредвиденных обстоятельств. Виды нарушений энергоснабжения, от которых необходима защита, включают:

a) полный отказ («затемнение»);

b) резкое снижение напряжения («частичное затемнение»);

c) выбросы;

d) скачки напряжения.

Кроме того, адекватное внимание следует уделить потенциальным электрическим помехам и их влиянию на чувствительное оборудование.

В.8.5 Альтернативное энергоснабжение

В.8.5.1 Общая информация

Провайдеры услуг должны обеспечить наличие альтернативного энергоснабжения, которое может быть использовано на площадках для восстановления на врéменной основе (в случае нарушения обычного энергоснабжения) и способно удовлетворять все потребности организаций, связанные с восстановлением, пока не будет возобновлено нормальное энергоснабжение.

В.8.5.2 Генераторы

Провайдеры услуг должны предоставить и установить необходимое число генераторов, выполняющих роль резерва, используемого для предупреждения влияния серьезных нарушений энергоснабжения на операции по восстановлению. Приобретаемые генераторы должны удовлетворять требованиям мощности и минимальным стандартам безопасности, надежности и качества.

Генераторы мощности следует размещать там, где они не смогут помешать операциям на площадках для восстановления или не будут представлять никакую операционную опасность или нарушение безопасности (например, из-за зашумленности, воспламенения или взрыва).

Топливные баки генераторов должны быть размещены так, чтобы минимизировать риски (например, вредительства или возгорания), предпочтительно ниже уровня земли, с количеством хранимого топлива, поддерживаемым на таком уровне, чтобы сделать возможным доступность резервного энергоснабжения в течение периода, не меньше оговоренного времени выполнения поставки топлива, которое определено в договоре с поставщиком. Должны быть приняты меры для немедленного пополнения топлива после использования в случае *ЧС* или аварии. Качество топлива необходимо регулярно тестировать в компетентных лабораториях.

Генераторы мощности необходимо регулярно тестировать путем включения и использования, чтобы гарантировать поддержание резервного уровня готовности. Тестирование генераторов необходимо осуществлять в соответствии с процедурами и спецификациями производителей.

В.8.5.3 Источники бесперебойного питания

Провайдеры услуг должны приобретать, устанавливать и поддерживать необходимые блоки источников бесперебойного питания, чтобы дать возможность эксплуатировать и упорядоченным образом отключать критические для целевой задачи организации сети и вычислительное оборудование.

Для критических сетей и вычислительного оборудования, требующих высокой доступности, следует использовать источники бесперебойного питания класса VFI (без времени переключения), которые электроэнергию подают непрерывно.

Все источники бесперебойного питания должны проходить техническое обслуживание и регулярно тестироваться в соответствии с процедурами и спецификациями производителей, чтобы гарантировать операционную готовность источников бесперебойного питания к поддержке систем организации во время *ЧС* или аварии.

Поскольку все источники бесперебойного питания имеют внутренний потенциальный источник опасности, они должны быть отделены от критических сетей и вычислительного оборудования, требующих высокой доступности, или размещены на безопасном расстоянии от них.

Все аккумуляторные батареи, используемые в резервных блоках питания, должны проходить техническое обслуживание, тестироваться и (или) периодически заменяться, например, ежегодно в соответствии со спецификациями производителей.

В.8.5.4 Безопасное переключение

Провайдеры услуг должны установить процедуры и средства для обеспечения того, чтобы переключение с обычных источников электроэнергии на генераторы мощности во время нарушений энергоснабжения осуществлялось безопасным образом и не влияло на обычные операции. Процедуры и средства должны также обеспечивать безопасное переключение на обычные источники энергоснабжения при их восстановлении.

В.8.5.5 Уведомление о переключении

Провайдеры услуг должны обеспечить, чтобы любое переключение с обычного источника электроэнергии на альтернативный источник было обнаружено с последующим уведомлением соответствующего персонала для мониторинга и действий.

В.8.6 Аварийные автоматические выключатели

Если это требуется организациям, провайдеры услуг должны обеспечить установку аварийных автоматических выключателей в обозначенных организацией помещениях, где есть потенциальная опасность возгорания из-за тепла, выделяемого электрическими устройствами. Ситуации *ЧС*/аварии могут возникать, если подача электроэнергии будет способствовать интенсификации и (или) стимулированию распространения возгорания внутри соответствующих площадок/помещений. Аварийные автоматические выключатели должны быть:

a) установлены в зонах/помещениях с оборудованием, потребляющим большое количество электроэнергии (например, трехфазные электрические устройства);

b) установлены рядом с входными дверьми (либо внутри, либо снаружи) в зоны/помещения, полностью предназначенные для организации;

c) установлены вблизи обозначенных организацией индивидуальных участков для зон/помещений, коллективно используемых организациями;

d) защищены кожухами, предохраняющими от случайной активации;

e) способны вызывать отключение всего энергоснабжения, включая источники бесперебойного питания, в зонах/помещениях во время аварийной ситуации.

Инструкции по приведению в действие аварийных автоматических выключателей должны быть размещены на видном месте.

B.9 Менеджмент кабельной системы

B.9.1 Общая информация

Поскольку кабели необходимы для передачи электроэнергии, а также электронной информации, провайдеры услуг должны обеспечить принятие мер для их защиты от внешнего повреждения и вмешательства. Эти меры должны включать грамотное проектирование, тщательное размещение, создание и поддержку качественной документации (например, чертежей и методик) и техническое обслуживание установленной системы. При проектировании следует учитывать текущие и будущие запланированные мощности, простоту размещения и технического обслуживания.

B.9.2 Защита

Провайдеры услуг должны установить процедуры и средства для изолирования и обеспечения защиты всей кабельной системы, включая следующие:

a) телекоммуникационные и силовые кабели должны быть изолированы друг от друга, чтобы предотвратить помехи, например, путем использования отдельных шахтных стволов или применения соответствующего экранирования;

b) кабели, проходящие через зоны/помещения, которые посещаются публикой или не могут охраняться, должны быть защищены посредством, например, скрытого монтажа линий, кабельных каналов и (или) кабельных лотков с соответствующей прочностью материалов для защиты линий от физического повреждения, проводки линий в механически прочных и запираемых шахтах и запирания распределительных коробок;

c) кабели необходимо выбрать на основе требований к передаче и внешней среды. Например, свободные от растяжения кабели следует использовать для воздушных линий и при большой величине уклона (хотя использование воздушных кабелей не рекомендуется), сохраняющие функции кабели необходимо использовать в помещениях, подверженных тепловой опасности и опасности возгорания, экранированные кабели необходимо использовать для помещений с сильными электрическими и наведенными помехами, армированные кабели должны быть использованы в ситуациях, где достаточная механическая защита не может быть обеспечена никаким другим образом (например, при вре́менном размещении на полу или стенах);

d) вся кабельная система, кабельные лотки и шахты необходимо периодически проверять на предмет повреждения, несанкционированной модификации, прослушивания или других сфер потенциального риска. Например, реконструкция или изменение использования площадки могут привести к тому, что экранированные кабели могут случайно подвергнуться внешнему воздействию.

(См. также *B.7.4*.)

B.9.3 Планы прокладки

Провайдеры услуг должны обеспечить поддержание точных и актуальных планов расположения всей кабельной системы. Такие планы обеспечивают полезную информацию для размещения, технического обслуживания, отыскания повреждений и ремонта кабельной системы, а также помогают идентифицировать места потенциальной опасности.

Индивидуальные подробные планы прокладки должны быть предусмотрены для каждой из следующих кабельных систем:

a) телекоммуникации/сети (данные);

b) телекоммуникации/сети (голос);

c) телекоммуникации/сети (данные/голос/видео, например сведение их в один поток);

d) энергоснабжение.

Провайдеры услуг должны также обеспечить создание и поддержку общих планов прокладки кабельной системы, содержащих следующие подробности:

a) физическая прокладка через различные части площадок для восстановления (например, местоположение любых кабельных лотков и межэтажных шахт);

b) общие виды кабелей (например, с разграничением силовых и телекоммуникационных кабелей);

c) маркировки при необходимости для идентификации использования конкретных кабелей (например, для групп сетевых пользователей).

B.10 Противопожарная защита

B.10.1 Общая информация

Провайдеры услуг должны обеспечить наличие соответствующих систем обнаружения и ликвидации пожара для защиты вычислительного оборудования и персонала, работающего на площадках для восстановления. Мощность этих систем должна быть пропорциональна размеру площадки/помещения и степени необходимой защиты.

Приведенные ниже пункты содержат необходимые рекомендации для систем обнаружения и ликвидации пожара и обеспечения безопасности персонала на площадках для восстановления.

В.10.2 Нормативное соответствие

Провайдеры услуг должны обеспечить соблюдение существующих предписаний и требований в отношении пожаробезопасности и техники безопасности, устанавливаемых инспекцией, осуществляющей строительный надзор, и (или) другими уполномоченными органами.

В.10.3 Служащий, отвечающий за противопожарную защиту

Провайдеры услуг должны обеспечить назначение конкретных членов персонала для осуществления надзора за соблюдением предписаний, касающихся пожаробезопасности и техники безопасности. Эти члены персонала могут быть служащими, отвечающими за противопожарную защиту, или другими лицами, прошедшими адекватное обучение правилам техники безопасности и пожаробезопасности. Должны быть также назначены заместители, которые должны быть достаточно компетентными для выполнения обязанностей ответственных лиц в случае, когда основные назначенные лица недоступны или иным образом неспособны выполнять работу.

В.10.4 Пожарные выходы

Провайдеры услуг должны обеспечить наличие пожарных выходов и проинформировать о них весь персонал.

Пожарные выходы должны:

a) быть ясно помечены знаками выхода, которые светятся, например, во время отключения электричества и во время пожара;

b) быть незагроможденными в любое время (например, объемные предметы нельзя размещать вдоль пожарных выходов, препятствуя или задерживая движение по проходам).

Несмотря на то что по причинам безопасности двери пожарных выходов не должны открываться снаружи, они не должны быть заперты изнутри.

Весь персонал организации по прибытии на площадки для восстановления должен быть проинструктирован о пожарных выходах в ходе тестирования плана восстановления после *ЧС* или его активации в случае *ЧС* или аварии.

В.10.5 План реагирования на возгорание

Провайдеры услуг должны обеспечить, чтобы были установлены планы и процедуры для принятия мер при появлении возгорания и задымления, которые включают:

a) процедуры, которые должны быть приняты для различных ситуаций возгорания и задымления;

b) планы эвакуации людей, расположенных в различных частях площадок для восстановления;

c) помещения для инструктирования персонала;

d) подробности для уведомления аварийных служб;

e) цепочку связи и управления;

f) процедуры, регламентирующие исправление недостатков, обнаруженных при пожарных учениях, и требования к персоналу, не соблюдающему правила.

Необходимо проводить периодические эвакуационные учения на случай пожара для тестирования различных аспектов этих планов/процедур реагирования на возгорание/задымление.

Точки подачи воды для пожаротушения должны быть ясно помечены, чтобы они могли быть быстро обнаружены во время пожара, и, если этого требуют местные предписания, копии планов зданий с указанием точек подачи воды должны быть переданы на хранение местным аварийным службам.

В.10.6 Ручные огнетушители

Провайдеры услуг должны обеспечить, чтобы:

a) ручные огнетушители были размещены в зонах/помещениях, требующих защиты (например, в серверной и других машинных залах);

b) персонал и подрядчики, находящиеся на площадке по долгосрочным договорам, были проинструктированы по использованию ручных огнетушителей с демонстрацией и практическим применением при необходимости;

c) размещение ручных огнетушителей позволяло легко их достать, снять и активировать для использования во время пожара;

d) в помещениях, содержащих оборудование, которое будет повреждено в случае тушения возгорания водой, были использованы соответствующие виды огнетушителей, например углекислотные огнетушители;

e) огнетушители были хорошо видны или были бы указатели, где их можно найти;

f) условия хранения и эксплуатации огнетушителей отвечали требованиям спецификаций производителей и нормативной технической документации.

В.10.7 Безопасность персонала

Поскольку используемый в некоторых системах обнаружения и ликвидации возгорания подавляющий кислород/гасящий газ не только приводит к гашению пламени, но также может вызывать удушье у людей, провайдеры услуг должны серьезно подойти к рассмотрению применения систем, использующих газы, которые не вредны для здоровья, особенно для зон/помещений с большим количеством людей. Если системы, использующие не вредные для здоровья газы, установить невозможно, то персонал, работающий в зонах/помещениях, где установлены системы, использующие гасящий газ или газ, подавляющий кислород, должен быть подробно проинструктирован перед началом работы в таких зонах/помещениях о необходимости очень быстро покинуть помещение, когда система обнаружения и ликвидации возгорания активируется, и о пожарных выходах. Должны быть разработаны соответствующие предупреждающие плакаты, которые должны быть вывешены на видных местах.

В.11 Центр работы в чрезвычайных ситуациях

В.11.1 Общая информация

Провайдеры услуг должны предоставить на своих площадках для восстановления центры работы в чрезвычайных ситуациях, соответствующим образом оборудованные, чтобы дать возможность организациям осуществлять надзор и поддерживать связь со своими деловыми подразделениями и внешними сторонами во время ЧС или аварии. (В контексте настоящего стандарта приведенные ниже пункты не относятся к центрам работы в чрезвычайных ситуациях, создаваемых организациями на других площадках, не имеющих отношение к провайдеру услуг.)

В.11.2 Оборудование и принадлежности

Провайдеры услуг должны предоставить основное оборудование и принадлежности, чтобы дать возможность организациям привести в действие свои центры работы в чрезвычайных ситуациях, включая:

a) телекоммуникационное оборудование, например выделенные телефонные линии, телефоны, факсы;

b) офисное оборудование, например персональные компьютеры, принтеры, бумагорезательные машины и фотокопировальные устройства;

c) канцелярские принадлежности (например, ручки, карандаши, маркеры, карманные фонари с запасными батарейками, ножницы, бумагу для печати).

В.11.3 Специализированные помещения

В.11.3.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы в центрах работы в чрезвычайных ситуациях имелись специализированные помещения и соответствующее оборудование с зонами/помещениями, удовлетворяющими требованиям, описанным в *В.11.3.2 — В.11.3.4*.

В.11.3.2 Помещение для связи

Провайдеры услуг должны обеспечить предоставление зон/помещений, способствующих проведению переговоров по телефону, которые должны быть:

a) оборудованы соответствующим числом выделенных телефонных линий (для входящих и исходящих звонков) для использования организацией;

b) оборудованы для приема внешних новостей (например, телевизорами для просмотра местных, и при необходимости национальных и зарубежных новостей);

c) свободны от шумовых помех от других источников (например, шума, создаваемого принтерами).

В.11.3.3 Зоны/помещения для собраний

Провайдеры услуг должны обеспечить предоставление зон/помещений для проведения собраний и обсуждений персоналом организации, которые должны быть:

a) достаточно большими, чтобы с удобством вмещать необходимое максимальное число членов персонала организации (например, руководителей групп по восстановлению);

b) оборудованы статусными табло для мониторинга и отслеживания продвижения восстановления (например, виртуальными досками и настенными презентационными планшетами);

c) соответствующим образом оборудованы для приема внешних новостей (например, телевизионной связью и телевизорами, если требуются телевизионные пресс-конференции).

В.11.3.4 Зоны/помещения для брифингов

Провайдеры услуг должны обеспечить предоставление зон/помещений для содействия общению с прессой и посторонними лицами, которые должны быть:

a) расположены в отдельных местах вдали от других помещений центра работы в чрезвычайных ситуациях, чтобы предотвратить несанкционированный доступ представителей прессы или посетителей к кадровой и конфиденциальной информации организации и площадкам для восстановления (например, находиться в другом месте за пределами основного периметра площадки для восстановления);

b) доступны только для приглашенных представителей прессы или посетителей, с контролем входа в зоны/помещения;

c) соответствующим образом оборудованы и обставлены для поддержки брифингов с представителями средств массовой информации (например, иметь достаточную площадь, чтобы вмещать ожидаемое количество представителей прессы, которые, вероятно, посетят связанные с ЧС/аварией брифинги).

В.11.4 Рабочее пространство для групп по восстановлению рабочей зоны

Провайдеры услуг должны обеспечить предоставление рабочего пространства для использования представителями различных групп по восстановлению, которое должно быть соответствующим образом оборудовано, чтобы поддерживать потребности организации (например, иметь телефонные линии, телефоны, факсы и соответствующие офисные принадлежности).

В.12 Помещения с ограниченным доступом

В.12.1 Общая информация

Провайдеры услуг должны обеспечить предоставление помещений, в которые разрешен только санкционированный доступ для предназначенных целей и которые имеют взаимосвязанные уровни защиты, включая:

a) серверные;

b) другие машинные залы;

c) помещения с архивами носителей данных;

d) помещения с оборудованием для контроля влияния внешней среды (вмещающие оборудование для кондиционирования);

e) помещения с основными коммутаторами связи;

f) помещения с системой бесперебойного электропитания;

g) аккумуляторные (если они не соединены с помещениями с системой бесперебойного электропитания);

h) помещения с силовым трансформатором или генераторной установкой;

i) помещение с главным распределительным щитом или для конференц-связи;

j) другие телекоммуникационные помещения (например, вмещающие распределительные коробки для проводки и штепсельных соединений).

B.12.2 Зоны/помещения, вмещающие основные компьютерные системы

B.12.2.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы зоны/помещения, вмещающие основное компьютерное оборудование, были спроектированы и построены таким образом, чтобы иметь дополнительный уровень безопасности по сравнению с обычными зонами/помещениями, и в соответствии с требованиями *B.12.2.2 — B.12.2.5.*

B.12.2.2 Физический доступ

Провайдеры услуг должны обеспечить надежную конструкцию дверей, открывающих доступ к зонам/помещениям с оборудованием ограниченного доступа и оснащенных высококачественными механизмами контроля доступа и надежными замками, а также надежные окна, как минимум, цокольного и первого этажа, из небьющегося стекла и при необходимости оснащенные жалюзями.

Постоянный мониторинг доступа обязателен.

B.12.2.3 Потенциальные опасности

Провайдеры услуг должны обеспечить наличие адекватной изоляции, защиту, предотвращение и устранение потенциальных источников разрушения из зон/помещений, вмещающих оборудование с ограниченным доступом, с принятием следующих мер:

a) избегание трасс водопроводных или газовых труб и кабелей в зданиях как сверху, так и снизу (например, водопроводные трубы не должны проходить через серверные);

b) включение соответствующей защиты при проектировании этих помещений (например, фальшпол, средства, предотвращающие протечку воды, детекторы протечки воды/жидкостей с автоматическими электромагнитными клапанами, системы огнетушения, не наносящие ущерб чувствительному оборудованию при их активации).

Провайдеры услуг должны также обеспечить, чтобы адекватное внимание было уделено защите от потенциальных электромагнитных помех от расположенных поблизости передающих устройств сотовой связи, трехфазных генераторов, трансформаторов, линий высокого напряжения, например посредством использования экранирования или сохранения безопасного расстояния от источников электромагнитных помех.

B.12.2.4 Энергоснабжение

Провайдеры услуг должны обеспечить для каждой зоны/помещения, вмещающих оборудование с ограниченным доступом, отдельное энергоснабжение, отделенное и изолированное от энергоснабжения остального строения. При этом должны быть:

a) предусмотрены отдельные распределительные щиты и соответствующие автоматические выключатели для этих зон/помещений;

b) надлежащим образом закрыты распределительные щиты.

B.12.2.5 Электрические соединения

Провайдеры услуг должны обеспечить периодические проверки электрических соединений от распределительных щитов до критических мощностей и оборудования, поскольку плохой контакт в электрических соединениях может генерировать тепло и, следовательно, представляет потенциальную опасность (например, посредством проведения периодического инфракрасного сканирования распределительных щитов).

B.12.3 Кондиционирование воздуха

Провайдеры услуг должны обеспечить, чтобы:

a) в зонах/помещениях, вмещающих оборудование с ограниченным доступом, проводили измерения температуры и влажности, чтобы проверять, работают ли системы кондиционирования воздуха в режиме, который требуется системам ИКТ и оборудованию, установленным в этих зонах/помещениях;

b) измерения проводились в разное время суток;

c) системы кондиционирования воздуха были:

1) способны поддерживать температуру и влажность помещения в пределах, требуемых системами ИКТ, находящимися в этих зонах/помещениях;

2) спроектированы таким образом, чтобы иметь возможность продолжать работу при поломке или техническом обслуживании отдельных блоков кондиционирования (например, посредством проектирования резервной мощности или дополнительных резервных блоков кондиционирования).

B.12.4 Возгорание и задымление

Тепло, дым и пары при возгорании могут представлять существенную угрозу для жизни людей и чувствительного вычислительного оборудования. Поэтому провайдеры услуг должны обеспечить, чтобы не только существовала противопожарная защита, непосредственно предоставляемая для чувствительного к теплу вычислительного оборудования, но также было установлено достаточное число противопожарных перегородок для предупрежде-

ния теплового излучения и распространения огня, дыма и паров. Следует отметить, что для различных частей площадок для восстановления могут потребоваться отдельные зоны противопожарной и противодымной защиты.

B.12.5 Здоровье и безопасность персонала

B.12.5.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы здоровье и безопасность персонала были приоритетными по отношению ко всем политикам и процедурам защиты помещений и оборудования ИКТ.

B.12.5.2 Вентиляция

Провайдеры услуг должны обеспечить вентилирование зон/помещений с постоянным нахождением персонала для обеспечения достаточного уровня свежего воздуха находящимся там людям, например с подсчетом воздухообмена в час в данной зоне/помещении на основе тепла, вырабатываемого оборудованием в помещении, и требуемого охлаждения.

B.12.5.3 Освещение

Провайдеры услуг должны обеспечить адекватное освещение для безопасных операций, осуществляемых персоналом в зонах/помещениях, вмещающих оборудование с ограниченным доступом, включая аварийное освещение, предназначенное для использования во время *ЧС*, например, если энергоснабжение отключено во время пожара.

B.12.5.4 Противопожарная система

Используемый в некоторых системах обнаружения и ликвидации возгорания подавляющий кислород/гасящий газ может представлять опасность для людей. Более подробно изложено в *B.10.7*.

B.12.5.5 Управляемые электричеством двери

Провайдеры услуг должны обеспечить, чтобы зоны/помещения, в которых двери запираются электричеством для контроля доступа персонала, могли быть открыты изнутри во время нарушения энергоснабжения или пожара в целях безопасного выхода персонала из этих зон/помещений. Например, изнутри должно быть ручное отключение электрического запирания дверей во время нарушения энергоснабжения или пожара, или двери должны быть сконструированы таким образом, чтобы оставаться открытыми во время таких ситуаций.

B.12.5.6 Система общественного оповещения

Провайдеры услуг должны обеспечить установку систем общественного оповещения или эквивалентных систем на площадках для восстановления, а также их регулярное тестирование. Это позволит делать голосовые объявления для всего персонала на площадке для восстановления. Например, при пожаре на площадке для восстановления система общественного оповещения может быть использована для оповещения персонала о необходимости покинуть площадку.

B.12.6 Системы сигнализации

Провайдеры услуг должны обеспечить установку соответствующих устройств обнаружения и сигнализации, которые предупреждают, как минимум, о задымлении, возгорании, протечке воды/жидкостей, физических вторжениях и могут быть слышны внутри и вне рассматриваемых зон/помещений.

B.12.7 Общие соображения относительно размещения

Провайдеры услуг должны обеспечить, чтобы зоны/помещения, вмещающие оборудование с ограниченным доступом, не имели никакой маркировки, касающейся их использования, чтобы способствовать защите конфиденциальности и усилению безопасности, например табличек с названиями организаций не должно быть на дверях абонируемых организациями помещений. Кроме того, зоны/помещения, вмещающие оборудование с ограниченным доступом, должны отвечать следующим требованиям:

a) размещение вдали от помещений общего доступа, таких, как приемные и туалеты, и наличие средств предупреждения доступа неуполномоченных лиц;

b) малозаметность извне периметра здания, что может быть достигнуто, например, посредством экранирования всех окон или отсутствием окон вообще;

c) наличие соответствующей защиты, такой, как предотвращающая протечку воды, детекторы протечки воды с автоматическими электромагнитными клапанами и система огнетушения, не наносящая ущерба оборудованию при ее активации;

d) использование стекла особой марки, которое нелегко разбить, либо оснащение системой обнаружения разбивания стекла, если эти зоны/помещения имеют стеклянные стены или окна, которые доступны извне здания;

e) максимально допустимая нагрузка для всех поддерживающих структур, особенно фальшполов и пандусов, должна быть спланирована с учетом соображений текущей и потенциальной будущей нагрузки;

f) размещение оборудования с учетом циркуляции горячего и холодного воздуха, чтобы исключить чрезмерную концентрацию тепла в определенных частях зон/помещений;

g) проект должен учитывать как текущие, так и будущие требования, например, с адекватным энергоснабжением и мощностями системы кондиционирования, покрывающими текущее и проектируемое будущее потребление.

B.12.8 Подлежащие исключению зоны

Провайдеры услуг должны обеспечить, чтобы зоны/помещения, вмещающие оборудование с ограниченным доступом, не размещались в перечисленных ниже местах, если присутствует любая из взаимосвязанных опасностей:

a) в подвальных помещениях, если они подвержены риску разрыва труб, протечки воды или затопления;

b) в помещениях, расположенных непосредственно под плоской крышей, если есть риск протечки во время дождя;

c) в помещениях цокольного этажа, если они развернуты в сторону зон общественного движения и подвержены риску атак, вандализма и форс-мажорных обстоятельств из-за дорожно-транспортных происшествий вблизи здания;

d) в помещениях, находящихся в непосредственной близости с другими зонами/помещениями (рядом, этажом выше или ниже), которые используют для обработки или хранения опасных веществ, таких, как легковоспламеняющиеся материалы, химические или взрывчатые вещества.

В.13 Не относящиеся к восстановлению удобства

В.13.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы в дополнение к предоставлению помещений и оборудования, делающих возможным фактическое восстановление, обеспечивались удобства, ориентированные на здоровье и благополучие персонала организации, размещенного в их помещениях во время восстановления.

В.13.2 Персонал

Провайдеры услуг должны обеспечить предоставление адекватных основных удобств, ориентированных на персонал организации, работающий в их помещениях во время восстановления, включая:

a) зоны отдыха;

b) туалеты;

c) питьевую воду;

d) трехразовое питание каждый день (с учетом договорных соглашений с организациями).

В.13.3 Автостоянка

В тех случаях, когда позволяют обстоятельства, провайдеры услуг должны обеспечить доступность для персонала организации, работающего в помещениях провайдера услуг во время восстановления, адекватных мест для стоянки автомобилей, а также при единоличном использовании помещений провайдером услуг — мониторинг и контроль этих мест для стоянки 24 часа в сутки и 365 дней в году.

В.13.4 Перевозка

Провайдеры услуг должны обеспечить доступность их площадок для восстановления персоналу организации 24 часа в сутки и 365 дней в году, например, посредством размещения площадок для восстановления вблизи остановок общественного транспорта и (или) — с учетом договорных соглашений с организациями — предоставления заказного транспорта, доставляющего персонал организации от выбранных остановок общественного транспорта до площадки для восстановления и обратно.

В.13.5 Лечение

Провайдеры услуг должны обеспечить возможность принятия мер для оказания первичной доврачебной помощи персоналу организации, который может работать с огромной рабочей и временной нагрузкой на площадках для восстановления во время восстановительных работ, например, посредством наличия в помещениях медицинских аптечек.

В.14 Жизненный цикл физических мощностей и вспомогательного оборудования

В.14.1 Общая информация

Посредством менеджмента жизненного цикла мощностей/оборудования провайдеры услуг должны обеспечить постоянное соответствие всех физических мощностей и вспомогательного оборудования предназначенным целям, чтобы гарантировать доступность для организаций абонированных услуг.

Провайдеры услуг должны учредить надлежащие программы по обслуживанию и уходу, охватывающие срок службы каждого элемента используемых мощностей и оборудования, жизненный цикл которых включает создание, установку, введение в строй, эксплуатацию, ремонт, техническое обслуживание, модернизацию и при необходимости замену физических мощностей и оборудования.

В.14.2 Политики и процедуры

Провайдеры услуг должны обеспечить установление политик и процедур для физических мощностей и оборудования, охватывающих установку, введение в строй, эксплуатацию, ремонт, техническое обслуживание, модернизацию и замену (например, политику, определяющую, что должны быть предприняты все попытки для ремонта оборудования на месте, прежде чем перевозить его на площадку поставщика).

В.14.3 Соответствие требованиям

Провайдеры услуг должны обеспечить полное соответствие всех физических мощностей и вспомогательного оборудования текущим рекомендациям производителей оборудования, профессиональным стандартам (практическим приемам) и (или) нормативным требованиям.

В.14.4 Квалифицированные специалисты

Провайдеры услуг должны обеспечить эксплуатацию всех физических мощностей и вспомогательного оборудования квалифицированными специалистами, например, чтобы монтаж и ввод в строй электроустановки высокого напряжения осуществляли квалифицированные инженеры-специалисты.

В.14.5 Ситуации, связанные с обслуживанием

Провайдеры услуг должны обеспечить установление политик и процедур для регулирования приведенных ниже ситуаций во время ремонта, технического обслуживания, модернизации и замены физических мощностей и оборудования:

a) на месте — поскольку во время технического обслуживания поставщиками может быть использовано дополнительное оборудование, должны быть приняты меры для обеспечения того, чтобы дополнительное оборудование не оказывало влияния на безопасность и работу оборудования и мощностей для восстановления. Во время технического обслуживания должно быть предпринято надлежащее изолирование оборудования, например с наличием соответствующих процедур для замены неисправного оборудования и установки нового оборудования;

b) вне места эксплуатации — хотя здесь существуют вопросы, сходные с техническим обслуживанием на месте, вследствие затруднений с непосредственным надзором за поставщиком должны быть приняты дополнительные меры. Например, если неисправный элемент оборудования должен быть возвращен на площадку поставщика для тщательного изучения, перед вводом отремонтированного элемента оборудования повторно в эксплуатацию должны быть предприняты дополнительные проверки и тестирование безопасности и функциональных возможностей;

c) недоступность — поскольку оборудование может быть недоступно во время технического обслуживания, должны быть предприняты соответствующие меры для обеспечения того, чтобы предлагаемые организациям услуги сохранить в полном объеме и ситуация оставалась бы под контролем в течение этого периода, например, посредством активации резервного или альтернативного запасного оборудования перед проведением технического обслуживания оборудования;

d) повторное подключение — оборудование, которое должно быть повторно введено в эксплуатацию после ремонта, технического обслуживания, модернизации или замены, должно быть проверено и протестировано, чтобы гарантировать, что оно установлено на правильный режим функционирования и интегрировано с соответствующими системами. Например, замененный датчик охранной сигнализации, подключенный к основной системе физической безопасности, должен быть вновь протестирован на связность.

B.14.6 Проверки

B.14.6.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы:

a) были установлены процедуры периодических аудиторских проверок каждого элемента физических мощностей и оборудования в их помещениях как часть аудитов физических мощностей и оборудования;

b) был назначен персонал (внутренний или внешний) с соответствующей квалификацией, обладающий полномочиями и обязанностями по проведению аудиторских проверок физических мощностей и оборудования.

B.14.6.2 Отчеты проверок

Провайдеры услуг должны обеспечить, чтобы после каждой проверки формировались отчеты, формат которых включает:

a) область применения и цели;
b) последовательность действий и процедуры;
c) выводы и результаты;
d) корректирующие меры, которые должны быть приняты;
e) отклонения и подкрепляющее логическое обоснование для дальнейшей проверки и действий.

B.14.6.3 Область применения

Провайдеры услуг должны обеспечить, чтобы проверки охватывали:

a) физическую защиту периметра и помещений площадки для восстановления;
b) оборудование физической защиты;
c) оборудование для контроля влияния внешней среды;
d) оборудование и средства ИКТ;
e) оборудование и средства телекоммуникаций;
f) энергоснабжение;
g) противопожарную и противодымную защиту;
h) защиту от протечек воды/жидкостей.

B.14.6.4 Инициирующие условия

Провайдеры услуг должны обеспечить осуществление проверок физических мощностей и оборудования в случаях, когда происходят существенные изменения требований организации. Например, когда организация добавляет дополнительные элементы оборудования с большим потреблением электроэнергии, должна быть пересмотрена мощность существующего энергоснабжения, источников бесперебойного питания и генераторов.

B.14.7 Списание

Провайдеры услуг должны обеспечить списание и (или) устранение всех физических мощностей и оборудования, выработавшего свой ресурс, персоналом, имеющим соответствующую квалификацию, в соответствии с текущими рекомендациями производителей оборудования, профессиональными стандартами (практическими приемами) и (или) нормативными требованиями.

B.14.8 Запасные части и аксессуары

Провайдеры услуг должны обеспечить наличие и доступность адекватных запасных частей и аксессуаров в целях возможного проведения необходимого ремонта, технического обслуживания и замены физических мощностей и оборудования таким образом, чтобы нарушение обычных операций было сведено к минимуму. Объем и виды запасных частей и аксессуаров, которые должны быть в распоряжении, должны отражать время простоя,

фигурирующее в соглашениях об уровне сервиса провайдеров услуг с организациями, и способность поставщиков осуществлять поставку и ремонт неисправного оборудования в оговоренный интервал времени.

В.14.9 Инвентаризационная опись

Провайдеры услуг должны обеспечить поддержку актуальных инвентаризационных описей элементов своих физических мощностей и оборудования.

В.14.10 Постоянный мониторинг

Провайдеры услуг должны обеспечить постоянный мониторинг критических элементов физических мощностей и оборудования, чтобы гарантировать их доступность. Например, мониторинг системы бесперебойного питания для основной вычислительной системы осуществляют из сетевого операционного центра, к которому она подключена.

В.14.11 Программные и программно-аппаратные средства

Провайдеры услуг должны обеспечить, чтобы политики и процедуры, относящиеся к работе физических мощностей и оборудования, были при необходимости в равной степени применимы к взаимосвязанным программно-аппаратным и программным средствам, встроенным или составляющим часть работы оборудования или мощностей.

В.15 Тестирование

В.15.1 Общая информация

Провайдеры услуг должны обеспечить, чтобы тестирование составляло неотъемлемую часть поддержания физических мощностей и оборудования в необходимом высококачественном состоянии для поддержки услуг, предлагаемых организациям.

В.15.2 Область применения

Провайдеры услуг должны обеспечить, чтобы физические мощности и оборудование, включая перечисленные в *В.14.6.3*, периодически проверяли и (или) тестировали.

В.15.3 Персонал

Провайдеры услуг должны обеспечивать тестирование персонала, управляющего их физическими мощностями и оборудованием для восстановления, а также их операционных процедур (в идеальном случае — в сочетании с тестированием физических мощностей и оборудования).

В.15.4 Жизненный цикл тестирования

Провайдеры услуг должны обеспечить, чтобы при планировании, проведении, документировании и проверке тестирования учитывали:

a) тестирование, проводимое по крайней мере ежегодно для критически важных мощностей и оборудования, влияющих на предоставляемые организациям услуги;

b) тестирование, проводимое, когда возникают какие-либо существенные изменения требований организации и (или) изменения мощностей и возможностей провайдера услуг, влияющих на предоставляемые организациям услуги, например модернизация физических мощностей, оборудования, телекоммуникаций и источников энергоснабжения;

c) тестирование, объявленное и необъявленное, надлежащим образом разработанное и спланированное, чтобы не причинять никакого ущерба, либо носящее постоянный характер, либо применяемое при наличии затруднений;

d) меры, принимаемые для обеспечения того, чтобы во время тестирования ситуация оставалась под контролем;

e) критическое тестирование, утвержденное и санкционированное руководством провайдера услуг;

f) в случае критического тестирования информирование руководства провайдера услуг и организации до начала каждого тестирования;

g) процесс тестирования, цели тестирования, планы тестирования и результаты тестирования, задокументированные для последующей проверки или аудита на предмет эффективности;

h) обнаруженные во время тестирования недостатки, исправляемые как можно раньше и не позднее следующего тестирования;

i) перечень (неисправленных) недостатков, доведенный до руководства провайдера услуг с изложением потенциальных последствий каждого представленного несовершенного действия;

j) временной график, обеспечивающий проведение всех возможных видов тестирования в определенный момент (например, различные виды тестирования должны проводиться по крайней мере каждые пять лет);

k) тестирование, отличающееся в каждом году, по возможности в целях внесения разнообразия и непредсказуемости для участников. Например, тестирование, проводимое в этом году, не должно быть точно таким же, как тестирование, проведенное в прошлом году.

Приложение С
(обязательное)

Выбор площадок для восстановления

С.1 Общая информация

В дополнение к стабильности внешней среды хорошая инфраструктура и доступность квалифицированной местной рабочей силы в данном географическом регионе будут вносить свой вклад в благоприятную обстановку для размещения и эксплуатации провайдерами услуг по восстановлению ИКТ после *ЧС* своих площадок для восстановления. Кроме того, присутствие других провайдеров услуг по восстановлению ИКТ после *ЧС* и их поставщиков в данном географическом регионе создаст их необходимое количество для местных организаций. Послужной список основных действующих лиц — еще один показатель зрелости и энергичности местных организаций по восстановлению ИКТ после *ЧС*. В зависимости от местной политической среды и ее возможностей активная поддержка местных властей будет играть решающую роль для роста и расширения такой области деятельности, как восстановление ИКТ после *ЧС*.

С.2 Инфраструктура

Внешняя инфраструктура географического региона, в котором привлеченные провайдеры услуг размещают свои площадки для восстановления, будет оказывать влияние на уровень и качество услуг, которые могут быть предоставлены. Помимо доступности на операции по восстановлению, проводимые на площадках для восстановления, может оказывать влияние наличие неустойчивости, частных флуктуаций или нарушений в любом из следующих компонентов инфраструктуры:

a) телекоммуникации;
b) энергоснабжение;
c) наземный транспорт

и в зависимости от конкретной местной среды:

1) воздушная связь и перевозки;
2) морская связь и перевозки.

С.3 Квалифицированная рабочая сила и поддержка

На местном уровне должен быть доступен готовый ресурс квалифицированных и опытных специалистов по восстановлению ИКТ после *ЧС*. Должна быть предусмотрена возможность расширения трудовых ресурсов в соответствии с географическим регионом, где:

a) достаточно высокий уровень навыков у неквалифицированных работников, чтобы их можно было легко обучить и дать необходимые знания для выполнения работ по восстановлению ИКТ после *ЧС*;

b) широкий диапазон поставщиков образовательных услуг в сфере восстановления ИКТ после *ЧС*, которые могут постоянно переобучать персонал, совершенствовать его знания и навыки.

С.4 Необходимое количество поставщиков и продавцов

В данном географическом регионе должны быть необходимое количество и широкий диапазон поставщиков и продавцов, связанных с восстановлением ИКТ после *ЧС*, которые могут предоставлять необходимые консультации, оборудование, аппаратную и программную поддержку и замену 24 часа в сутки и 365 дней в году.

Диапазон поставщиков и продавцов, связанных с восстановлением ИКТ после *ЧС*, включает:

a) консультантов;
b) поставщиков аппаратных, программных и технологических решений;
c) поставщиков площадок для восстановления и восстановления рабочей зоны;
d) поставщиков телекоммуникационных услуг.

С.5 Послужной список местных провайдеров услуг

Краткая справка о деятельности провайдеров услуг по восстановлению ИКТ после *ЧС* в данном географическом регионе служит показателем зрелости местной отрасли восстановления ИКТ после *ЧС*. Эта краткая справка может включать:

a) стаж работы в сфере локальных операций;
b) число выполненных тестирований во время локальных операций;
c) число восстановленных на локальных площадках организаций;
d) профиль поддерживаемых организаций.

С.6 Активная местная поддержка

В зависимости от страны и ее политического окружения, а также взаимосвязанных возможностей поддержка местных и федеральных властей может играть решающую роль для роста и расширения организаций по восстановлению ИКТ после *ЧС*. В зависимости от роли местных и федеральных властей в стране примеры местной поддержки могут включать:

a) установление стандарта восстановления ИКТ после *ЧС* и программы сертификации;

b) содействие основным поставщикам услуг по восстановлению ИКТ после *ЧС* в местной деятельности;

c) установление активной телекоммуникационной стратегии для привлечения основных поставщиков услуг по восстановлению ИКТ после *ЧС* к местной деятельности;

d) рекламирование местных организаций по восстановлению ИКТ после *ЧС* на широкой географической основе;

e) выделение и предварительную планировку земли для использования в качестве площадок для восстановления.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО/МЭК ТО 18044—2007	IDT	ИСО/МЭК ТО 18044:2004 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»
ГОСТ Р ИСО/МЭК 27001—2006	IDT	ИСО/МЭК 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

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

- IDT — идентичные стандарты.

Приложение ДБ
(справочное)

Терминологические статьи международного стандарта ИСО/МЭК ТО 24762, которые применены в настоящем стандарте с модификацией их содержания

ДБ.1 **информационная безопасность**: Обеспечение защиты конфиденциальности, целостности и доступности информации. (3.1.3, MOD, 3.3)*

Примечания

1 Кроме того, могут быть также включены другие свойства, такие, как подлинность, учетность, невозможность отказа от авторства и надежность.

2 Адаптировано из ИСО/МЭК 27002:2005.

ДБ.2 **организации**: Сущности, использующие услуги по восстановлению ИКТ после бедствия. (3.1.6, MOD, 3.5)*

* В скобках приведены номера терминологических статей настоящего стандарта (слева) и международного стандарта ИСО/МЭК ТО 24762:2008 (справа), а между ними — условное обозначение степени их соответствия (MOD).

Приложение ДВ
(справочное)

Сопоставление структуры настоящего стандарта со структурой международного стандарта ИСО/МЭК ТО 24762

Таблица ДВ.1

Структура настоящего стандарта	Структура международного стандарта ИСО/МЭК ТО 24762:2008
Введение*	0 Введение
1 Область применения**	1 Сфера действия
2 Нормативные ссылки***	2 Нормативные ссылки
3 Термины, определения и сокращения	3 Термины и определения
	4 Термины-аббревиатуры
4 Восстановление и обеспечение информационной безопасности информационных и телекоммуникационных систем организации при чрезвычайной ситуации и обеспечение непрерывности деятельности организации	
5 Понимание рисков непрерывности и их влияния на цели деятельности организации и восстановление защитных мер обеспечения информационной безопасности информационных и телекоммуникационных систем	
6 Восстановление после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий 6.1 Организационная основа	
6.2 Вопросы системы менеджмента информационной безопасности организации и менеджмента непрерывности бизнеса**** 6.3 Восстановление и обеспечение функционирования процессов системы менеджмента информационной безопасности организации и защитных мер информационной безопасности при чрезвычайных ситуациях****	9 Постоянное совершенствование
Приложение А. Восстановление информационно-коммуникационных технологий после чрезвычайной ситуации	5 Восстановление информационно-коммуникационных технологий после бедствия
А.1 Общая информация	5.1 Общая информация
А.2 Стабильность внешней среды	5.2 Стабильность внешней среды
А.3 Менеджмент активов	5.3 Менеджмент активов
А.4 Близость площадки	5.4 Близость площадки
А.5 Менеджмент отношений с поставщиками	5.5 Менеджмент отношений с поставщиками
А.6 Соглашения о привлечении внешних ресурсов	5.6 Соглашения о привлечении внешних ресурсов
А.7 Информационная безопасность	5.7 Информационная безопасность
А.8 Активация и дезактивация плана восстановления после чрезвычайной ситуации	5.8 Активация и дезактивация плана восстановления после бедствия
А.9 Обучение и образование	5.9 Обучение и образование
А.10 Тестирование систем ИКТ	5.10 Тестирование систем ИКТ
А.11 Планирование обеспечения непрерывности бизнеса для провайдеров услуг по восстановлению ИКТ после чрезвычайной ситуации	5.11 Планирование обеспечения непрерывности бизнеса для провайдеров услуг по восстановлению ИКТ после бедствия
А.12 Документация и периодический пересмотр	5.12 Документация и периодический пересмотр

Окончание таблицы ДБ.1

Структура настоящего стандарта	Структура международного стандарта ИСО/МЭК ТО 24762.2008
Приложение В. Средства восстановления информационно-коммуникационных технологий после чрезвычайной ситуации В.1 Общая информация В.2 Местоположение площадок для восстановления В.3 Средства физического контроля доступа В.4 Физическая безопасность помещений В.5 Специально выделенные зоны В.6 Средства контроля влияния внешней среды В.7 Телекоммуникации В.8 Энергоснабжение В.9 Менеджмент кабельной системы В.10 Противопожарная защита В.11 Центр работы в чрезвычайных ситуациях В.12 Помещения с ограниченным доступом В.13 Не относящиеся к восстановлению удобства В.14 Жизненный цикл физических мощностей и вспомогательного оборудования В.15 Тестирование	6 Средства восстановления информационно-коммуникационных технологий после бедствия 6.1 Общая информация 6.2 Местоположение площадок для восстановления 6.3 Средства физического контроля доступа 6.4 Физическая безопасность помещений 6.5 Специально выделенные зоны 6.6 Средства контроля влияния внешней среды 6.7 Телекоммуникации 6.8 Энергоснабжение 6.9 Менеджмент кабельной системы 6.10 Противопожарная защита 6.11 Центр работы в чрезвычайных ситуациях 6.12 Помещения с ограниченным доступом 6.13 Не относящиеся к восстановлению удобства 6.14 Жизненный цикл физических мощностей и вспомогательного оборудования 6.15 Тестирование
*****	7 Возможности привлеченного провайдера услуг
Приложение С Выбор площадок для восстановления С.1 Общая информация С.2 Инфраструктура С.3 Квалифицированная рабочая сила и поддержка С.4 Необходимое количество поставщиков и продавцов С.5 Послужной список местных провайдеров услуг С.6 Активная местная поддержка	8 Выбор площадок для восстановления 8.1 Общая информация 8.2 Инфраструктура 8.3 Квалифицированная рабочая сила и поддержка 8.4 Необходимое количество поставщиков и продавцов 8.5 Послужной список местных провайдеров услуг 8.6 Активная местная поддержка
*****	Приложение А (информационное) Соответствие между ИСО/МЭК 27002:2005 и данным международным стандартом
Приложение ДА Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте	
Приложение ДБ Терминологические статьи международного стандарта ИСО/МЭК ТО 24762, которые применены в настоящем стандарте с модификацией их содержания	
Приложение ДВ Сопоставление структуры настоящего стандарта со структурой международного стандарта ИСО/МЭК ТО 24762	
Библиография******	Библиография

* Положения раздела изложены в соответствии с требованиями ГОСТ Р 1.5 (подраздел 8.2) и Р 50.1.035.

** Положения раздела изложены в соответствии с требованиями ГОСТ 1.5 (подраздел 3.7).

*** Данный раздел приведен в соответствие с требованиями ГОСТ Р 1.5 (пункт 3.6).

**** Положения подраздела заменяют положения раздела 9 международного стандарта ИСО/МЭК ТО 24762, как не отвечающие объекту и предмету стандартизации настоящего стандарта.

***** Данные разделы исключены, как не имеющие непосредственного отношения к объекту и предмету стандартизации настоящего стандарта.

****** Данный раздел приведен в соответствие с требованиями ГОСТ Р 1.5 (пункт 3.11).

Библиография

[1]	ГОСТ Р ИСО/МЭК 13335-1—2006	Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
[2]	ГОСТ Р 1.4—2004	Стандартизация в Российской Федерации. Стандарты организаций. Общие положения
[3]	ГОСТ Р 22.0.02—94	Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий
[4]	PAS 77:2006	Управление непрерывностью ИТ сервисов (IT Service Continuity Management)
[5]	ГОСТ Р ИСО/МЭК ТО 13569—2007	Финансовые услуги. Рекомендации по информационной безопасности
[6]	Рекомендации по стандартизации Р 50.1.056—2005	Техническая защита информации. Основные термины и определения
[7]	Рекомендации по стандартизации Р 50.1.053—2005	Информационные технологии. Основные термины и определения в области технической защиты информации
[8]	Стандарт Банка России СТО БР ИББС-1.0—2008	Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения
[9]	ИСО/МЭК 20000-1:2005	Информационные технологии. Сервисный менеджмент. Часть 1. Спецификация (Information technology — Service Management — Part 1: Specification)
[10]	ИСО/МЭК 20000-2:2005	Информационные технологии. Сервисный менеджмент. Часть 2. Общепринятая практика (Information technology — Service Management — Part 2: Code of practice)
[11]	ИСО/МЭК 27001:2005	Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (Information technology — Security techniques — Information security management systems — Requirements)
[12]	ИСО/МЭК 27002:2005	Информационные технологии. Свод правил по управлению защитой информации (Information technology — Security techniques — Code of practice for information security management)

УДК 351.864.1:004:006.354 ОКС 35.040

Ключевые слова: защита информации, информационная безопасность, чрезвычайная ситуация, автоматизированные системы, информационно-телекоммуникационные системы, информационные и телекоммуникационные технологии, конфиденциальность, доступность, целостность, риски информационной безопасности, средства защиты информационной безопасности, функций и механизмов безопасности, восстановление информационной безопасности, восстановление защитных мер, услуги по восстановлению информационной безопасности, непрерывность, роли

Редактор *П. М. Смирнов*
Технический редактор *Н. С. Гришанова*
Корректор *С. В. Смирнова*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 22.03.2011. Подписано в печать 15.04.2011 Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 6,05. Уч.-изд. л. 5,45. Тираж 154 экз. Зак. 223

ФГУП «СТАНДАРТИНФОРМ». 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул Московская, 256.

gost.e-ecolog.ru