ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27031— 2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса

ISO/IEC 27031:2011

Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

(IDT)

Издание официальное

Москва
Стандартинформ
2014

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 Обществом с ограниченной ответственностью «Информационный аналитический вычислительный центр» (ООО «ИАВЦ») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 г. № 426-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27031:2011 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса» (ISO/IEC 27031:2011 «Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity»)

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

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования – на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет

Содержание

Введение

Информационно-коммуникационные технологии (ИКТ) со временем стали составной частью многих видов деятельности, являющихся элементами критических инфраструктур во всех секторах: государственном, частном или общественном. Распространение Интернета и других электронных сетевых услуг и современные возможности систем и прикладных программ также означают, что организации стали еще более зависимы от заслуживающих доверия, надежных и безопасных инфраструктур ИКТ.

Между тем, потребность в менеджменте непрерывности бизнеса (МНБ), включая готовность к инцидентам, планирование восстановления после бедствия, реагирование на чрезвычайные ситуации и их менеджмент, была признана и поддерживается в конкретных областях знаниями, опытом, и разработанными и опубликованными за последние годы стандартами, включая международные стандарты по менеджменту непрерывности бизнеса, разработанные ИСО/ТК 223.

Примечание – В ИСО/ТК 223 находится в процессе разработки соответствующий международный стандарт по менеджменту непрерывности бизнеса (ИСО 22301).

Сбои услуг ИКТ, включая возникновение таких проблем безопасности, как вторжение в систему или инфицирование вредоносной программой, будут оказывать влияние на непрерывность операций бизнеса. Следовательно, менеджмент ИКТ и связанная с ними непрерывность, а также другие аспекты безопасности формируют ключевую часть требований по обеспечению непрерывности бизнеса. Кроме того, в большинстве случаев критические функции бизнеса, которые необходимы для обеспечения непрерывности бизнеса, обычно зависят от ИКТ. Такая зависимость означает, что нарушения ИКТ могут создавать стратегические риски для репутации организации и ее возможности функционирования.

Для многих организаций готовность ИКТ является важнейшей составляющей в реализации менеджмента непрерывности бизнеса и менеджмента информационной безопасности. Частью реализации и функционирования системы менеджмента информационной безопасности (СМИБ), определенной в ИСО/МЭК 27001, и системы менеджмента непрерывности бизнеса (СМНБ), соответственно, является необходимость разработки и реализации плана обеспечения готовности услуг ИКТ для обеспечения уверенности в непрерывности бизнеса.

В результате эффективность менеджмента непрерывности бизнеса часто зависит от фактической готовности ИКТ, обеспечивающей уверенность в том, что в период нарушения продолжают выполняться цели организации. Это особенно важно в связи с тем, что последствия нарушений ИКТ часто имеют дополнительные осложнения, будучи скрытыми и (или) трудно обнаруживаемыми.

Чтобы организация достигла готовности ИКТ к обеспечению непрерывности бизнеса (ГИКТОНБ), ей необходимо ввести систематический процесс предупреждения, прогнозирования и менеджмента нарушений ИКТ и инцидентов, обладающих возможностью нарушения услуг ИКТ. Лучше всего этого можно достичь путем применения фаз цикла «Планирование – Осуществление – Проверка – Действие» (PDCA – Plan-Do-Check-Act) как части системы менеджмента в ГИКТОНБ. Таким способом ГИКТОНБ будет поддерживать менеджмент непрерывности бизнеса, обеспечивая уверенность в соответствующей устойчивости услуг ИКТ и возможности их восстановления до заранее определенных уровней в рамках временных сроков, требуемых и согласованных организацией.

Таблица 1 – Цикл «Планирование – Осуществление – Проверка – Действие» в ГИКТОНБ

Планирование	Установление политики, целей, планов, процессов и процедур ГИКТОНБ, относящихся к менеджменту риска и совершенствованию готовности ИКТ, для достижения результатов в соответствии с общими политиками и целями обеспечения непрерывности бизнеса организации
Осуществление	Внедрения и выполнение политики, мер и средств контроля и управления, процессов и процедур ГИКТОНБ
Проверка	Оценка и, где это применимо, измерение показателей эффективности процесса по отношению к политике ГИКТОНБ, целям и практическому опыту, и уведомление о результатах руководства для рассмотрения
Действие	Принятие корректирующих и превентивных мер на основе результатов проводимой руководством проверки для достижения постоянного совершенствования ГИКТОНБ

Если организация применяет ИСО/МЭК 27001 для создания СМИБ и (или) применяет соответствующие стандарты для создания СМНБ, предпочтительно, чтобы

при создании ГИКТОНБ учитывались существующие или планируемые процессы, связанные с этими стандартами. Такая связь поможет поддержать создание ГИКТОНБ, а также поможет избежать любых двойственных процессов для организации. На рисунке 1 показано взаимодействие ГИКТОНБ и СМНБ.

При планировании и реализации ГИКТОНБ организация может обращаться к ИСО/МЭК 24762:2008 по вопросу планирования и предоставления услуг по восстановлению ИКТ после бедствия независимо от того, предоставляются ли такие услуги самой организацией или привлеченным поставщиком услуг.

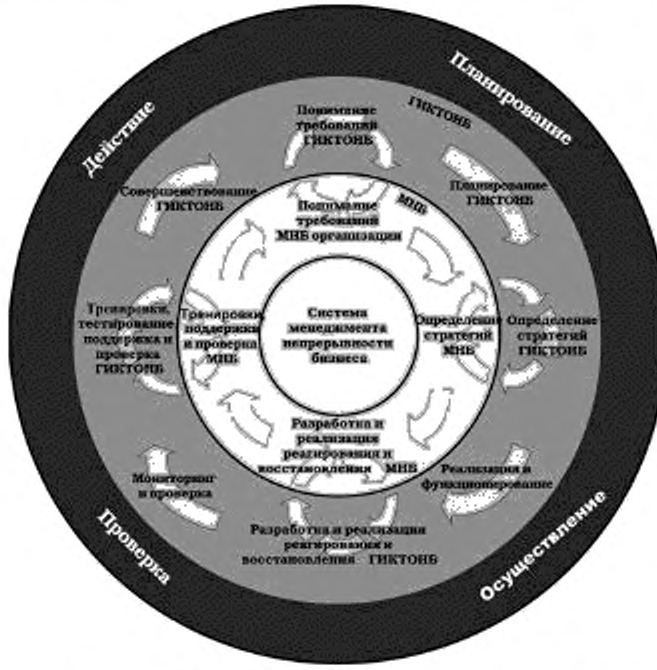

Рисунок 1 – Интеграция ГИКТОНБ и СМНБ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса

Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity

Дата введения – 2014-01-01

1 Область применения

В настоящем стандарте описываются концепции и принципы готовности информационно-коммуникационных технологий (ИКТ) к обеспечению непрерывности бизнеса (ОНБ), и предоставляется система методов и процессов определения и точного изложения всех аспектов (таких как критерии эффективности, проектирование и реализация) для совершенствования готовности ИКТ организации к обеспечению непрерывности бизнеса. Он применим для любой организации (частной, государственной, негосударственной, независимо от ее размера), разрабатывающей программу готовности ИКТ к обеспечению непрерывности бизнеса (ГИКТОНБ) и требующей от своих услуг/инфраструктур ИКТ готовности к поддержке операций бизнеса в случае возникновения событий, инцидентов и связанных с ними нарушений, которые могут оказывать влияние на непрерывность (включая безопасность) критических функций бизнеса. Он также дает возможность организации измерять параметры эффективности, связанные с ГИКТОНБ, согласованным и признанным способом.

Область применения настоящего стандарта охватывает все события и инциденты (в том числе связанные с безопасностью), которые могут оказывать влияние на инфраструктуры и системы ИКТ. Он включает и развивает практические приемы урегулирования и менеджмента инцидентов информационной безопасности, а также услуг ИКТ и планирования готовности ИКТ.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных документов используют только указанное издание. Для недатированных документов используют самое последнее издание ссылочного документа (с учетом всех изменений).

ИСО/МЭК ТО 18044:2004[1)] Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (ISO/IEC TR 18044:2004, Information technology – Security techniques – Information security incident management).

ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология (ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary)

ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements)

ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод правил для менеджмента информационной безопасности (ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management)

ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности (ISO/IEC 27005, Information technology – Security techniques – Information security risk management).

[1)] ИСО/МЭК ТО 18044:2004 заменен на ИСО/МЭК 27035:2011.

3 Термины и определения

Для целей данного документа применяются термины и определения, приведенные в ИСО/МЭК ТО 18044, ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27005 и представленные ниже.

3.1 **альтернативная площадка** (alternative site): Альтернативное рабочее помещение, выбранное организацией для использования в случае, если после аварии обычные операции бизнеса не могут осуществляться в обычном помещении.

3.2 **менеджмент непрерывности бизнеса;** МНБ (business continuity management – BCM): Целостный управленческий процесс, идентифицирующий потенциальные угрозы для организации и их влияние на операции бизнеса, и обеспечивающий основу для повышения устойчивости организации с возможностью эффективного реагирования, что обеспечивает защиту интересов основных причастных сторон организации, ее репутации, бренда и деятельности по созданию ценностей.

3.3 **план обеспечения непрерывности бизнеса;** ПНБ (business continuity plan – BCP): Документированные процедуры, которым следует организация при осуществлении реагирования, восстановления, возобновления и возвращения к заранее определенному уровню операций после нарушения.

Примечание – Обычно он охватывает ресурсы, услуги и мероприятия, необходимые для обеспечения непрерывности критических функций бизнеса.

3.4 **анализ влияния на бизнес;** АВБ (business impact analysis – BIA): Процесс анализа оперативных функций и влияния, которое может оказывать на них нарушение функционирования бизнеса.

3.5 **критический** (critical): Качественная характеристика, используемая, чтобы подчеркнуть важность ресурса, процесса или функции, которые должны быть постоянно доступными и действующими или доступными и действующими с наиболее раннего возможного момента времени после инцидента, чрезвычайной ситуации или бедствия.

3.6 **нарушение** (disruption): Ожидаемый (например, ураган) или непредвиденный (например, нарушение/прекращение энергоснабжения, землетрясение или атака на системы/инфраструктуру ИКТ) инцидент, который нарушает обычный ход операций на площадке организации.

3.7 **восстановление ИКТ после бедствия** (ICT disaster recovery): Способность элементов ИКТ организации поддерживать ее критические функции бизнеса на приемлемом уровне в течение определенного периода времени после нарушения.

3.8 **план восстановления ИКТ после бедствия** (ICT disaster recovery plan – ICT DRP): Четко определенный и документально оформленный план по восстановлению возможностей ИКТ в случае возникновения нарушения.

Примечание – В некоторых организациях его называют планом обеспечения непрерывности ИКТ.

3.9 **характер отказа** (failure mode): Признаки, посредством которых отказ проявляется.

Примечание – Характер отказа обычно описывает, как происходит отказ, и какое влияние он оказывает на функционирование системы.

3.10 **готовность ИКТ к обеспечению непрерывности бизнеса; ГИКТОНБ** (ICT readiness for business continuity – IRBC): Способность организации поддерживать свои операции бизнеса путем предупреждения, обнаружения, реагирования на нарушения и восстановления услуг ИКТ.

3.11 **минимальная цель обеспечения непрерывности бизнеса; МЦНБ** (minimum business continuity objective – MBCO): Обеспечение минимального уровня услуг и (или) продуктов, которые являются приемлемыми для организации в достижении ее целей бизнеса во время нарушения.

3.12 **заданная точка восстановления; ЗТВ** (recovery point objective – RPO): Момент времени, к которому должны быть восстановлены данные после произошедшего нарушения.

3.13 **заданное время восстановления; ЗВВ** (recovery time objective – RTO): Период времени после произошедшего нарушения, в течение которого должны быть восстановлены минимальные уровни услуг и (или) продукты, а также поддерживающие системы, прикладные программы или функции.

3.14 **устойчивость** (resilience): Способность организации противостоять нарушению, будучи затронутой им.

3.15 **инициатор** (trigger): Событие, которое инициирует реакцию системы.

Примечание – Также известен, как инициирующее событие.

3.16 **важнейшая запись** (vital record): Электронная или бумажная запись, которая необходима для сохранения, продолжения или восстановления деятельности организации и для защиты прав организации, ее служащих, клиентов и заинтересованных сторон.

4 Сокращения

В настоящем стандарте применяют следующие сокращения:

CFIA – анализ влияния отказа компонентов (component failure impact analysis);

DRP – планирование восстановления после бедствия (disaster recovery planning);

FMEA – анализ вида отказов и их влияния (failure mode effect analysis);

PDCA – планирование–осуществление–проверка–действие (Plan-Do-Check- Act);

RAID – избыточные дисковые массивы (Redundant Array of Disks);

SAN – сеть хранения данных (storage area network);

АВБ – анализ влияния на бизнес (BIA – business impact analysis);

ГИКТОНБ – готовность ИКТ к обеспечению непрерывности бизнеса (IRBC – ICT readiness for business continuity);

ЗВВ – заданное время восстановления (RTO – recovery time objective);

ЗТВ – заданная точка восстановления (RPO – recovery point objective);

ИКТ – нформационно-коммуникационные технологии (ICT – information and communication technology);

МНБ – менеджмент непрерывности бизнеса (BCM – business continuity management);

МЦНБ – минимальная цель обеспечения непрерывности бизнеса (MBCO – minimum business continuity objective);

ОНБ – обеспечение непрерывности бизнеса;

ПНБ – план непрерывности бизнеса (BCP – business continuity plan);

СМИБ – система менеджмента информационной безопасности (ISMS – information security management system);

СМНБ – система менеджмента непрерывности бизнеса.

5 Обзор

5.1 Роль ГИКТОНБ в менеджменте непрерывности бизнеса

Менеджмент непрерывности бизнеса (МНБ) – это целостный управленческий процесс, идентифицирующий потенциальные воздействия, которые угрожают непрерывности бизнес-деятельности организации, и обеспечивающий основу для создания устойчивости и возможности эффективного реагирования, что обеспечивает защиту интересов организации от нарушений.

Как часть процесса МНБ, ГИКТОНБ относится к системе менеджмента, которая дополняет и поддерживает программу МНБ и (или) СМИБ организации для повышения готовности организации к:

a) реагированию на постоянно изменяющуюся среду риска;

b) обеспечению уверенности в продолжении критических операций бизнеса, поддерживаемых связанными с ними услугами ИКТ;

c) реагированию при обнаружении одного или серии взаимосвязанных событий, которые становятся инцидентами, до возникновения нарушений услуг ИКТ; и

d) реагированию на инциденты/бедствия и отказы, а также к восстановлению после них.

Рисунок 2 иллюстрирует желаемый результат ИКТ для поддержки мероприятий менеджмента непрерывности бизнеса.

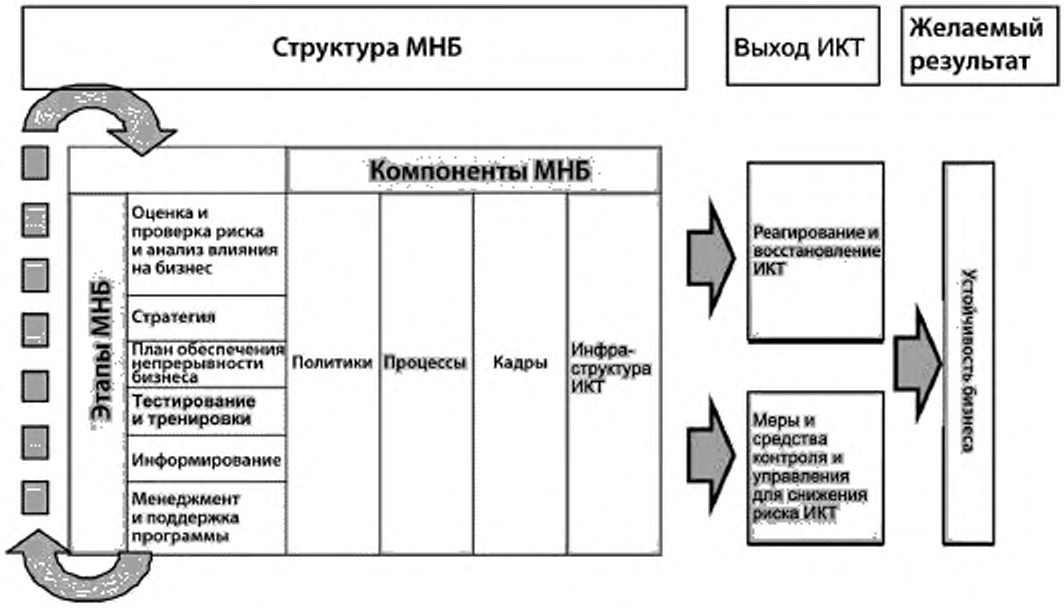

Рисунок 2 – Структура обеспечения непрерывности бизнеса, связанный с ней выход ИКТ и желаемый результат

Разработанный ИСО/ТК 223 международный стандарт по МНБ обобщает подход МНБ к предупреждению инцидентов, реагированию на них и восстановлению после них. Входящие в МНБ деятельности включают обеспечение готовности к инцидентам, менеджмент непрерывности операций, планирование восстановления после бедствия (DRP – disaster recovery planning) и уменьшение риска, которые сосредоточены на повышении устойчивости организации и ее подготовке к эффективному реагированию на инциденты, а также на восстановлении после них в рамках заранее определенных временных шкал.

Таким образом, организация четко расставляет свои приоритеты в отношении МНБ, и именно ими руководствуются в деятельности ГИКТОНБ. В свою очередь, МНБ зависит от ГИКТОНБ в обеспечении уверенности в том, что организация может достичь своих общих целей по обеспечению непрерывности в любое время, особенно во время нарушения.

Как показано на рисунке 3, такие деятельности по обеспечению готовности направлены на:

a) совершенствование возможностей обнаружения инцидентов;

b) предупреждение внезапного или резкого отказа;

c) допущение возможности приемлемого ухудшения рабочего состояния, если отказ непреодолим;

d) дальнейшее сокращение времени восстановления; и

e) сведение к минимуму влияния при возможном возникновении инцидента.

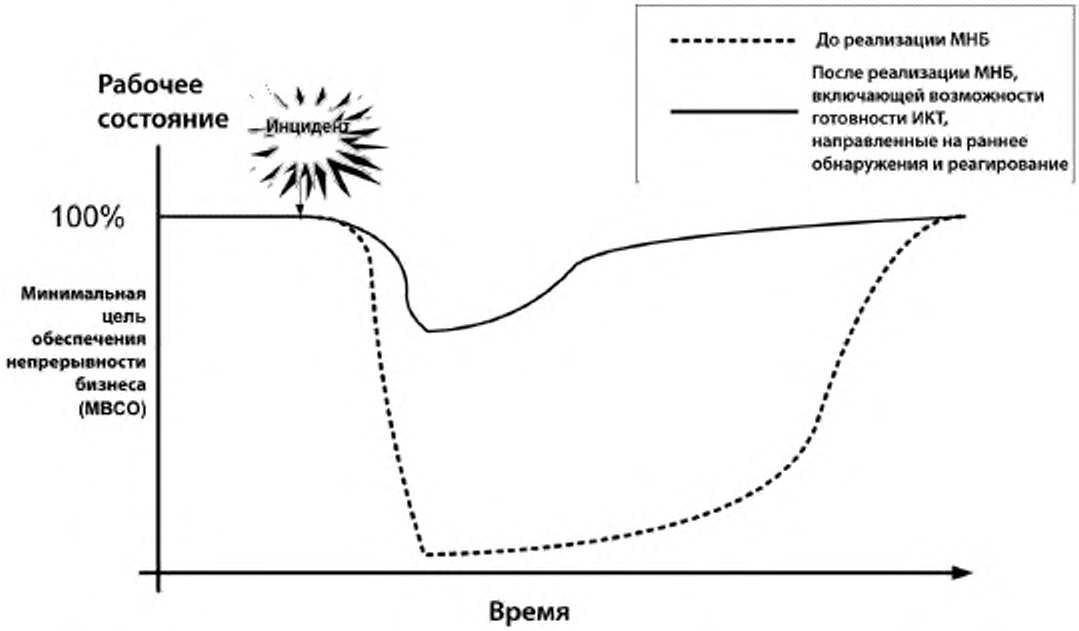

Рисунок 3 – Концепция готовности ИКТ к обеспечению непрерывности бизнеса

5.2 Принципы ГИКТОНБ

ГИКТОНБ основывается на следующих ключевых принципах:

a) предупреждение инцидентов – защита услуг ИКТ от таких угроз, как неблагоприятное влияние внешней среды и аппаратные сбои, операционные ошибки, злоумышленные атаки и природные бедствия, является крайне важной для поддержки желаемых уровней доступности систем в организации;

b) обнаружение инцидентов – самое быстрое обнаружение инцидентов будет сводить к минимуму их влияние на услуги, сокращать работы по восстановлению и сохранять качество услуг;

c) реагирование – реагирование на инцидент наиболее подходящим способом приведет к более эффективному восстановлению и уменьшит любые простои. Неудачное

реагирование может привести к перерастанию незначительного инцидента в нечто более серьезное;

d) восстановление – определение и реализация соответствующей стратегии восстановления будет обеспечивать уверенность в своевременном возобновлении услуг и поддержке целостности данных. Понимание приоритетов восстановления позволит восстанавливать в первую очередь наиболее критические услуги. Услуги, носящие менее критический характер, могут восстанавливаться позднее или, при некоторых условиях, вообще не восстанавливаться;

e) совершенствование – уроки, усвоенные из реагирования на мелкие и крупные инциденты, должны документироваться, анализироваться и пересматриваться. Понимание этих уроков даст возможность организации лучше подготавливаться, контролировать и избегать инцидентов и нарушений.

Рисунок 4

бедствия и, в свою очередь, поддерживает деятельности по обеспечению непрерывности бизнеса. Реализация ГИКТОНБ дает возможность организации эффективно реагировать на новые и возникающие угрозы, а также реагировать на нарушения и восстанавливаться после них.

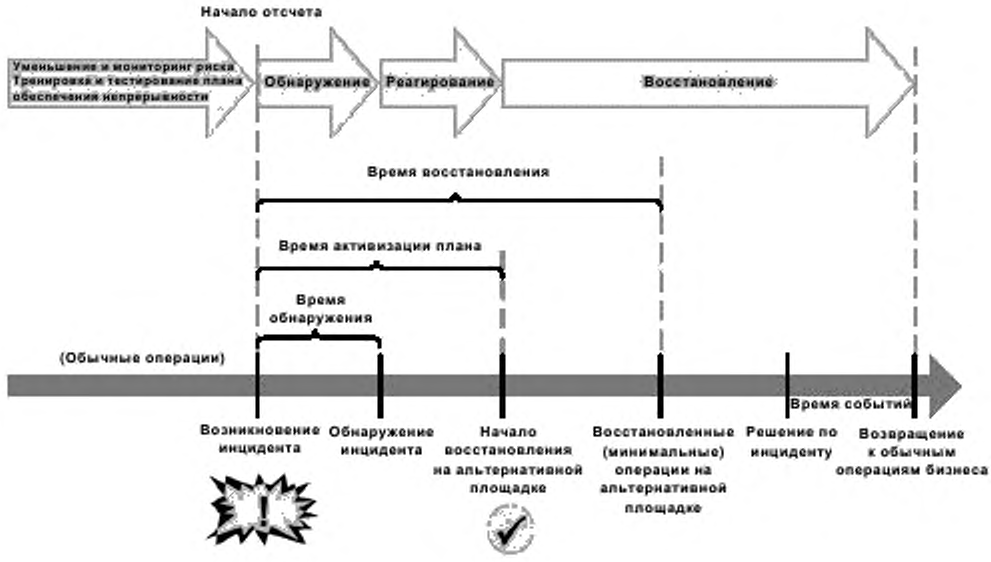

Рисунок 4 – Принципы ГИКТОНБ на типичной временной шкале восстановления ИКТ после бедствия

Примечание – Этап восстановления включает своевременное восстановление/возобновление услуг, устойчивые операции восстановления ИКТ после бедствия и возврат к обычным операциям. Подробности см. на рисунке А.1 в приложении А.

5.3 Элементы ГИКТОНБ

Ключевые элементы ГИКТОНБ можно обобщить следующим образом:

a) кадры: специалисты, обладающие соответствующими навыками и знаниями, и компетентный резервный персонал;

b) сооружения: физическая среда, в которой расположены ресурсы ИКТ;

c) техническое оснащение:

1) аппаратные средства (включая стойки, серверы, дисковые массивы, накопители на магнитной ленте и приборы);

2) сети (включая услуги передачи данных и голоса), коммутаторы и маршрутизаторы; и

3) программные средства, включая операционную систему и прикладные программы, связь или интерфейсы между прикладными программами и подпрограммы пакетной обработки данных;

d) данные: данные прикладных программ, голосовые данные и другие виды данных;

e) процессы: восстановления и поддержки услуг ИКТ, включая поддерживающую документацию для описания конфигурации ресурсов ИКТ и создания возможности эффективного функционирования;

f) поставщики: компоненты цепочки поставки услуг, где предоставление услуг ИКТ зависит от внешнего поставщика услуг или другой организации, участвующих в цепочке поставок, например, поставщик данных по финансовым рынкам, поставщик телекоммуникационных услуг или поставщик Интернет-услуг.

5.4 Результаты и выгоды ГИКТОНБ

Выгоды эффективной ГИКТОНБ для организации состоят в том, что организация:

a) понимает риски по отношению к непрерывности услуг ИКТ и их уязвимости;

b) определяет потенциальные влияния от нарушения услуг ИКТ;

c) содействует улучшению сотрудничества между руководителями бизнеса и поставщиками её услуг ИКТ (внутренними и внешними);

d) развивает и повышает компетентность своего персонала ИКТ путем демонстрации надежного реагирования посредством проведения тренировок по планам обеспечения непрерывности бизнеса и тестирования механизмов ГИКТОНБ;

e) обеспечивает высшему руководству уверенность в том, что оно может рассчитывать на заранее определенные уровни услуг ИКТ и получать адекватную поддержку и средства сообщения в случае аварии;

f) обеспечивает высшему руководству уверенность в надлежащем сохранении уровня информационной безопасности (конфиденциальность, целостность и доступность) при обеспечении строгого следования политикам информационной безопасности;

g) предоставляет дополнительную уверенность в стратегии обеспечения непрерывности бизнеса, связывая инвестиции в информационные технологии с потребностями бизнеса и обеспечивая защиту услуг ИКТ на соответствующем уровне с учетом их значимости для организации;

h) использует рентабельные услуги ИКТ, а не услуги с недостаточным или чрезмерным финансированием, благодаря пониманию уровня зависимости организации от этих услуг ИКТ и характера, месторасположения, взаимозависимостей и использования компонентов, составляющих услуги ИКТ;

i) может улучшать свою репутацию в отношении предусмотрительности и эффективности;

j) потенциально получает конкурентное преимущество благодаря продемонстрированной способности обеспечивать непрерывность бизнеса и поддерживать предоставление услуг и продуктов во время нарушения; и

k) понимает и документирует ожидания причастных сторон, их связь с услугами ИКТ и их использование.

Таким образом, ГИКТОНБ обеспечивает достоверный способ определения статуса услуг ИКТ организации в поддержке ее целей обеспечения непрерывности бизнеса, рассматривая вопрос «Способна ли наша ИКТ реагировать?», а не «Является ли наша ИКТ безопасной?».

5.5 Установление ГИКТОНБ

ГИКТОНБ, вероятно, будет более эффективной и рентабельной, когда она спроектирована и встроена в услуги ИКТ с самого начала, как часть стратегии ГИКТОНБ, поддерживающей цели обеспечения непрерывности бизнеса организации. Это обеспечит уверенность в том, что услуги ИКТ будут лучше созданы, лучше поняты и более устойчивы. Изменение ГИКТОНБ может быть сложной, вызывающей нарушения и дорогостоящей задачей.

Организация должна разрабатывать, реализовывать, поддерживать и постоянно совершенствовать совокупность документально оформленных процессов, которые будут поддерживать ГИКТОНБ.

Эти процессы должны обеспечивать уверенность в том, что цели ГИКТОНБ четко изложены, поняты и доведены до сведения, а также демонстрировать заинтересованность высшего руководства в ГИКТОНБ.

Рисунок 5 графически представляет виды деятельности, происходящие на различных этапах обеспечения ГИКТОНБ.

Рисунок 5 – Этапы ГИКТОНБ

5.6 Использование цикла «Планирование-Осуществление-Проверка-Действие» для установления ГИКТОНБ

ГИКТОНБ предполагает создание в организации процессов разработки и совершенствования ключевых элементов ГИКТОНБ (см. 5.3), чтобы повысить их способность реагировать на нарушения любого вида, включая меняющиеся ситуации риска, посредством использования подхода «Планирование-Осуществление-Проверка-Действие». На рисунке 5 графически представлены виды деятельности, происходящие на различных этапах ГИКТОНБ.

5.7 Обязанности руководства

5.7.1 Руководящая роль и заинтересованность руководства

Чтобы программа ГИКТОНБ была эффективной, она должна быть процессом, полностью интегрированным с управленческой деятельностью верхнего звена организации, одобренным и поддержанным высшим руководством. Для поддержки и менеджмента программы ГИКТОНБ может потребоваться ряд специалистов с практическим опытом в области ГИКТОНБ и персонал других ведущих направлений деятельности и служб. Количество ресурсов, требуемых для поддержки такой программы, будет зависеть от величины и сложности организации.

5.7.2 Политика ГИКТОНБ

Организация должна иметь документально оформленную политику ГИКТОНБ. Первоначально это может быть высокоуровневый документ, уточняемый и расширяемый по мере достижения зрелости всего процесса ГИКТОНБ. Политика должна регулярно проверяться и обновляться в соответствии с потребностями организации и должна согласовываться с более обширными целями менеджмента непрерывности бизнеса организации.

Политика ГИКТОНБ должна предоставлять организации документально оформленные принципы, к выполнению которых она будет стремиться и по которым может измеряться эффективность ГИКТОНБ. Политика должна:

a) устанавливать и демонстрировать заинтересованность высшего руководства в программе ГИКТОНБ;

b) включать цели ГИКТОНБ организации или ссылаться на них;

c) определять область применения ГИКТОНБ, включая ограничения и исключения;

d) утверждаться и одобряться высшим руководством;

e) доводиться до сведения соответствующих внутренних и внешних причастных сторон;

f) определить и обеспечить для соответствующих структур доступность ресурсов, таких как бюджетные средства; персонал, необходимый для осуществления деятельностей в соответствии с политикой ГИКТОНБ; и

g) подвергаться проверке через запланированные интервалы времени и в случае возникновения значительных изменений, таких как изменения внешней среды, изменения бизнеса и структуры организации.

6 Планирование ГИКТОНБ

6.1 Общая информация

Основной задачей этапа планирования является установление требований готовности ИКТ организации, включая:

a) стратегию ГИКТОНБ и план ГИКТОНБ, требуемые для поддержки бизнеса, законные (т. е. основанные на законе) нормативно-правовые требования, связанные с определенной сферой деятельности и достижением целей и задач непрерывности бизнеса организации; и

b) критерии эффективности, необходимые организации для мониторинга степени готовности ИКТ, которая требуется для достижения этих задач и целей.

6.2 Ресурсы

6.2.1 Общая информация

В рамках политики организация должна определить потребность в программе ГИКТОНБ, исходя из общих целей менеджмента непрерывности бизнеса, а также определить и обеспечить ресурсы, необходимые для установления, реализации, функционирования и поддержки такой программы ГИКТОНБ.

Должны определяться и документироваться связанные с ГИКТОНБ роли, обязанности, компетентность и полномочия.

Высшее руководство должно:

a) назначить или предложить лицо с соответствующим должностным положением и авторитетом для несения ответственности за политику и реализацию ГИКТОНБ; и

b) назначить одно или несколько компетентных лиц, которые вне зависимости от других обязанностей должны реализовывать и поддерживать систему менеджмента ГИКТОНБ, как описывается в настоящем стандарте.

6.2.2 Компетентность персонала, обеспечивающего ГИКТОНБ

Организация должна обеспечить уверенность в том, что весь персонал, которому поручены обязанности, связанные с ГИКТОНБ, был компетентен в выполнении требуемых задач. Подробнее см. в 7.2.1.

6.3 Определение требований

6.3.1 Общая информация

В рамках программы МНБ организация должна определить категорию своих видов деятельности в соответствии с их приоритетами для обеспечения непрерывности (как определено анализом влияния на бизнес) и определить минимальный уровень, на котором должна выполняться каждая критическая деятельность при ее возобновлении. Высшее руководство должно согласовать требования непрерывности бизнеса организации, исходя из которых будет задано время восстановления (ЗВВ) и задана точка восстановления (ЗТВ) для минимальной цели обеспечения непрерывности бизнеса (МЦНБ) на продукт, услугу или вид деятельности. Это ЗВВ начинается с момента возникновения нарушения до восстановления продукта, услуги или деятельности.

6.3.2 Понимание критических услуг ИКТ

Существует целый ряд услуг ИКТ, которые могут считаться критическими и необходимыми для обеспечения восстановления. Для каждой из этих критических услуг ИКТ должны быть заданы и документально оформлены заданное время восстановления (ЗВВ) и заданные точки восстановления (ЗТВ) для минимальной цели обеспечения непрерывности бизнеса (МЦНБ) услугами ИКТ. (Это может включать такие аспекты предоставляемых услуг ИКТ, как служба технической поддержки.) ЗВВ критических услуг ИКТ неизменно будет значительно меньше, чем ЗВВ непрерывности бизнеса. (См. приложение А, где приводится детальный разбор ЗВВ и ЗТВ.)

Организация должна определить и документально оформить свои критические услуги ИКТ, включая краткие описания и названия, значимые для организации на уровне пользователя услуг. Это обеспечит общее понимание услуг ИКТ персоналом, имеющим отношение к бизнесу и ИКТ, так как для одной и той же услуги ИКТ могут использоваться разные названия. Для каждой перечисленной критической услуги ИКТ необходимо определить поддерживаемый ею продукт или услугу организации, и высшее руководство должно согласовать услуги ИКТ и связанные с ними требования ГИКТОНБ.

Для каждой определенной и согласованной критической услуги ИКТ должны быть описаны и документированы все компоненты ИКТ в цепочке поставки услуги, показывая, каким образом они конфигурируются или связываются для предоставления каждой услуги. Должны быть документально оформлены конфигурации как обычной среды поставки услуг ИКТ, так и среды поставки услуг обеспечения непрерывности ИКТ.

Для каждой критической услуги ИКТ текущие возможности обеспечения непрерывности (например, существование единой точки отказа) следует пересматривать с профилактической точки зрения, чтобы оценить риски прерывания или ухудшения услуг (оценка может быть предпринята как часть общей оценки риска в МНБ). Следует также искать возможности повышения устойчивости услуг ИКТ и, таким образом, снижения вероятности и (или) влияния нарушения услуг. Это также может придать большее значение возможности раннего обнаружения нарушений услуг ИКТ и реагирования на них. Организация может принять решение, если существует бизнес-обоснование относительно вложения средств в установленные возможности для повышения устойчивости услуг. Такая оценка риска услуг (которая может стать частью общей структуры менеджмента риска организации) может также привести к уточнению бизнес-обоснования для расширения возможностей восстановления услуг ИКТ.

6.3.3 Определение расхождений между возможностями обеспечения готовности ИКТ и требованиями непрерывности бизнеса

Для каждой критической услуги ИКТ следует сравнивать используемые механизмы обеспечения готовности ИКТ, такие как предупреждение, мониторинг, обнаружение, реагирование и восстановление, с требованиями непрерывности бизнеса и документировать любые расхождения.

Высшее руководство должно быть проинформировано о любых расхождениях между критическими возможностями ГИКТОНБ и требованиями непрерывности бизнеса. Такие

расхождения могут указывать на риски и потребность в дополнительных ресурсах для обеспечения устойчивости и восстановления, таких как:

a) персонал, включая количество, навыки и знания;

b) помещения для размещения средств ИКТ, например, машинный зал;

c) поддерживающая технология, аппаратура, оборудование и сети (технология);

d) информационные прикладные программы и базы данных;

e) распределение финансовых или бюджетных средств; и

f) внешние услуги и поставщики (поставки).

Высшее руководство должно одобрить описания услуг ИКТ, документально оформленный перечень критических услуг ИКТ и риски, связанные с установленными расхождениями между критическими возможностями ГИКТОНБ и требованиями непрерывности бизнеса. В соответствующих случаях это должно включать одобрение идентифицированных рисков. Затем должны исследоваться варианты решения вопроса, касающегося установленных расхождений и рисков, посредством определения стратегий ГИКТОНБ.

6.4 Определение вариантов стратегии ГИКТОНБ

6.4.1 Общая информация

Стратегии ГИКТОНБ должны определять подходы к реализации необходимой устойчивости, чтобы вводились принципы предупреждения инцидентов, обнаружения, реагирования, восстановления и возобновления.

Необходимо оценивать полный спектр вариантов стратегий ГИКТОНБ. Выбранные стратегии должны быть способны поддерживать требования обеспечения непрерывности бизнеса организации.

При разработке стратегии организация должна учитывать реализацию и текущую потребность в ресурсах. Может быть заключен договор с внешними поставщиками о предоставлении услуг специалистов и передаче опыта, что играет важную роль в поддержке стратегии.

Стратегия ГИКТОНБ должна быть достаточно гибкой, чтобы удовлетворять разным стратегиям бизнеса в условиях рыночных отношений. Кроме того, стратегия должна учитывать такие внутренние ограничения и факторы, как:

a) бюджет;

b) доступность ресурсов;

c) потенциальные затраты и выгоды;

d) технологические ограничения;

e) готовность организации рисковать;

f) существующая стратегия ГИКТОНБ организации; и

g) нормативные обязательства.

6.4.2 Варианты стратегии ГИКТОНБ

Организация должна рассмотреть спектр вариантов для обеспечения готовности к инцидентам своих критических услуг ИКТ. Варианты должны учитывать усиление защиты и устойчивости, а также обеспечение возобновления и восстановления после незапланированного нарушения и могут включать внутренние механизмы, услуги, предоставляемые организацией, и услуги, предоставляемые извне одной или несколькими третьими сторонами.

Варианты должны учитывать различные компоненты, необходимые для обеспечения уверенности в непрерывности и восстановлении критических услуг ИКТ. ГИКТОНБ может быть достигнута различными способами, и следует принимать во внимание описанные в 5.3 элементы ГИКТОНБ.

6.4.2.1 Навыки и знания

Организация должна определить соответствующие стратегии для поддержки основных знаний и навыков в отношении ИКТ. Это может также распространяться на персонал подрядчиков и других причастных сторон, обладающих обширными специальными навыками и знаниями, связанными с ИКТ. Стратегии защиты или обеспечения таких навыков могут включать:

a) документирование способа выполнения критических услуг ИКТ;

b) разностороннюю подготовку персонала ИКТ и подрядчиков для повышения избыточности навыков;

c) разделение основных навыков для снижения концентрации риска (это может привести к физическому разделению персонала, обладающего основными навыками, или к обеспечению уверенности в том, что необходимыми основными навыками обладает не один человек);

d) сохранение знаний и управление знаниями.

6.4.2.2 Помещения

В соответствии с идентифицированными рисками организация должна разрабатывать стратегии, направленные на уменьшение влияния непригодности обычных помещений ИКТ. Это может включать один или несколько следующих факторов:

a) альтернативные помещения (площадки) в рамках организации, включая перемещение других видов деятельности;

b) альтернативные помещения, предоставляемые другими организациями;

c) альтернативные услуги, предоставляемые специалистами третьей стороны;

d) работа дома или на других удаленных площадках;

e) другие согласованные подходящие рабочие места;

f) использование альтернативной рабочей силы на установленной площадке; и

g) альтернативные средства, которые могут быть транспортированы на площадку, где произошло нарушение, и использованы для обеспечения прямой замены некоторых из затронутых физических активов.

Стратегии в отношении помещений ИКТ могут значительно различаться, может быть доступен ряд вариантов. Разные виды инцидентов или угроз могут требовать реализации многих стратегий (подход «выбери и смешай»), которые в частности будут определяться величиной, широтой деятельности, местоположением, технологиями, бюджетом организации и т. д.

При рассмотрении вопроса использования альтернативных помещений нужно принимать во внимание следующее:

a) безопасность площадки;

b) доступ персонала;

c) близость к существующим помещениям; и

d) доступность.

6.4.2.3 Технология

Услуги ИКТ, от которых зависит критическая деятельность бизнеса, должны стать доступными до возобновления зависящей от них критической деятельности бизнеса. Таким образом, требуются решения, обеспечивающие уверенность в доступности прикладных программ не позднее определенных временных сроков, например, заданного времени восстановления, определяемого в рамках анализа влияния на бизнес.

Технологические платформы и прикладное программное обеспечение должны быть установлены в сроки, требуемые организацией в целом.

Технологиям, поддерживающим критические услуги ИКТ, часто требуются сложные механизмы обеспечения непрерывности, так что при выборе стратегий ГИКТОНБ нужно учитывать следующее:

a) ЗВВ и ЗТВ для критических услуг ИКТ, поддерживающих критические виды деятельности, идентифицированные МНБ;

b) местоположение и расстояние между технологическими площадками;

c) количество технологических площадок;

d) удаленный доступ к системам;

e) требования охлаждения;

f) требования энергоснабжения;

g) использование необслуживаемых (темных) площадок в отличие от площадок с персоналом;

h) телекоммуникационная связь и резервная схема маршрутизации;

i) характер восстановления после отказа (требуется ли ручное вмешательство для активации альтернативных средств ИКТ или это должно происходить автоматически);

j) уровень требуемой автоматизации;

k) устаревание технологии; и

l) возможность связи с привлеченным поставщиком услуг и другие внешние каналы связи.

6.4.2.4 Данные

Критическая деятельность бизнеса может, кроме того, зависеть от предоставления новейших или почти новейших данных. Должны быть разработаны связанные с критической деятельностью бизнеса решения по обеспечению непрерывности данных для достижения заданной точки восстановления (ЗТВ) каждой критической деятельности бизнеса организации.

Выбранные варианты ГИКТОНБ должны обеспечивать уверенность в постоянной конфиденциальности, целостности и доступности критических данных, поддерживающих критические виды деятельности (см. ИСО/МЭК 27001 и ИСО/МЭК 27002).

Стратегии ГИКТОНБ и хранения данных должны удовлетворять требованиям обеспечения непрерывности бизнеса организации и учитывать следующие факторы:

a) требования ЗТВ;

b) как обеспечивается безопасное хранение данных, например, диска, магнитной ленты или оптического носителя данных; должны существовать соответствующие механизмы резервного копирования и восстановления для обеспечения уверенности в безопасности данных и в безопасности среды;

c) где хранится и куда транспортируется или передается информация, расстояние, местонахождение

; и

d) , определяемые объемом данных, способом их хранения и сложностью технического процесса восстановления, наряду с требованиями пользователя услуг и потребностями в обеспечении организационной непрерывности.

Договоренность об использовании данных «из конца в конец» крайне важна. Это может включать передачу и поступление информации от третьих сторон.

Следует помнить о том, что характер, актуальность и ценность данных могут быть весьма разнообразными в пределах организации.

6.4.2.5 Процессы

При выборе своей стратегии ГИКТОНБ организация должна учитывать процессы, необходимые для обеспечения уверенности в жизнеспособности этой стратегии, включая те, что необходимы для предупреждения инцидентов, обнаружения инцидентов, реагирования на инциденты и восстановления после бедствия. Организация также должна устанавливать любые факторы, необходимые для эффективной реализации этих отдельных процессов, например, совокупность основных навыков, критические данные, основные эффективные технологии или критическое оборудование/средства.

6.4.2.6 Поставщики

Организация должна устанавливать и документировать внешние отношения, поддерживающие предоставление услуг

сроки. Такие зависимости могут существовать для аппаратных и программных средств, телекоммуникаций, прикладных программ, услуг хостинга третьей стороны, вспомогательных услуг и вопросов, связанных с внешней средой, таких как кондиционирование воздуха, экологический мониторинг и ликвидация пожаров.

Стратегии для этих услуг могут включать:

a) хранение дополнительного оборудования и копий программ на другой площадке;

b) соглашения с поставщиками о поставке оборудования для замены в кратчайшие сроки;

c) быстрый ремонт и (или) замена неисправных частей в случае неисправности оборудования;

d) двойные источники ресурсов, таких как энергетика и телекоммуникации;

e) аварийное генераторное оборудование; и

f) определение альтернативных поставщиков/замены поставщиков.

Организация должна включать требования менеджмента непрерывности бизнеса и ИКТ в договоры со своими партнерами и поставщиками услуг. Графики выполнения договоров должны включать ссылки на обязательства каждой стороны, согласованные уровни услуг, реагирование на существенные инциденты, распределение затрат, частоту проведения тренировок и корректирующие меры.

6.5 Одобрение

Выбранные варианты стратегии ГИКТОНБ должны быть представлены высшему руководству с рекомендациями для принятия решений на основе готовности организации рисковать и затрат.

Высшее руководство должно быть уведомлено, что если выбранные варианты стратегии ГИКТОНБ не способны отвечать требованиям непрерывности бизнеса, то оно может быть проинформировано о существующих возможностях.

Высшее руководство должно выбрать стратегии ГИКТОНБ из представленных ему вариантов, утвердить и подписать документально оформленные варианты для подтверждения того, что были приняты надлежащие варианты, и что они поддерживают общие требования обеспечения непрерывности бизнеса.

Выбранные варианты стратегии ГИКТОНБ должны:

a) принимать во внимание вероятные риски и последствия повреждений;

b) интегрироваться с выбранными стратегиями обеспечения непрерывности бизнеса организации; и

c) соответствовать выполнению общих целей организации в рамках ее готовности рисковать.

6.6 Улучшение возможностей ГИКТОНБ

6.6.1 Повышение устойчивости

Организация должна включить в свою высокоуровневую стратегию и планы ГИКТОНБ ссылку на конкретные улучшения возможностей ГИКТОНБ, которые требуются для удовлетворения ее установленных требований ГИКТОНБ. Такие улучшения могут быть достигнуты путем применения превентивных и корректирующих мер (см. 9.2 и 9.3), а также других конкретных процессов или методик, которые предлагают адекватные реакции на анализ влияния на бизнес организации и ее готовности рисковать.

Информацию о таких процессах и (или) методиках можно найти в приложениях В и С.

6.7 Критерии эффективности готовности ИКТ

6.7.1 Определение критериев эффективности

В любой среде ИКТ существует много потенциально опасных событий – например, отказы аппаратных средств, вторжения, угрожающие безопасности, и т. д. – и организация должна быть способна проводить мониторинг угроз и понимать, может ли система ГИКТОНБ адекватно бороться с ними.

Таким образом, организация должна определить критерии для измерения эффективности готовности ее ИКТ. Такие критерии могут использоваться для определения желаемого качества реагирования на нарушение, как в терминах эффективности, так и в терминах результативности.

Критерии эффективности ГИКТОНБ должны быть основаны на требованиях ГИКТОНБ, а также на общих целях МНБ с точки зрения реагирования на инциденты и требований обеспечения непрерывности (обращайтесь к 8.3.1).

7 Реализация и функционирование

7.1 Общая информация

Стратегии ГИКТОНБ должны реализовываться только после получения санкций высшего руководства. С этого момента начинается этап реализации. В этом разделе

представлены рекомендации по реализации выбранных стратегий ГИКТОНБ организации вместе с необходимой организационной структурой, планами и процедурами, необходимыми для поддержки реализации.

Организация должна управлять ресурсами (см. 7.2), процедурами и процессами по обеспечению ГИКТОНБ, а также осуществлять программы информирования и обучения. Реализация должна управляться, начиная с плана, посредством формального процесса управления изменениями организации, а также мер и средств контроля и управления менеджмента проекта МНБ, чтобы обеспечить уверенность в полной прозрачности управления и отчетности.

Во время внедрения компонентов обнаружения и реагирования на инциденты и компонентов восстановления после бедствия следует обращаться к соответствующим международным стандартам, включая:

a) ИСО/МЭК 18043 по вопросу выбора и эксплуатации систем обнаружения вторжений;

b) ИСО/МЭК 18044 по вопросу процесса реагирования на инциденты; и

c) ИСО/МЭК 24762 по вопросу услуг восстановления после бедствия.

Примечание – ИСО/МЭК 18044 перерабатывается и будет переиздан как ИСО/МЭК 27035.

7.2 Реализация элементов стратегий ГИКТОНБ

7.2.1 Осведомленность, навыки и знания

Общая осведомленность о готовности элементов услуг ИКТ (см. 5.3) – кадров, помещений, технологий, данных, процессов и поставщиков, а также их критических компонентов – является решающим элементом обеспечения уверенности в требуемой поддержке системы менеджмента и управления непрерывностью бизнеса, включая готовность ИКТ. Следовательно, организация должна:

a) повышать, улучшать и поддерживать осведомленность с помощью непрерывного обучения и информационных программ для соответствующего персонала и установить процесс оценки эффективности обеспечения осведомленности; и

b) обеспечить уверенность в осведомленности персонала о том, какой вклад он вносит в достижение целей ГИКТОНБ.

Организация должна обеспечить уверенность в том, что компетентность всего персонала, на который возложены обязанности по управлению ГИКТОНБ, достаточна для выполнения требуемых задач посредством:

a) определения необходимой компетентности такого персонала;

b) проведения анализа потребности в обучении такого персонала;

c) предоставления обучения;

d) обеспечения уверенности в достижении необходимой компетентности; и

e) сохранения записей об образовании, профессиональной подготовке, навыках, опыте и квалификации.

7.2.2 Помещения

Системы восстановления ИКТ и критические данные, по возможности, должны быть физически отделены от рабочей площадки, чтобы предотвратить влияние на них одного и того же инцидента.

При реализации стратегии следует обратить внимание на местонахождение всего оборудования ИКТ. Например, при наличии систем ИКТ для обучения или макетирования они должны быть логически отделены от производственных систем, чтобы можно было переконфигурировать их в случае бедствия для быстрого увеличения производимых услуг.

Должны быть изучены общие характеристики масштабируемости, управляемости, поддержки, эффективности и стоимости для различных стратегий реализации, чтобы определить наиболее подходящие методы для выбранных стратегий, поддерживающие общие цели и задачи обеспечения непрерывности бизнеса.

7.2.3 Технология

Должны быть реализованы технологические стратегии ИКТ. К ним можно отнести один или несколько из следующих механизмов реализации:

a) горячий резерв, когда инфраструктура ИКТ дублируется на двух площадках;

b) теплый резерв, когда восстановление происходит на дополнительной площадке с частично подготовленной инфраструктурой ИКТ;

c) холодный резерв, когда инфраструктура создается или конфигурируется с нуля на альтернативной площадке;

d) механизмы поставки, в соответствии с которыми внешние поставщики услуг предоставляют аппаратные средства; и

e) составной механизм предыдущих стратегий: подход «выбери и смешай».

7.2.4 Данные

Меры обеспечения доступности данных должны соответствовать требованиям, установленным в стратегиях менеджмента ГИКТОНБ, и могут включать:

a) дополнительное хранение данных в виде, обеспечивающем их доступность в пределах сроков, установленных в программе обеспечения непрерывности бизнеса; и

b) альтернативные места хранения данных, которые могут быть физическими или виртуальными, при условии поддержки безопасности и конфиденциальности данных; следовательно, должны существовать соответствующие процедуры доступа, а при использовании для хранения такой информации мер третьих сторон владельцы информации должны убедиться в наличии соответствующих мер и средств контроля и управления.

7.2.5 Процессы

Процессы обеспечения ГИКТОНБ должны быть четко и достаточно детально документированы, чтобы дать возможность компетентному персоналу их выполнять (некоторые из этих процессов могут отличаться от повседневных операций).

Процедуры ГИКТОНБ могут зависеть от возникающей ситуации и на практике могут потребовать адаптации в зависимости от характера аварии (например, степени потерь или повреждений), приоритетов деятельности организации и требований причастных сторон.

7.2.6 Поставщики

Организация должна обеспечивать уверенность в том, что критические поставщики способны обеспечивать услуги по поддержке ГИКТОНБ, требуемые организацией. Это включает наличие у них собственных документально оформленных и протестированных планов обеспечения непрерывности бизнеса и ГИКТОНБ с возможностью поддержки одновременного приведения в действие клиентами планов реагирования на инциденты или восстановление. Организация должна установить процесс оценки мощностей и возможностей поставщиков, прежде чем привлекать их услуги, а также осуществлять постоянный мониторинг и проверку возможностей поставщиков после заключения договора. Полезным средством определения возможностей поставщиков является их соответствие требованиям/хорошим практическим приемам из соответствующих стандартов, например, принятие лучших практических приемов из ИСО/МЭК 24762

поставщиками, осуществляющими хостинг/менеджмент альтернативных средств обработки и предоставляющими услуги по восстановлению ИКТ после бедствия.

7.3 Реагирование на инциденты

В случае любого инцидента ИКТ должно осуществляться реагирование на инциденты с целью:

a) подтверждения характера и степени инцидента;

b) взятия ситуации под контроль;

c) сдерживания инцидента; и

d) взаимодействия с причастными сторонами.

Реагирование на инциденты должно инициировать соответствующие действия в отношении ГИКТОНБ. Это реагирование должно быть интегрировано с общим реагированием на инциденты в МНБ и может потребовать привлечения группы управления инцидентами или, в небольших организациях, отдельного лица, в чьи обязанности входит управление инцидентами и обеспечение непрерывности бизнеса.

Более крупные организации могут использовать многоуровневый подход и создавать различные группы, предназначенные для выполнения разных функций. В рамках ИКТ это может быть основано на технических вопросах или вопросах, связанных с услугами.

Лица, отвечающие за управление инцидентами, должны иметь планы активизации, работы, координации и связи относительно реагирования на инциденты.

7.4 Документы плана ГИКТОНБ

7.4.1 Общая информация

Организации должна иметь документы (планы) для управления при возможных нарушениях, чтобы обеспечить непрерывность услуг ИКТ и восстановление критической деятельности.

Планы организации по менеджменту инцидентов ИКТ, обеспечению непрерывности бизнеса и техническому восстановлению могут быть быстро активированы последовательно или одновременно.

Организация может разработать специальные документы планов восстановления или возвращения услуг ИКТ в «нормальное» состояние (планы восстановления). Однако определить, что такое «нормальное» состояние иногда можно только через некоторое время после инцидента, поэтому немедленная реализация планов восстановления может быть недопустимой. В этой связи организация должна обеспечить уверенность в том, что механизмы непрерывности способны к дополнительным действиям по поддержке в более обширном плане непрерывности бизнеса, предоставляя время на приведение в действие планов восстановления («возвращения в нормальное состояние»).

7.4.2 Содержание документов плана восстановления

У небольшой организации может быть единственный документ – план, охватывающий все мероприятия по восстановлению услуг ИКТ для всей ее деятельности. У очень большой организации может быть много документов плана восстановления, каждый из которых детально определяет восстановление конкретного элемента услуг ИКТ.

Планы реагирования и восстановления ИКТ должны быть лаконичными и доступными для лиц, чьи обязанности определены в планах. Планы должны содержать следующие элементы:

a) назначение и сфера действия.

Назначение и область применения каждого конкретного плана должны быть определены, одобрены высшим руководством и понятны лицам, которые будут осуществлять план. Должны быть четко сформулированы любые взаимосвязи с другими соответствующими планами или документами организации, особенно с планами обеспечения непрерывности бизнеса, должны быть даны четкие ссылки и описан способ получения этих планов и доступа к ним.

В каждом плане менеджмента инцидентов, реагирования и восстановления ИКТ должны быть изложены приоритетные цели с точки зрения:

i) критических услуг ИКТ, подлежащих восстановлению;

ii) ;

iii) уровней восстановления, необходимых для каждой критической услуги ИКТ; и

iv) ситуаций, в которых может быть активизирован каждый план.

В соответствующих случаях планы могут также содержать процедуры и перечни контрольных вопросов, поддерживающие процесс проверки после инцидента;

b) роли и обязанности.

Должны четко документироваться роли и обязанности лиц и групп, обладающих полномочиями (как с точки зрения принятия решений, так и осуществления расходов) во время инцидента и после него;

c) активизация плана.

Примечание – Потерянное на реагирование время, несомненно, нельзя возвратить. Практически всегда лучше инициировать реагирование ИКТ, а позднее свернуть его, чем упустить возможность сдержать инцидент на ранней стадии и предотвратить его расширение.

По этой причине организации должны использовать эскалацию менеджмента инцидентов и обращаться к протоколам активизации, содержащимся в более подробных планах обеспечения непрерывности бизнеса, для того, чтобы сформировать основу для менеджмента потенциальных нарушений, связанных с услугами ИКТ.

Метод активизации плана реагирования и восстановления ИКТ должен быть четко документирован. Этот процесс должен предусматривать активизацию соответствующих планов или частей планов в кратчайшие сроки, либо до потенциально разрушительного события, либо немедленно после такого события.

План должен включать ясное и точное описание:

i) способа мобилизации назначенного лица или группы;

ii) пунктов незамедлительного сбора;

iii) последующих мест сбора группы и подробностей о любых альтернативных местах сбора (в более крупных организациях эти места сбора могут упоминаться как командные центры); и

iv) обстоятельств, в которых организация считает реагирование ГИКТОНБ ненужным (например, незначительные неисправности и простои, которые, возможно, затрагивают критические услуги ИКТ, но менеджмент которых осуществляется посредством обычной службы технической поддержки, а также механизмов и соглашений о поддержке).

Организация должна документально оформить четкий процесс отзыва группы реагирования ИКТ после завершения инцидента и возвращения к обычной деятельности;

d) владелец и ответственный за поддержку документации плана реагирования и восстановления ИКТ.

Руководство должно назначить владельца документации плана реагирования и восстановления ИКТ, отвечающего за регулярный пересмотр и обновление документации.

Следует применять систему управления версиями и официально уведомлять все заинтересованные стороны об изменениях, а также поддерживать формальные записи о распространении документов плана по обеспечению непрерывности;

e) контактная информация.

Примечание – Записи о контактах могут содержать информацию для связи во внерабочее время. Однако в тех случаях, когда планы упоминают такую информацию частного характера, особое внимание должно быть уделено соблюдению приватности информации.

В соответствующих случаях каждый документ плана должен содержать или предоставлять ссылки на необходимую контактную информацию для всех основных причастных сторон.

7.4.3 Документация плана реагирования и восстановления ИКТ

Документация плана реагирования и восстановления ИКТ должна:

a) быть гибкой, выполнимой и относящейся к делу;

b) быть легко читаемой и понимаемой; и

c) обеспечивать основу для управления серьезными проблемами, которые рассматриваются организацией как заслуживающие реагирования ГИКТОНБ (обычно после существенного разрушительного события).

Документация должна определять общую структуру, в рамках которой формируются планы восстановления, охватывая:

a) общую стратегию;

b) критические услуги (с ЗВВ/ЗТВ);

c) шкалу восстановления; и

d) группы восстановления и их обязанности.

Планы должны быть так документально оформлены, чтобы компетентный персонал мог использовать их в случае инцидента. Они должны включать:

a) цели: краткое описание целей планов;

b) область применения: охватывая со ссылкой на результаты анализа влияния на бизнес следующее:

i) критичность услуг: описание соответствующих услуг и определение их критичности;

ii) технологию: обзор основной технологии, поддерживающей услуги, включая ее размещение;

iii) организацию: обзор организаций (отделов, важнейших лиц, процедур), управляющих технологиями; и

iv) документацию: обзор основной документации для технологии, включая (внешние) площадки, где она хранится;

c) требования доступности: определенные бизнесом требования в отношении доступности услуг и связанных с ними технологий;

d) требования информационной безопасности: требования обеспечения информационной безопасности услуг, систем и данных, включая требования конфиденциальности, целостности и доступности;

e) процедуры восстановления технологии: описание процедур, которым нужно следовать для восстановления услуг ИКТ, включая следующее:

i) перечень мероприятий, например, техническая поддержка настольных компьютеров и восстановление контактной информации;

ii) перечень мероприятий для возвращения сетей, систем, прикладных программ, баз данных и т. д. на согласованный уровень на альтернативной площадке с учетом изменившейся среды (например, это может влиять на пропускную способность линий связи, межсистемную коммуникацию и т. д.);

iii) перечень мероприятий по восстановлению основных функциональных возможностей, таких как безопасность, определение доступных маршрутов передачи данных, регистрация;

iv) координацию в рамках прикладной программы или между прикладными программами, синхронизацию данных и потенциальные автоматизированные процедуры для обработки накопившейся информации;

v) процессы, необходимые для восстановления услуг ИКТ и передачи их пользователям для эксплуатации в режиме восстановления;

vi) процедуры резервного копирования; и

vii) где и как люди могут получать дополнительную информацию, например, телефоны «горячей линии», и предпринимаемые шаги для возвращения в нормальное состояние;

f) приложения:

i) инвентарная опись информационных систем, прикладных программ и баз данных;

ii) обзор сетевой инфраструктуры и наименований серверов;

iii) инвентарная опись аппаратных средств и системного программного обеспечения; и

iv) договоры и соглашения об уровне услуг;

g) основные поставщики ИКТ:

i) поставщики при обычной деловой деятельности; и

ii) поставщики услуг по восстановлению.

7.5 Программа обеспечения осведомленности, компетентности и профессиональной подготовки

Должна быть реализована скоординированная программа для обеспечения уверенности в наличии процессов регулярной поддержки осведомленности о ГИКТОНБ в целом, а также для оценки и повышения компетентности всего соответствующего персонала, играющего ключевую роль в успешной реализации ГИКТОНБ (см. 7.2.1).

7.6 Контроль документации

7.6.1 Контроль записей, связанных с ГИКТОНБ

Должны быть установлены меры и средства контроля и управления записями, связанными с ГИКТОНБ, с целью:

a) обеспечения уверенности в том, что они остаются удобочитаемыми, легко идентифицируемыми и извлекаемыми; и

b) обеспечения их хранения, защиты и извлечения.

7.6.2 Контроль документации ГИКТОНБ

Должны быть установлены меры и средства контроля и управления для документации ГИКТОНБ для обеспечения уверенности в том, что:

a) документы проверены на соответствие до их выпуска;

b) по мере необходимости документы пересматриваются, обновляются и вновь утверждаются;

c) определены изменения и текущее состояние пересмотренных версий документации;

d) соответствующие версии применяемых документов доступны в точках использования;

e) документы из внешних источников идентифицированы и их распространение контролируется; и

f) предотвращено непреднамеренное использование устаревших документов и осуществлена соответствующая маркировка таких документов, если они сохраняются для каких-либо целей.

8 Мониторинг и проверка

8.1 Поддержка ГИКТОНБ

8.1.1 Общая информация

Изменения приносят с собой риск – не только риск отказа, но также риск дестабилизации существующих политик и стратегий. Поэтому стратегии ГИКТОНБ должны быть устойчивыми и адаптируемыми.

Любое изменение услуг ИКТ, которое может оказывать влияние на возможности ГИКТОНБ, должно реализовываться только после оценки и рассмотрения последствий изменения для обеспечения непрерывности бизнеса.

Для обеспечения уверенности в том, что стратегии и планы ГИКТОНБ остаются актуальными для организации:

a) высшее руководство должно обеспечить уверенность в том, что стратегии ГИКТОНБ продолжают поддерживать требования менеджмента непрерывности бизнеса организации;

b) процесс управления изменениями должен включать все стороны, ответственные за стратегии ГИКТОНБ, как за их планирование, так и за их реализацию;

c) процесс внедрения новых услуг ИКТ должен быть одобрен, чтобы устойчивость не была скомпрометирована в результате даже самых простых модернизаций или усовершенствований;

d) при слияниях и поглощениях должна осуществляться оценка устойчивости деятельности; и

e) вывод из эксплуатации компонента ИКТ следует отразить в системе менеджмента связанной с ГИКТОНБ.

8.1.2 Мониторинг, обнаружение и анализ угроз

Организация должна установить процесс постоянного мониторинга и обнаружения возникающих угроз безопасности ИКТ, включающий следующие сферы, но не ограничивающийся ими:

a) сохранение персонала, навыков и знаний;

b) управление объектами, содержащими оборудование ИКТ (например, путем мониторинга количества и характера инцидентов/уязвимостей безопасности, связанных с машинным залом);

c) управление изменениями поддерживающей технологии, аппаратуры, оборудования и сетей;

d) управление изменениями информационных прикладных программ и баз данных;

e) управление распределением финансовых или бюджетных средств; и

f) управление эффективностью внешних услуг и поставщиками (поставками).

8.1.3 Тесты и тренировки

8.1.3.1 Общая информация

Организация должна проводить тренировки не только в отношении процесса восстановления услуги ИКТ, но также ее элементов защиты и устойчивости, чтобы определить следующее:

a) может ли обеспечиваться защита, поддержка и (или) восстановление услуги независимо от серьезности инцидента;

b) могут ли механизмы менеджмента ГИКТОНБ сводить к минимуму влияние на бизнес; и

c) являются ли действенными процедуры возвращения к обычному состоянию бизнеса.

8.1.3.2 Тесты и программа тренировок

В большинстве случаев всю совокупность элементов и процессов ГИКТОНБ, включая восстановление ИКТ, нельзя проверить одним тестом и тренировкой. Поэтому

может быть уместен режим последовательного проведения тренировок, направленный на создание полной имитации реального инцидента. Программа должна включать разные уровни тренировок, от ознакомительного до проверки способности системы машинного зала восстанавливать функции, как показано на рисунке 5, и должна учитывать все аспекты цепочки поставки услуг ИКТ.

С тестами и тренировками связаны риски, и такие действия не должны подвергать организацию неприемлемому уровню риска. Тест и программа тренировок должны определять, как решается вопрос риска каждой тренировки. Следует получить одобрение программы высшим руководством и документально оформить четкое объяснение связанных с ней рисков.

Цели тестов и программы тренировок должны быть полностью совместимы с более широкими целями и сферой действия менеджмента непрерывности бизнеса и должны дополнять более общую программу тренировок организации. Каждый тест и тренировка должны отвечать целям бизнеса (даже когда нет прямого вовлечения бизнеса) и определенным техническим целям тестов или подтверждения правильности определенного элемента стратегии ГИКТОНБ.

Отдельная тренировка для каждого отдельного элемента на компонентном уровне дополняет полноту системы тренировок и должна поддерживаться как часть действующего теста и программы тренировок.

Тесты и программа тренировок должны определять частоту, область применения и вид каждой тренировки. Ниже приведены высокоуровневые примеры областей применения тренировок:

a) восстановление данных: восстановление отдельного файла или базы данных после порчи;

b) восстановление отдельного сервера (включая полную перекомпоновку данных);

c) восстановление прикладной программы (оно может включать несколько серверов, другие прикладные программы и инфраструктуру);

d) обход отказа услуг, размещенных на платформе высокой доступности (например, кластеризация: имитация потери какого-то элемента кластера – см. приложение В);

e) восстановление данных с магнитной ленты (восстановление отдельного файла или серии файлов из внешнего хранилища магнитных лент);

f) тестирование сети; и

g) тесты на отказоустойчивость инфраструктуры связи.

Тренировки должны быть последовательными, чтобы включать усиленную проверку зависимостей и взаимосвязей и соответствующих сообществ конечных пользователей.

8.1.3.3 Область применения тренировок

Тренировки должны выполняться для:

a) формирования уверенности всей организации в том, что стратегия обеспечения устойчивости и восстановления соответствует требованиям бизнеса;

b) демонстрации того, что критические услуги ИКТ могут поддерживаться и восстанавливаться в пределах согласованных уровней услуг или целей восстановления независимо от инцидента;

c) демонстрации того, что в случае инцидента критические услуги ИКТ могут быть возвращены в состояние, предшествующее тестированию в месте восстановления;

d) предоставления возможности ознакомления персонала с процессом восстановления;

e) обучения персонала и обеспечения уверенности в том, что персонал обладает адекватными знаниями планов и процедур ГИКТОНБ;

f) проверки того, что ГИКТОНБ осталась синхронизированной с инфраструктурой ИКТ и общей инфраструктурой;

g) определения любых необходимых усовершенствований стратегии ГИКТОНБ, архитектуры или процессов восстановления; и

h) обеспечения свидетельств для целей аудита и демонстрации способности услуг ИКТ организации.

Тренировки должны применяться к среде ИКТ в целом и ко всем компонентам, участвующим в цепочке предоставления услуг, от машинного зала до настольного компьютера пользователя или любого другого канала поставки услуг.

8.1.3.4 Элементы восстановления услуг

Организация должна применять все элементы восстановления услуг ИКТ в соответствии с ее размерами, а также сложностью и областью применения менеджмента непрерывности бизнеса. Применение не должно сосредотачиваться только на услугах восстановления и возобновления, а должно также охватывать надежность возможностей обеспечения устойчивости, мониторинг системы и менеджмент сигналов тревоги.

Для достижения высоких уровней уверенности и устойчивости организация должна применять тестирование от уровня компонента до полной (исходя из места нахождения) системы.

Рисунок 6 – Поступательность тестирования и программ тренировок

Тренировками должны быть охвачены следующие элементы:

a) машинный зал, например, физическая безопасность; системы обнаружения возгорания и протечек воды; процесс эвакуации; отопление, вентиляцию и кондиционирование воздуха; мониторинг окружающей среды; действия при тревоге и электропроводка;

b) инфраструктура, включая общую устойчивость связности узлов сети; сетевое разнообразие; сетевая безопасность, включая защиту от вирусов, а также предупреждение и обнаружение вторжений;

c) аппаратные средства, включая серверы, телекоммуникационное оборудование, дисковые массивы и сменные носители данных;

d) программное обеспечение;

e) данные;

f) услуги; и

g) роли и реагирование поставщиков.

8.1.3.5 Планирование тренировок

Для обеспечения уверенности в том, что тренировка не вызывает инцидентов или не подрывает возможности обслуживания, необходимо тщательное планирование для сведения к минимуму риска возникновения инцидентов как прямого результата тренировки.

Менеджмент риска должен соответствовать уровню выполняемых тренировок (т. е. элементам восстановления услуг). Это может включать:

a) обеспечение уверенности в том, что непосредственно перед тренировкой все данные имеют резервные копии;

b) выполнение тренировок в изолированной среде; и

c) планирование тренировок на нерабочее время или спокойные периоды производственного цикла с извещением конечных пользователей.

Тренировки должны быть реалистичными, тщательно спланированными и согласованными с причастными сторонами, чтобы риск нарушения процессов бизнеса был минимальным. Однако они не должны проводиться во время инцидентов.

Масштаб и сложность тренировок должны соответствовать целям восстановления организации.

Каждая тренировка должна иметь заранее согласованный и одобренный заказчиком тренировки «круг полномочий», который может включать следующее:

a) описание;

b) цели;

c) область применения;

d) предположения;

e) ограничения;

f) риски;

g) критерии успеха;

h) ресурсы;

i) роли и обязанности;

j) высокоуровневые график/сроки;

k) сбор данных по тренировкам;

l) регистрацию тренировки/инцидента;

m) «разбор полета»; и

n) действия после тренировки (последующая деятельность и отчетность).

Планирование тренировки должно предоставить организации возможность достижения определенных критериев успеха.

8.1.3.6 Менеджмент тренировок

Должна быть разработана четкая структура управления тренировками с распределением ролей и обязанностей между соответствующими лицами. Структура управления тренировками может включать:

a) руководителя тренировок (участвующего в общем управлении тестом и тренировкой);

b) связь во время тренировки;

c) подтверждение наличия достаточного количества сотрудников для безопасного проведения тренировок;

d) достаточное количество наблюдателей и (или) посредников, чтобы фиксировать ход тренировок и вести регистрацию проблем;

e) ключевые контрольные точки тренировок;

f) протоколы по окончанию тренировок; и

g) протоколы тренировок по аварийной остановке.

Тренировками необходимо управлять для обеспечения уверенности в том, что:

a) цели и ключевые контрольные точки будут выполнены;

b) весь материал и мероприятия тренировок имеют соответствующие уровни конфиденциальности;

c) любые текущие риски отслеживаются и уменьшаются;

d) любые контролеры/наблюдатели имеют полномочия;

e) ход тренировок фиксируется согласованным образом; и

f) после тренировки проводится «разбор полета» всех участников и рассматриваются замечания и предложения.

8.1.3.7 Проверка, отчет и последующая деятельность

В конце тренировки полученные данные должны быть проверены и незамедлительно приняты меры. Это должно включать:

a) сбор результатов и выводов;

b) анализ результатов и выводов относительно целей тренировки и критериев успеха;

c) определение любых расхождений;

d) установление направления действий с определенными сроками;

e) составление отчета о тренировке для формального рассмотрения заказчиком тренировки; и

f) последующие объединенные действия по отчету о тренировке.

8.2 Внутренний аудит ГИКТОНБ

План внутреннего аудита ГИКТОНБ должен определять и документировать критерии, область действия, метод и частоту аудитов (например, проводимый ежегодно внутренний аудит ГИКТОНБ). План аудита должен обеспечивать уверенность в том, что для проведения аудита назначаются только квалифицированные внутренние аудиторы. Выбор аудиторов и проведение аудита должны обеспечивать объективность и беспристрастность процесса аудита. Аудиторы, проводящие внутренний аудит ГИКТОНБ, должны быть компетентными в выполнении возложенной на них задачи. Например, аудиторы должны проходить соответствующее обучение для приобретения знаний и навыков, необходимых для проведения аудита.

Должна быть установлена процедура, обеспечивающая уверенность в исправлении недостатков, выявленных во время внутренних аудитов ГИКТОНБ.

План аудита должен охватывать также внешние стороны. Например, аудиту должны подвергаться виды деятельности привлеченных поставщиков-производителей, реализуемые на основе аутсорсинга, для определения их способности поддерживать стратегии и планы ГИКТОНБ организации во время повседневной деятельности, а также при реагировании на бедствие и восстановлении после него.

Внутренние аудиты должны проводиться в случае существенных изменений критических услуг ИКТ, требований непрерывности бизнеса (имеющих отношение к сфере действия ГИКТОНБ) или требований ГИКТОНБ.

Результаты внутреннего аудита ГИКТОНБ должны быть зафиксированы и доведены до сведения заинтересованных лиц. Руководство должно рассматривать результаты внутренних аудитов ГИКТОНБ и состояние последующих корректирующих мер.

8.3 Проводимая руководством проверка

8.3.1 Общая информация

Высшее руководство должно обеспечивать проверку системы менеджмента ГИКТОНБ через запланированные интервалы времени. Входными данными для этой проверки могут быть данные внутренних или внешних аудитов или самооценки. Проверка должна включать оценку возможностей совершенствования и необходимости изменений менеджмента ГИКТОНБ, включая политику и цели ГИКТОНБ.

Кроме того, высшее руководство должно ежегодно проверять утвержденные требования ГИКТОНБ, включая определения услуг ИКТ, документально оформленный перечень критических услуг ИКТ и риски, связанные с расхождениями, выявленными между критическими возможностями готовности ИКТ и требованиями непрерывности бизнеса.

Результаты проверки должны четко документироваться, а записи должны поддерживаться.

8.3.2 Входные данные для проверки

Входные данные для проводимой руководством проверки должны включать информацию о:

a) уровнях внутренних услуг;

b) способности внешнего поставщика услуг поддерживать соответствующие уровни услуг;

c) результатах соответствующих аудитов;

d) замечаниях и предложениях заинтересованных сторон, в том числе независимых наблюдений;

e) состоянии предупреждающих и корректирующих мер;

f) уровне остаточного риска и допустимом риске;

g) последующих действиях, вытекающих из предыдущих проводимых руководством проверок и рекомендаций;

h) уроках, извлеченных из результатов тестов и тренировок, инцидентах и о программе обучения и повышения осведомленности; и

i) новых соответствующих практических приемах и руководствах.

8.3.3 Выходные данные проверки

Выходные данные проверки должны быть одобрены высшим руководством и должны включать:

a) изменение сферы действия системы менеджмента ГИКТОНБ;

b) повышение эффективности системы менеджмента ГИКТОНБ;

c) пересмотренные требования ГИКТОНБ, включая определения услуг ИКТ, документально оформленный перечень критических услуг ИКТ и риски, связанные с расхождениями, выявленными между критическими возможностями готовности ИКТ и требованиями непрерывности бизнеса;

d) необходимую модификацию стратегии и процедур ГИКТОНБ, чтобы реагировать на внутренние и (или) внешние события, которые могут оказывать влияние на услуги ИКТ, включая изменения:

1) требований бизнеса;

2) требований устойчивости; и

3) уровней риска и (или) уровней принятия риска;

e) потребности в ресурсах; и

f) финансовые и бюджетные требования.

8.4 Измерение критериев эффективности готовности ИКТ

8.4.1 Мониторинг и измерение готовности ИКТ

Организация должна проводить мониторинг и измерение готовности ИКТ посредством реализации процесса измерения определенных критериев эффективности готовности ИКТ (см. 6.7).

8.4.2 Количественные и качественные критерии эффективности

Критерии эффективности для ГИКТОНБ могут быть качественными или количественными.

Количественные критерии могут включать:

a) число инцидентов за данный период времени, которые не были обнаружены до нарушения (это может служить показателем полноты механизмов обнаружения и предупреждения об опасности);

b) время обнаружения инцидентов;

c) число инцидентов, которое не может быть эффективно сдержано для уменьшения влияния;

d) доступность источников данных, указывающих на появление инцидентов посредством мониторинга тенденции событий; и

e) время противодействия и реагирования на обнаруженные возникшие инциденты.

Когда для определения эффективности ГИКТОНБ используются качественные критерии, они являются субъективными, но обычно требуют меньше ресурсов для процесса измерений (что может быть уместным для организаций небольшого или среднего размера, ограниченных в ресурсах). Они могут включать определение эффективности процессов, используемых в планировании, подготовке и выполнении деятельностей ГИКТОНБ, и измеряться путем:

a) анкетирования с использованием структурированных или неструктурированных анкет;

b) замечаний и предложений от участников и причастных сторон;

c) проведения семинаров по обмену опытом; и

d) других узкоспециализированных совместных совещаний.

9 Совершенствование ГИКТОНБ

9.1 Постоянное совершенствование

Организация должна постоянно совершенствовать ГИКТОНБ посредством применения предупреждающих и корректирующих мер, которые соответствуют потенциальному влиянию, определяемому анализом влияния на бизнес организации и ее готовности рисковать.

9.2 Корректирующие меры

Организация должна принимать меры по исправлению любых фактических отказов услуг ИКТ и элементов ГИКТОНБ. Документально оформленная процедура для корректирующих мер должна определять требования для:

a) идентификации отказов;

b) определения причин отказов;

c) оценивания потребности в действиях для обеспечения уверенности в том, что несоответствия не повторятся;

d) определения и реализации необходимых корректирующих мер;

e) фиксирования результатов принятых мер; и

f) проверки принятых корректирующих мер.

9.3 Предупреждающие меры

Организация должна определить потенциальные слабые места элементов ГИКТОНБ и установить документально оформленную процедуру для:

a) определения потенциальных отказов;

b) определения причин отказов;

c) определения и реализации необходимых предупреждающих мер; и

d) фиксирования и проверки результатов принятых мер.

Приложение А
(справочное)

ГИКТОНБ и контрольные точки во время нарушения

Рисунок А.1 иллюстрирует, как элементы ГИКТОНБ поддерживают ключевые контрольные точки во время серьезного нарушения. События и контрольные точки отмечены по шкале, начинающейся с момента возникновения аварийного события или события, нарушающего услуги ИКТ. Примером аварийного сценария является атака вторжения из специализированной системы (обычно называемой «хакерством») в критическую систему ИКТ организации.

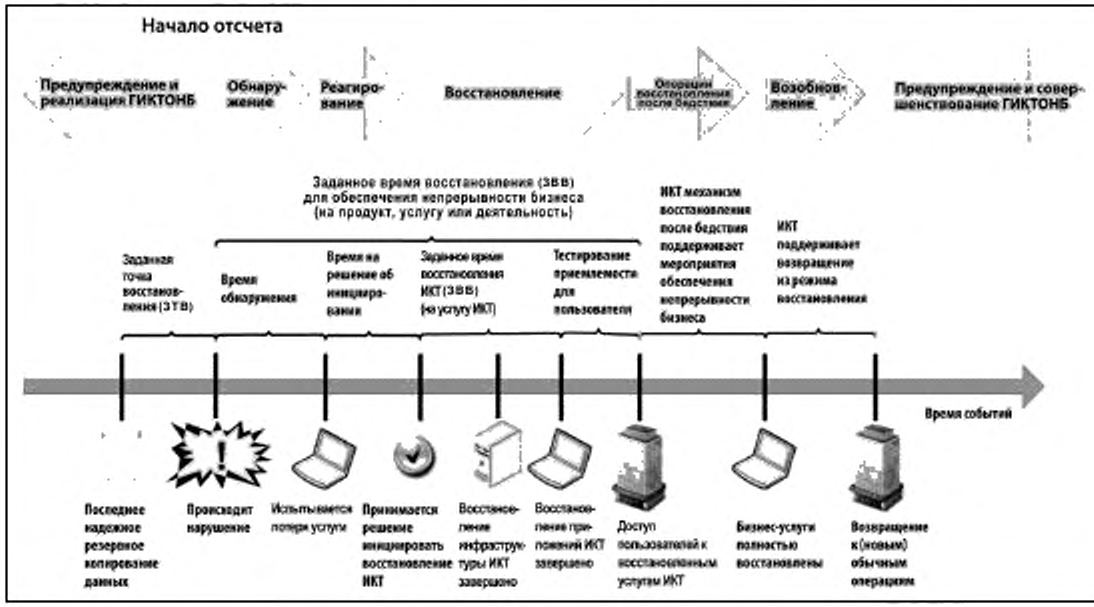

Рисунок А.1 – ГИКТОНБ и контрольные точки во время нарушения

Заданная точка восстановления (ЗТВ

промежутка времени между последним надежным резервным копированием и возникновением нарушения. Заданная точка восстановления зависит от используемой стратегии восстановления услуги ИКТ, особенно от плана резервирования.

Началом отсчета времени является вторжение хакера в критическую систему ИКТ и нарушение услуги. Первой контрольной точкой после возникновения нарушения услуг ИКТ является непосредственное обнаружение инцидента безопасности (т. е. событие вторжения) или

косвенное обнаружение потери (или ухудшения) услуги, до извещения о котором проходит какое-то время; например, в некоторых случаях извещение может осуществляться через звонок пользователя в службу технической поддержки.

Пока нарушение услуг ИКТ расследуется, анализируется, о нем сообщается и принимается решение активизировать ГИКТОНБ, может пройти дополнительное время. От начала нарушения услуг ИКТ до принятия решения об активизации ГИКТОНБ может пройти несколько часов, с учетом времени на информирование и на принятие решения. В некоторых ситуациях решение об активизации может требовать тщательного рассмотрения, например, когда услуга не полностью утрачена или кажется, что существуют серьезные предпосылки скорого восстановления услуги, потому что активизация ГИКТОНБ часто оказывает влияние на обычные операции бизнеса.

После активизации может начинаться восстановление услуг ИКТ. Оно может подразделяться на восстановление инфраструктуры (сеть, аппаратные средства, операционная система, программные средства резервного копирования и т. д.) и восстановление прикладных программ (базы данных, прикладные задачи, процессы пакетной обработки, интерфейсы и т. д.). (Дополнительную информацию см. в ИСО/МЭК 24762).

Когда услуга ИКТ восстановлена, и персоналом ИКТ проведено тестирование системы, услуга может быть предоставлена на тестирования приемлемости для пользователя, прежде чем будет передана персоналу для использования в операциях по обеспечению непрерывности бизнеса.

С точки зрения обеспечения непрерывности бизнеса, существует заданное время восстановления (ЗВВ) на продукт, услугу или вид деятельности, начиная с момента возникновения нарушения и до момента восстановления продукта, услуги или вида деятельности, но для обеспечения такой возможности может потребоваться ряд услуг ИКТ, и каждая из этих услуг ИКТ может содержать несколько систем или прикладных программ ИКТ. Каждая из этих составляющих систем или прикладных программ ИКТ будет иметь свое собственное заданное время восстановления, как составная часть общего заданного времени восстановления «сквозной» услуги ИКТ[1)], которое должно быть меньше, чем заданное время восстановления непрерывности бизнеса, учитывающее время обнаружения и принятия решения и время проведения пользовательской проверки применения (если только продукт, услуга или деятельность по обеспечению непрерывности бизнеса могут поддерживаться без ИКТ в течение какого-то периода, например, используя ручные процедуры).

Восстановленные услуги ИКТ обычно функционируют в течение какого-то периода времени, поддерживая деятельность по обеспечению непрерывности бизнеса, и, если это продолжительный период, то восстановленные услуги ИКТ могут потребовать расширения для поддержки

[1)] Услуга, в предоставлении которой (от источника до получателя) принимают участие несколько промежуточных компонентов ИКТ (примечание редактора).

увеличивающегося объема деятельности, возможно до момента полного восстановления продукта, услуги или деятельности до обычных объемов операций.

Впоследствии в определенный момент времени, восстановление будет выполнено, и операции по восстановлению после бедствия будут возвращены к «обычным» операциям. Возвращенные «обычные» операции могут служить либо исходным состоянием, либо средой до нарушения, либо новым операционным механизмом (особенно когда нарушение при бедствии вызвало долговременное изменение бизнеса).

Хотя персонал ИКТ имеет возможность тщательно планировать восстановление, чтобы оно происходило во время естественного периода низкой активности деятельности, тем не менее, это является сложной задачей, исходя из их возможностей.

Приложение В
(справочное)

Встраиваемые системы высокой доступности

В информационно-коммуникационных технологиях «высокая доступность» относится к системам или компонентам, которые непрерывно функционируют в течение желаемого длительного периода времени. Доступность может измеряться по отношению к «100 % работоспособности» или «полному отсутствию отказов». Существует широко распространенный, но труднодостижимый эталон доступности систем или продуктов, известный как «пять девяток» (99,999 %) доступности.

Компьютерная система или сеть состоит из многих компонентов, каждый из которых должен быть в наличии и быть функциональным, чтобы все в целом было работоспособным, и, хотя планирование высокой доступности часто сосредотачивается на резервировании, обработке отказа, хранении данных и доступе к ним, другие компоненты инфраструктуры, такие как энергоснабжение и охлаждение, являются в равной степени важными.

Например, доступность энергоснабжения может обеспечиваться с помощью таких мер, как:

a) источники бесперебойного питания (ИБП);

b) аварийные генераторы; и

c) дублирование источников энергоснабжения из энергосистемы.

Резервирование и доступность данных могут быть достигнуты при использовании разнообразных технологий хранения, таких как избыточные дисковые массивы (RAID – redundant array of disks), сеть хранения данных (SAN – storage area network) и т. д.

Доступность прикладных программ тоже требует рассмотрения и часто достигается посредством кластеризации.

Такие технологии могут быть реально эффективными в обеспечении высокой доступности только при одновременной реализации более чем в одном месте. Например, просто наличие «отказоустойчивого» сервера на той же площадке, что и основной или «рабочий» сервер, не обеспечит необходимого уровня устойчивости, если площадка будет затронута серьезным нарушением. Это нарушение окажет влияние на оба сервера. Чтобы могли быть достигнуты требуемые уровни доступности, «отказоустойчивый» сервер или другие поддерживающие технологии должны размещаться на другой площадке.

Для многих организаций расходы и усилия, связанные с достижением таких уровней высокой доступности, могут выглядеть пугающе, но в последние годы наблюдается значительный

рост использования услуг третьей стороны, которая может предложить навыки, ресурсы и устойчивые технологии по доступной цене путем предоставления управляемых или «облачных» услуг.

Однако следует помнить, что хотя высокая доступность является эффективным средством повышения устойчивости, возможность отказов все равно остается. Поэтому крайне важно наличие хорошо распланированных и протестированных процессов и процедур восстановления после бедствия.

Приложение С
(справочное)

Оценка сценариев отказов

С.1 Общая информация

Существует целый ряд возможных методов менеджмента риска, которые могут помочь в оценке готовности ИКТ к обеспечению непрерывности бизнеса и разработке соответствующей структуры для постоянного развития и совершенствования устойчивости ИКТ.

Стандарт ИСО 31010:2009 «Менеджмент риска. Методы оценки риска» (ISO/IEC 31010:2009 Risk management – Risk assessment techniques) предназначен для отражения современных лучших практических приемов выбора и использования методов оценки риска. К этому стандарту следует обращаться с целью определения наиболее соответствующего метода для использования в организации.

Оценка сценариев отказов является одним из методов, который может быть полезен для повышения эффективности ГИКТОНБ, и в этом приложении представлена дополнительная информация о том, как она может быть реализована.

С.2 Методика оценки

В период между оценками могут возникать проблемы неизвестного риска, как результат изменений во внутренней и внешней среде организации, которые могут препятствовать обеспечению непрерывности бизнеса и устойчивости. Целью оценки сценариев отказов является определение приемлемых индикаторов событий и обеспечение уверенности в том, что планы ГИКТОНБ предоставляют возможность обнаруживать такие возникающие аспекты риска и смогут подготовить организацию к обеспечению принятия соответствующих мер прежде, чем произойдет отказ.

Для этой цели доступен ряд специальных методик, включая анализ вида отказов и их влияния (FMEA – Failure Mode Effect Analysis) и анализ влияния отказа компонентов (CFIA – Component Failure Impact Analysis). С демонстрационной целью в этом приложении детально прорабатывается методика FMEA, в то же время организации следует выбирать методику, которая соответствует ее среде и структуре.

Анализ вида отказов и их влияния (FMEA) – это процесс определения и анализа возможных видов отказов системы с целью их классификации по степени серьезности или определения

влияния отказов на систему. В контексте настоящего стандарта FMEA может применяться для определения индикаторов критических событий, которые следует подвергать мониторингу с целью обнаружения серьезных видов отказов в системе ИКТ организации. Процесс, основанный на подходе FMEA, может применяться к каждому критическому компоненту услуг ИКТ, как описано в 6.3.2.

Для каждого критического компонента:

a) определяется возможный вид отказа;

b) устанавливается возможное влияние на услугу ИКТ, т. е. серьезность каждого вида отказа и последствия, которые он будет иметь;

c) определяется ранее испытываемая организацией частота возникновения вида отказа, а также простота его мониторинга и обнаружения;

d) определяются индикаторы, которые будут сигнализировать или информировать об отказе компонента;

e) определяются прямые и косвенные события, которые связаны между собой и будут изменять состояние каждого индикатора;

f) определяются существующие меры и средства контроля и управления, которые предотвращают отказ критических компонентов или могут обнаруживать возникновение таких отказов;

g) определяются взаимосвязанные источники данных и возможные методы мониторинга для обнаружения изменений значения индикатора; индикаторы событий группируются по доступности методов и простоте мониторинга; и

h) определяется возможность применения соответствующих мер и средств контроля и управления для снижения или устранения риска, чтобы предотвратить его повторное появление.

С.3 Результат оценки

Выходные данные FMEA включают список возможных видов отказов и их влияния, взаимосвязанные события и могут использоваться для определения индикаторов событий, требующих мониторинга.

Виды отказов, определенные с помощью процесса FMEA, могут быть расставлены согласно приоритетам в соответствии с оцененной серьезностью, частотой возникновения и простотой мониторинга и обнаружения.

FMEA также документирует текущие знания и меры в отношении рисков отказов для использования в процессе постоянного совершенствования. Если FMEA используется на этапе проектирования, чтобы избежать будущих отказов, то он может использоваться для управления до

и во время текущего функционирования процесса. В идеале FMEA начинается на самом раннем (концептуальном) этапе проектирования и продолжается в течение жизненного цикла продукта или услуги.

Приложение D
(справочное)

Разработка критериев эффективности

Поскольку эффективность ГИКТОНБ различается в разных организациях, каждая организация должна разработать собственные критерии эффективности ГИКТОНБ и поддерживать их как часть процесса постоянного совершенствования.

Основной подход состоит в использовании известных сценариев инцидентов и взаимосвязанных событий, чтобы установить базовый уровень реагирования для каждой категории инцидентов и связанных с ними событий следующим образом:

a) установление в рамках процессов МНБ и СМИБ известных инцидентов и индикаторов событий в качестве входных данных для последующих этапов;

b) установление совокупности известных инцидентов (например, атака взлома пароля, отказ сервера из-за недостатка места на жестком диске);

c) определение событий, ведущих к этим инцидентам (например, неудачная попытка входа в систему, использование жесткого диска);

d) определение соответствующего времени обнаружения (например, пороговое значение для событий, о которых должны быть уведомлены/предупреждены система/администратор);

e) определение соответствующего времени реагирования (например, период времени для принятия администратором мер с целью предотвращения реализации инцидента);

f) распределение событий по группам, исходя из требуемого времени реагирования и видов мер реагирования; события могут распределяться по группам угроз, группам прикладных программ, группам мер реагирования и (или) группам времени реагирования;

g) уточнение матриц и значений посредством тестирования сценариев и учений/тренировок;

h) проведение тестирования для определения того, являются ли меры реагирования осуществимыми, а цели достижимыми;

i) уточнение групп ожидаемого времени реагирования на событие и ожидаемых мер реагирования на события (например, поиск альтернативного метода мониторинга, обнаружения и действий);

j) совершенствование путем сбора информации о новых инцидентах и сценариях отказа и повторение процесса.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ИСО/МЭК 24762:2008	MOD	ГОСТ Р 53131—2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности»
ИСО/МЭК ТО 18044:2004	IDT	ГОСТ Р ИСО/МЭК ТО 18044—2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности»
ИСО/МЭК 27000	—	*
ИСО/МЭК 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002—2011 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
ИСО/МЭК 27005:2008	IDT	ГОСТ Р ИСО/МЭК 27005—2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
ИСО/МЭК 18043:2006	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание – В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

– IDT — идентичные стандарты;

– MOD — модифицированные стандарты.

Библиография

1 SS 540:2008, Singapore Standard for Business Continuity Management.

2 BS 25999-1:2006, Business Continuity Management – Part 1: Code of practice.

3 ISO 9000:2005, Quality management systems – Fundamentals and vocabulary (ИСО 9000:2005 Системы менеджмента качества. Основные положения и словарь). *

4 ISO/IEC 18043:2006, Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (ИСО/МЭК 18043:2006 Информационные технологии. Методы защиты. Выбор, применение и операции систем обнаружения вторжения). *

5 ISO/IEC 20000-1:2005, Information technology – Service management – Part 1: Specification (ИСО/МЭК 20000-1:2005 Информационные технологии. Менеджмент услуг. Часть 1. Технические требования). *

6 ISO/IEC 20000-2:2005, Information technology – Service management – Part 2: Code of practice (ИСО/МЭК 20000-2:2005 Информационные технологии. Менеджмент услуг. Часть 2. Свод установленных правил). *

7 ISO 22301, Societal security – Preparedness and continuity management systems – Requirements.

8 ISO/IEC 24762:2008, Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services (ИСО/МЭК 24762:2008 Информационная технология. Методы и средства обеспечения безопасности. Руководство по услугам по восстановлению информационно-коммуникационных технологий после бедствия). *

9 ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance.

10 ISO/IEC 27004, Information technology – Security techniques – Information security management – Measurement (ИСО/МЭК 27004:2009 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения). *

11 ISO 31010:2009, Risk management – Risk assessment techniques.

---

* Официальный перевод этого международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

УДК 001.4:025.4:006.354 ОКС 35.040

Ключевые слова: информационная технология, информационно-коммуникационная технология, услуга, мера и средство контроля и управления, менеджмент, непрерывность бизнеса, готовность к непрерывности бизнеса, планирование готовности, стратегия готовности, эффективность готовности, мониторинг

Подписано в печать 30.04.2014. Формат 60x84 1/8.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

www.gostinfo.ru info@gostinfo.ru