



Информационно-методическое пособие предназначено руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), внутренним и внешним аудиторам (CISA), менеджерам высшего эшелона компаний, ответственным за обеспечение непрерывности бизнеса, а также преподавателям и слушателям программ MBA, CIO и CSO, студентам и аспирантам соответствующих специальностей.

Введение

Глава 1. Актуальность и основы корпоративной программы ВСМ

1.1. Мотивация и преимущества обеспечения непрерывности бизнеса

- 1.1.1. Примеры инцидентов
- 1.1.2. Основные мотивы внедрения корпоративной программы ВСМ
- 1.1.3. Экономическая целесообразность ВСМ
- 1.1.4. Дополнительные преимущества

1.2. Основы управления непрерывностью бизнеса

- 1.2.1. История вопроса
- 1.2.2. Содержание ВСМ
- 1.2.3. Практика ВСМ

1.3. Постановка задачи построения ВСР

- 1.3.1. Цель и задачи работы
- 1.3.2. Ожидаемый эффект
- 1.3.3. Требования к разработке
- 1.3.4. Требования к составу работ
- 1.3.5. Требования к отчетным материалам
- 1.3.6. Продолжительность работ
- 1.3.7. Область реализации
- 1.3.8. Дополнительные требования
- 1.3.9. Квалификационные требования к исполнителю

1.4. Анализ технологий

- 1.4.1. Классификация уровня поставленной задачи
- 1.4.2. Общие подходы и направления
- 1.4.3. Инфраструктура ЦОД
- 1.4.4. Мультисервисная сеть
- 1.4.5. Помещения и инженерные системы
- 1.4.6. Обеспечение непрерывности функционирования программного обеспечения
- 1.4.7. Система управления и мониторинга

Глава 2. Лучшая практика управления непрерывностью бизнеса

2.1. Практика ВС

2.2. Практика DRII

2.3. Практика SANS

- Этап 1: Инициация проекта
- Этап 2: Анализ рисков – Risk Analysis (RA)
- Этап 3: Анализ воздействия на бизнес – Business Impact Analysis (BIA)
- Этап 4: Разработка плана BCP/DRP
- Этап 5: Тестирование плана BCP/DRP
- Этап 6: Сопровождение плана BCP/DRP
- Этап 7: Утверждение и внедрение плана BCP/DRP

2.4. Стандарт BS25999

- Этап 1. Управление программой ВСМ
- Этап 2. Анализ требований к программе ВСМ
- Этап 3. Определение стратегии ВСМ

- Этап 4. Разработка и реализация планов BCM
- Этап 5. Поддержка и сопровождение программы BCM
- Этап 6. Формирование культуры BCM в организации

2.5. Стандарт NB 292:2006

2.6. Практика управления рисками

NIST SP 800-30; OCTAVE; MG-2; CobIT; SA-CMM

2.7. Практика описания бизнес-процессов

Практика моделирования процессов
Методология NGOSS

2.8. Стандарт COBIT

2.9. Библиотека ITIL

- Этап 1. Инициация процесса ITSCM
- Этап 2. Анализ требований и выработка стратегии ITSCM
- Этап 3. Внедрение ITSCM
- Этап 4. Операционное управление
- Дополнительные вопросы обеспечения процесса ITSCM

2.10. Стандарт ISO/IEC 27002:2005 (BS ISO/IEC 17799:2005)

- Аспекты управления непрерывностью бизнеса
- Место и роль информационной безопасности
- Непрерывность бизнеса и оценка рисков
- Разработка и внедрение Плана непрерывности бизнеса
- Структура Плана непрерывности бизнеса
- Поддержка и сопровождение Плана непрерывности бизнеса

2.11. Отечественная практика BCM

Глава 3. Лучшие практики разработки ЕСР

3.1. Практика Accenture

- Этап сбора сведений об ИТ-рисках в части BCM
- Этап разработки стратегии управления непрерывностью бизнеса
- Этап внедрения стратегии BCM

3.2. Практика Ernst&Young

- Этап 1. Оценка зрелости корпоративной программы ЕСР
- Этап 2. Разработка стратегии обеспечения непрерывности бизнеса
- Этап 3. Реализация стратегии обеспечения непрерывности бизнеса

3.3. Практика IBM

- Методы выполнения работ
- Подход IBM BCRS
- Услуги IBM BCRS
- Пример выбора решения
- Пример постановки задачи

3.4. Практика Hewlett-Packard

- Этап 1. Оценка текущего состояния ЕСР
- Этап 2. Разработка стратегии управления непрерывностью бизнеса
- Этап 3. Внедрение стратегии управления непрерывностью бизнеса

3.5. Практика EMC

3.6. Практика Microsoft

Глава 4. Примеры разработки программы ЕСР

4.1. Описание объекта

- 4.1.1. Текущая архитектура объекта
- 4.1.2. Целевая архитектура объекта

4.2. Пример оценки воздействия на бизнес, VIA

- 4.2.1. Основные цели и задачи VIA

- 4.2.2. Методика BIA
- 4.2.3. Определение ИТ-услуг
- 4.2.4. Определение ИТ-ресурсов
- 4.2.5. Анализ рисков и сценариев нарушения непрерывности сервиса
- 4.2.6. Определение зависимых бизнес-сервисов
- 4.2.7. Определение требований к параметрам доступности ИТ-ресурсов

4.3. Пример стратегии непрерывности бизнеса

- 4.3.1. Заявление Руководства (Политика в области непрерывности бизнеса)
- 4.3.2. Методика выработки стратегии обеспечения непрерывности
- 4.3.3. Методика расчета временных показателей процесса восстановления ИТ-ресурса
- 4.3.4. Перечень общих технических решений для ИТ-ресурсов
- 4.3.5. Описание частных технических решений для ИТ-ресурсов
- 4.3.6. Анализ вариантов стратегий непрерывности для ИТ-ресурсов
- 4.3.7. Оценка состояния процесса обеспечения непрерывности для ИТ-сервисов
- 4.3.8. Описание частных технических решений для ИТ-сервисов
- 4.3.9. Анализ вариантов стратегий размещения серверной площадки
- 4.3.10. Анализ вариантов стратегий непрерывности для ИТ-сервисов
- 4.3.11. Описание частных технических решений обеспечения непрерывности бизнеса
- 4.3.12. Анализ вариантов стратегий непрерывности бизнеса
- 4.3.13. Принятые решения

4.4. Пример разработки Плана непрерывности бизнеса, ВСП

- 4.4.1. Цель и подход к созданию плана обеспечения непрерывности
- 4.4.2. Задачи плана обеспечения непрерывности
- 4.4.3. Состав плана ВСП
- 4.4.4. Управление планом ВСП
- 4.4.5. Аварийно-восстановительная команд
- 4.4.6. Резервные центры управления
- 4.4.7. Мероприятия по обеспечению непрерывности

4.5. Пример Плана тестирования ВСП

- 4.5.1. Цель тестирования
- 4.5.2. Задачи тестирования
- 4.5.3. Виды тестов плана ВСП
- 4.5.4. Программа тестирования
- 4.5.5. Методика процесса тестирования
- 4.5.6. Пример настольного теста плана ВСП
- 4.5.7. Пример частичного теста плана ВСП

Заключение

Приложение

Приложение 1. Непрерывность бизнеса и акт Сарбэйнса-Оксли

Приложение 2. План действий Мининформсвязи России в кризисных ситуациях

Приложение 3. Перечень возможных инструкций для надлежащего обеспечения непрерывностью бизнеса

Приложение 4. Пример представления контактных данных для ВСМ

Приложение 4.1. АВК: контактная информация и лист ознакомления

Приложение 4.2. Контактная информация ключевых служб Компании

Приложение 4.3. Контактная информация поставщиков оборудования и услуг

Список литературы



Стандарты информационной безопасности

- 1. ISO/IEC FDIS 27001:2005 (англ.)
- 2. ISO/IEC FDIS 27001:2005 (перевод на русский язык)
- 3. BS ISO/IEC 17799:2005 (англ.)
- 4. ГОСТ Р ИСО/МЭК 27001
- 5. ГОСТ Р ИСО/МЭК 17799