

Содержание

| | |
|---|-----------|
| Предисловие Председателя совета директоров группы компаний «АйТи» Тагира Яппарова..... | 9 |
| Предисловие директора Business Continuity Institute (BCI) Линдона Бирда..... | 11 |
| Введение..... | 14 |
| Глава 1. АКТУАЛЬНОСТЬ УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА..... | 21 |
| 1.1. Мотивация и преимущества ВСМ..... | 21 |
| 1.1.1. Примеры инцидентов..... | 22 |
| 1.1.2. Основные мотивы..... | 25 |
| 1.1.3. Экономическая целесообразность..... | 31 |
| 1.1.4. Дополнительные преимущества..... | 32 |
| 1.2. Основные компоненты программы ЕСР..... | 33 |
| 1.2.1. История вопроса..... | 34 |
| 1.2.2. Содержание ВСМ..... | 35 |
| 1.2.3. Практика ВСМ..... | 37 |
| 1.3. Постановка задачи построения ВСР..... | 46 |
| 1.3.1. Цель и задачи работы..... | 46 |
| 1.3.2. Ожидаемый эффект..... | 47 |
| 1.3.3. Требования к разработке..... | 48 |
| 1.3.4. Требования к составу работ..... | 51 |
| 1.3.5. Требования к отчетным материалам..... | 52 |
| 1.3.6. Продолжительность работ..... | 53 |
| 1.3.7. Область реализации..... | 53 |
| 1.3.8. Дополнительные требования..... | 53 |
| 1.3.9. Квалификационные требования к Исполнителю..... | 53 |
| 1.4. Анализ технологий..... | 54 |
| 1.4.1. Классификация уровня поставленной задачи..... | 54 |
| 1.4.2. Общие подходы и направления..... | 56 |
| 1.4.3. Инфраструктура ЦОД..... | 57 |
| 1.4.4. Мультисервисная сеть..... | 66 |
| 1.4.5. Помещения и инженерные системы..... | 71 |
| 1.4.6. Обеспечение непрерывности функционирования программного обеспечения..... | 74 |
| 1.4.7. Системы мониторинга и управления..... | 77 |
| Глава 2. ЛУЧШИЕ ПРАКТИКИ УПРАВЛЕНИЯ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА..... | 80 |
| 2.1. Практика ВСИ..... | 82 |

| | |
|---|-----|
| 2.1.1. Характеристика деятельности..... | 82 |
| 2.1.2. Основные достижения..... | 83 |
| 2.2. Практика института DRII..... | 86 |
| 2.2.1. Направления деятельности..... | 86 |
| 2.2.2. Модель DRII..... | 86 |
| 2.3. Практика SANS..... | 89 |
| 2.3.1. Инициация проекта..... | 90 |
| 2.3.2. Анализ рисков – Risk Analysis (RA)..... | 92 |
| 2.3.3. Анализ воздействия на бизнес – Business Impact Analysis (BIA)..... | 94 |
| 2.3.4. Разработка планов BCP&DRP..... | 95 |
| 2.3.5. Тестирование планов BCP&DRP..... | 97 |
| 2.3.6. Сопровождение планов BCP&DRP..... | 99 |
| 2.3.7. Утверждение и внедрение планов BCP&DRP..... | 100 |
| 2.4. Стандарт BS25999 (PAS 56)..... | 100 |
| 2.4.1. Управление программой BCM..... | 102 |
| 2.4.2. Анализ требований к программе BCM..... | 103 |
| 2.4.3. Определение стратегии BCM..... | 105 |
| 2.4.4. Разработка и реализация планов BCM..... | 106 |
| 2.4.5. Поддержка и сопровождение программы BCM..... | 108 |
| 2.4.6. Формирование культуры BCM в организации..... | 109 |
| 2.5. Стандарт AS/NZS 5050 (NB 292:2006)..... | 109 |
| 2.5.1. Рекомендации стандарта..... | 110 |
| 2.5.2. Особенности BCM..... | 112 |
| 2.6. Практика управления рисками..... | 116 |
| 2.6.1. Стандарт NIST SP 800-30..... | 119 |
| 2.6.2. Методология OCTAVE..... | 121 |
| 2.6.3. Жизненный цикл MG-2..... | 124 |
| 2.6.4. Стандарт CobIT..... | 125 |
| 2.6.5. Модель зрелости SA-CMM..... | 125 |
| 2.7. Практика описания бизнес-процессов..... | 127 |
| 2.7.1. Практика моделирования процессов..... | 129 |
| 2.7.2. Методология NGOSS..... | 131 |
| 2.8. Стандарт COBIT..... | 139 |
| 2.8.1. Характеристика стандарта..... | 140 |
| 2.8.2. Процесс DS4..... | 142 |
| 2.8.3. Уровни зрелости DS4..... | 146 |
| 2.9. Библиотека ITIL..... | 148 |
| 2.9.1. Инициация процесса ITSCM..... | 151 |
| 2.9.2. Анализ требований и выработка стратегии ITSCM..... | 152 |
| 2.9.3. Внедрение ITSCM..... | 154 |
| 2.9.4. Операционное управление..... | 157 |
| 2.9.5. Дополнительные вопросы..... | 158 |
| 2.10. Стандарт ISO/IEC 27002:2005 (BS ISO/IEC 17799:2005)..... | 160 |
| 2.10.1. Аспекты управления непрерывностью бизнеса..... | 161 |
| 2.10.2. Взаимосвязь непрерывности и безопасности..... | 162 |

| | |
|---|------------|
| 2.10.3. Непрерывность бизнеса и оценка рисков..... | 163 |
| 2.10.4. Разработка и внедрение Плана непрерывности бизнеса..... | 163 |
| 2.10.5. Структура Плана непрерывности бизнеса..... | 164 |
| 2.10.6. Поддержка и сопровождение Плана непрерывности бизнеса..... | 165 |
| 2.11. Отечественная практика ВСМ..... | 168 |
| 2.11.1. Развитие практики ВСМ..... | 168 |
| 2.11.2. Инициативы Банка России..... | 168 |
| Глава 3. УПРАВЛЕНИЕ ПРОЕКТАМИ В ОБЛАСТИ ВСМ..... | 181 |
| 3.1. Практика Accenture..... | 181 |
| 3.1.1. Определение рисков..... | 184 |
| 3.1.2. Разработки стратегии ВСМ..... | 191 |
| 3.1.3. Внедрение стратегии ВСМ..... | 198 |
| 3.2. Практика Ernst&Young..... | 201 |
| 3.2.1. Оценка зрелости программы ЕСР..... | 209 |
| 3.2.2. Разработка стратегии ВСМ..... | 217 |
| 3.2.3. Внедрение стратегии ВСМ..... | 220 |
| 3.3. Практика IBM..... | 221 |
| 3.3.1. Методы выполнения работ..... | 222 |
| 3.3.2. Подход IBM BCRS..... | 224 |
| 3.3.3. Услуги IBM BCRS..... | 228 |
| 3.3.4. Пример выбора решения..... | 237 |
| 3.3.5. Пример постановки задачи..... | 245 |
| 3.4. Практика Hewlett-Packard..... | 251 |
| 3.4.1. Оценка текущего состояния ЕСР..... | 254 |
| 3.4.2. Разработка стратегии ВСМ..... | 262 |
| 3.4.5. Внедрение стратегии ВСМ..... | 264 |
| 3.5. Практика EMC..... | 267 |
| 3.5.1. Виды работ..... | 267 |
| 3.5.2. Методология EMC..... | 271 |
| 3.6. Практика Microsoft..... | 276 |
| 3.6.1. Характеристика подхода..... | 278 |
| 3.6.2. Функция ИТСМ..... | 282 |
| Глава 4. ПРИМЕРЫ РАЗРАБОТКИ ПРОГРАММЫ ЕСР..... | 284 |
| 4.1. Описание объекта..... | 284 |
| 4.1.1. Текущая архитектура объекта..... | 285 |
| 4.1.2. Целевая архитектура объекта..... | 285 |
| 4.2. Пример оценки воздействия на бизнес, ВИА..... | 287 |
| 4.2.1. Основные цели и задачи ВИА..... | 287 |
| 4.2.2. Методика ВИА..... | 287 |
| 4.2.3. Определение ИТ-услуг..... | 288 |
| 4.2.4. Определение ИТ-ресурсов..... | 288 |
| 4.2.5. Анализ рисков и сценариев нарушения непрерывности сервиса..... | 290 |
| 4.2.6. Определение зависимых бизнес-сервисов..... | 300 |

| | |
|--|------------|
| 4.2.7. Определение требований к параметрам доступности ИТ-ресурсов..... | 300 |
| 4.3. Пример стратегии непрерывности бизнеса..... | 300 |
| 4.3.1. Заявление Руководства (Политика в области непрерывности бизнеса)..... | 303 |
| 4.3.2. Методика выработки стратегии обеспечения непрерывности..... | 303 |
| 4.3.3. Методика расчета временных показателей процесса восстановления ИТ-ресурса..... | 303 |
| 4.3.4. Перечень общих технических решений для ИТ-ресурсов..... | 308 |
| 4.3.5. Описание частных технических решений для ИТ-ресурсов..... | 309 |
| 4.3.6. Анализ вариантов стратегий непрерывности для ИТ-ресурсов..... | 312 |
| 4.3.7. Оценка состояния процесса обеспечения непрерывности для ИТ-сервисов..... | 318 |
| 4.3.8. Описание частных технических решений для ИТ-сервисов..... | 320 |
| 4.3.9. Анализ вариантов стратегий размещения серверной площадки..... | 320 |
| 4.3.10. Анализ вариантов стратегий непрерывности для ИТ-сервисов..... | 322 |
| 4.3.11. Описание частных технических решений обеспечения непрерывности бизнеса..... | 322 |
| 4.3.12. Анализ вариантов стратегий непрерывности бизнеса..... | 324 |
| 4.3.13. Принятые решения..... | 324 |
| 4.4. Пример разработки Плана непрерывности бизнеса, ВСР..... | 325 |
| 4.4.1. Цель и подход к созданию плана обеспечения непрерывности..... | 325 |
| 4.4.2. Задачи плана обеспечения непрерывности..... | 326 |
| 4.4.3. Состав плана ВСР..... | 326 |
| 4.4.4. Управление планом ВСР..... | 327 |
| 4.4.5. Аварийно-восстановительная команда..... | 328 |
| 4.4.6. Резервные центры управления..... | 334 |
| 4.4.7. Мероприятия по обеспечению непрерывности..... | 335 |
| 4.5. Пример Плана тестирования ВСР..... | 341 |
| 4.5.1. Цель тестирования..... | 341 |
| 4.5.2. Задачи тестирования..... | 341 |
| 4.5.3. Виды тестов плана ВСР..... | 341 |
| 4.5.4. Программа тестирования..... | 343 |
| 4.5.5. Методика процесса тестирования..... | 343 |
| 4.5.6. Пример настольного теста плана ВСР..... | 345 |
| 4.5.7. Пример частичного теста плана ВСР..... | 347 |
| Заключение..... | 351 |
| Приложение 1. Непрерывность бизнеса и акт Сарбэйнса-Оксли..... | 355 |
| Приложение 2. План действий Мининформсвязи России в кризисных ситуациях..... | 369 |
| Приложение 3. Перечень возможных инструкций для надлежащего обеспечения непрерывностью бизнеса..... | 374 |
| Приложение 4. Пример представления контактных данных для ВСМ..... | 375 |

Введение

“Тот, кто не закладывает фундамент изначально, может огромными усилиями сделать это затем... Но с большой сложностью для архитектора и опасностью для строения”.

Пикколо Макиавелли, XV век

Понятие «управление непрерывностью бизнеса» (*BCM—Business Continuity Management*) появилось сравнительно недавно и сегодня вызывает постоянный интерес у топ-менеджеров отечественных компаний. Примерно с 1988 года в ряде высокотехнологичных стран мира, главным образом в Великобритании, США, Австралии и Японии, проводятся ежегодные слушания и совещания специально созданных комитетов и комиссий по вопросам управления непрерывностью бизнеса. Подготовлено более десятка различных национальных стандартов и спецификаций, посвященных управлению непрерывностью бизнеса, среди которых наибольшую известность приобрели: *BS25999 (PAS 56)*, *ASIS SPC.1-2009*, *ISO/DIS 22399:2008*, *ISO/IEC 22301:2008*, *NIST SP800-34*, *NFPA 1600*, *CSA Z1600*, *AS/NZS 5050 (HB 292:2006)*, *SS540:2009 (TR19:2004)*, *SI 24001:2007*, *ISO/IEC 27002:2005 (BS ISO/IEC 17799:2005) (14 раздел)*, *High Level Principles for Business Continuity (2006)*, *COBIT*, *ITIL* и *MOF* в части *BCM* и др.

В настоящее время управление непрерывностью бизнеса представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента современного предприятия. Актуальность этого направления для каждой отечественной компании объясняется необходимостью обеспечить выживание и сохранение своего бизнеса в чрезвычайных ситуациях. Под термином управление непрерывностью бизнеса обычно понимается системный процесс оценки последствий возникших чрезвычайных ситуаций и принятия надлежащих решений по сохранению бизнеса компании. Поэтому основной целью соответствующих *корпоративных программ управления непрерывностью бизнеса (ECP – Enterprise Continuity Program)* является минимизация риска потери бизнеса в случае его прерывания и продолжение деятельности компании в чрезвычайных ситуациях.

В России практика разработки и внедрения корпоративных программ *ECP* только зарождается. В лучшую сторону здесь выделяются инициативы Банка России, который на основе рекомендаций 14 раздела *ISO/IEC 27002:2005 (BS ISO/IEC 17799:2005)* подготовил соответствующий раздел 8.11 *СТО БР ИББС-1.0-2008*, а затем на основе документа Базельского комитета по банковскому надзору (*High Level Principles for Business Continuity*) – Пункт 3.7

Положения Банка России от 16 декабря 2003 г. №242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» (обновлен в соответствии с Указанием от 5 марта 2009 г. №2194-У «О внесении изменений в Положение Банка России от 16 декабря 2003 г. №242-П»).

В тоже время в Европе и США внедрение и поддержка упомянутых корпоративных программ идет полным ходом, а в некоторых государственных и коммерческих структурах вопросам управления непрерывностью бизнеса уделяется самое пристальное внимание. Например, федеральные департаменты США осуществляют планирование непрерывности своей деятельности в соответствии с утвержденными директивами *COOP*. В финансовой области вопросы обеспечения непрерывности бизнеса американских компаний регулируются рекомендациями законов *Gramm-Leach-Bliley*, *The Expedited Funds Availability*, а также рекомендациями стандарта *SAS 78/94*. В области здравоохранения руководящим документом в части ВСМ является *HIPAA*. Кроме того, для большинства компаний поставщиков услуг первой необходимости (электроэнергия, вода, газ, связь и пр.) при использовании процедур непрерывности бизнеса предусмотрены определенные льготы со стороны государства. Дело в том, что непрерывность деятельности этих компаний играет важную роль в обеспечении непрерывности функционирования различных федеральных организаций и структур (больниц, полиции, пожарных, школ и правительственных учреждений), а также крупных коммерческих структур (банков, финансовых организаций, страховых компаний, Интернет-провайдеров и пр.). На западе наиболее активными пользователями *Планов непрерывности бизнеса (BCP – Business Continuity Plan)* являются различные финансовые институты и организации, предприятия сырьевой и нефтеперерабатывающей промышленности, авиакомпания, телекоммуникационные компании и пр. Для многих из них еще свежи в памяти недавние трагические события, такие как террористические атаки в сентябре 2001 года в Нью-Йорке на World Trade Center и отключения электроэнергии в Северо-восточной части США и Юго-восточной части Канады в 2003-2009 гг. Эти события убедительно показали, что только те компании, которые своевременно воспользовались рекомендациями по обеспечению непрерывности бизнеса, смогли избежать крупных финансовых потерь и сохранить свой бизнес. Остальные же компании понесли существенные финансовые потери и некоторые даже потеряли свой бизнес. Поэтому компании постоянно совершенствуют свои *Планы непрерывности бизнеса (Business Continuity Plan)* и его различные производные: *аварийный план (Business Crash Plan)*, *чрезвычайный план (Business Disaster Plan)*, *антитеррористический план*, *антибомбовый план*, *план продолжения (Business Contingency Plan)*, *план восстановления (Business Recovery Plan)*, *антикризисный план* и пр.

Для отечественных компаний вопросы обеспечения непрерывности бизнеса сегодня также актуальны и своевременны. В России вероятность техногенных и природных катастроф достаточно высока, спектр угроз безопасности бизнеса постоянно растет, чрезвычайные ситуации возникают, чуть ли не ежедневно. Например, взрывы на крупнейшей угольной шахте в России «Распадская» 8-9 мая 2010 года, атаки террористов в Москве и Дагестане весной 2010 года,

авария на крупнейшей в России Саяно-Шушенской ГЭС 17 августа 2009 года, энергетический кризис в Москве 25 мая 2005 года и пр. Поэтому в каждой отечественной компании наверняка задавались вопросами:

1. Какие существуют нормативно-методические указания и требования по обеспечению непрерывности бизнеса? Как правильно организовать работы в рамках этой деятельности?
2. Как правильно создать и внедрить экономически оправданную корпоративную программу управления непрерывностью бизнеса?
3. Какой вид решений или услуг ВСМ лучше всего соответствует потребностям нашей компании?
4. Должна ли наша компания сама создавать и поддерживать Планы непрерывности и восстановления бизнеса или достаточно заключить соответствующий договор с консалтинговой компанией?
5. Какие инструментальные средства существуют для автоматизации планирования и управления непрерывностью бизнеса?
6. Каким образом контролировать управление непрерывностью бизнеса?
7. Как оценить затраты на поддержание и сопровождение корпоративной программы управления непрерывностью бизнеса?

Ответы на эти и многие другие вопросы позволяют создать и внедрить по-настоящему действенную и экономически эффективную *корпоративную программу управления непрерывностью бизнеса (ECP – Enterprise Continuity Program)*. При этом сделать упомянутую программу «прозрачной» и понятной как для руководства и рядовых сотрудников, так и для партнеров по бизнесу и клиентов компании.

Таблица 1. Этапы жизненного цикла корпоративной программы ECP

| Этапы жизненного цикла корпоративной программы ECP | Возможные шаги компании |
|---|--|
| Этап 1: Анализ требований к обеспечению непрерывности бизнеса | |
| <p>Необходимо:</p> <ul style="list-style-type: none"> ◇ Провести анализ критически важных бизнес-процессов компании и поддерживающей инфраструктуры. ◇ Выявить и верифицировать актуальные угрозы и уязвимости бизнес-процессов. ◇ Оценить основные риски (RA) бизнес-процессов. ◇ Оценить потенциальные финансовые убытки в случае возникновения чрезвычайных ситуаций. | <p>Результаты:</p> <ul style="list-style-type: none"> ◇ Методика оценки и ранжирования критически важных бизнес-процессов компании. ◇ Методика верификации угроз и уязвимостей бизнес-процессов компании. ◇ Методика оценивания рисков. ◇ Отчет RA с анализом рисков и приоритетами и первоочередными задачами обеспечения непрерывности бизнеса. ◇ Методика оценки ущерба в случае чрезвычайных ситуаций. |

| | |
|---|--|
| <ul style="list-style-type: none"> ◇ Закупить необходимые инструментальные средства поддержки ВСР. ◇ Установить и настроить инструментальные средства поддержки ВСР. ◇ Выработать систему оповещения о корректировке и внесении изменений в ВСР. ◇ Разработать контрольные тесты эффективности планов непрерывности бизнеса и график контрольных проверок. ◇ Выработать формальные критерии оценивания проводимых проверок ВСР. ◇ Разработать порядок внесения изменений в ВСР. | <ul style="list-style-type: none"> ◇ Спецификации регламентов поддержки ВСР. ◇ Схемы оповещений о вносимых изменениях. ◇ Методика тестирования и верификации ВСР. ◇ Формальные критерии оценивания ВСР представления результатов тестирования. ◇ Отчеты о тестировании планов ВСР. ◇ Инструкция о порядке внесения изменений в ВСР. ◇ Руководства по сопровождению и поддержке непрерывности бизнеса. |
|---|--|

Зарождающийся первый опыт использования корпоративных программ ЕСР в отечественных компаниях выявил следующие проблемы:

- ◇ отсутствие у ряда российских компаний вообще какого-либо рода *Политик, Стратегий, Планов и процедур непрерывности и восстановления бизнеса в чрезвычайных ситуациях*;
- ◇ недостаточная системная проработка предметной области, и как следствие акцент на аварийное восстановление ИТ-сервисов и слабое освещение критически важных бизнес-процессов, в том числе сервисов, предоставляемых клиентам и партнерам;
- ◇ отсутствие формализованного описания бизнес-процессов с указанием ответственных лиц и как следствие трудности в определении допустимого времени восстановления и оптимальной точки восстановления;
- ◇ нерегулярный и/или неполный анализ внешних и внутренних воздействий на критические важные бизнес-процессы компании, что приводит к тому, что планы непрерывности бизнеса не всегда отвечают целям и задачам бизнеса, не говоря уже о неадекватных расходах на планирование и поддержание непрерывности бизнеса; упомянутый анализ должен проводиться регулярно, предшествовать разработке стратегий обеспечения непрерывности и восстановления, и затрагивать все критически важные бизнес-процессы компании;
- ◇ использование морально устаревших методик и подходов к планированию и управлению непрерывностью бизнеса, слабо адаптированных под требования отечественного и международного законодательства в области ВСМ и соответствующих регулирующих государственных органов;
- ◇ недостаточный уровень подготовки сотрудников компании по вопросам уп-

равления непрерывности бизнеса, недостаток соответствующих знаний и навыков действия в чрезвычайных ситуациях.

Предлагаемая вашему вниманию книга позволит своевременно устранить отмеченные недостатки.

По мнению авторов, книга является первым полным русскоязычным практическим руководством по вопросам управления непрерывностью бизнеса в чрезвычайных ситуациях. Книга отличается от других источников, преимущественно изданных за рубежом, тем, что в ней последовательно изложены все основные вопросы разработки и внедрения корпоративных программ управления непрерывностью бизнеса. В частности, рассмотрены принципы и методики оценивания *рисков (RA)* и *воздействия на бизнес (BIA)*, характеристики инструментальных средств планирования и управления непрерывностью бизнеса, практика выполнения проектов в различных государственных и коммерческих организациях и др.

Книга ориентирована на следующие основные группы читателей:

1. **Менеджеров высшего эшелона управления компанией (топ-менеджеров)**, которые хотят получить ответы на следующие вопросы: Как эффективно управлять непрерывностью бизнеса в интересах компании? Что такое корпоративная программа управления непрерывностью бизнеса, ЕСР? В чем ее суть? Зачем и кому она нужна? Насколько она актуальна для компании и ее бизнес-деятельности? Какова ее стоимость и последующие затраты? Кто отвечает за внедрение и сопровождение программы управления непрерывностью бизнеса? Какие существуют ограничения законодательного характера? Каковы последствия для компании? Какую роль играют инструментальные средства планирования и управления непрерывностью бизнеса? Какие отечественные и западные методики и технологии управления непрерывностью бизнеса предпочтительно использовать? Как подготовить свою компанию к аудиту и аккредитации в соответствии с требованиями британского стандарта BS25999.

Ответы на эти вопросы даются в Главах 1, 2, 4.

2. **Руководителей служб автоматизации (CIO)** и служб информационной безопасности (CISO), которые желают получить объективную и независимую оценку текущего состояния непрерывности критически важных бизнес-процессов и ИТ-сервисов, своевременно оценить последствия чрезвычайных ситуаций и выработать требования к возобновлению бизнеса, проверить адекватность и эффективность корпоративной программы управления непрерывностью бизнеса, рассчитать необходимые затраты на совершенствование упомянутой корпоративной программы, и предпринять все необходимые меры организационно-управленческого и технического характера для повышения (адекватного обеспечения) уровня непрерывности бизнеса компании.

Ответы на эти вопросы даются в Главах 2, 3, 4.

3. **Специалистов в области ВСМ, менеджеров по непрерывности и безопасности, специалистов служб внутреннего контроля**, которые желают

получить детальное представление об управлении непрерывностью бизнеса, достаточное для того, чтобы грамотно разбираться в этих вопросах, а возможно и руководить работами, связанными с разработкой и внедрением корпоративной программы управления непрерывностью бизнеса в своей компании. Этой категории читателей адресованы Главы 1, 2, 3.

4. **Внутренних и внешних аудиторов, консультантов и тренеров ВСМ.**

Данная категория читателей сможет получить ответы на интересующие их вопросы в Главах 1, 2, 4.

Книга также может использоваться в качестве учебного пособия студентами и аспирантами соответствующих специальностей, тем более что материалы многих глав основаны, в том числе и на опыте преподавания авторов в МГУ и СПбГУ.

Авторами книги являются эксперты и действующие практики в области непрерывности бизнеса (*Member BCI*) и защиты информации CISO *С.А.Петренко* и CISO *А.В. Беляев*.

Авторы выражают благодарность директору (*Technical & International Director*) британского института Business Continuity Institute (BCI) FBCI Линдону Бирду (*Lyndon Bird*), а также вице-президенту (*Research VP Litchfield, CT USA*) аналитической компании Gartner, Inc. Роберте Уитти (*Roberta J. Witty*) за ценные советы в ходе работы над книгой и сделанные ими замечания, устранение которых способствовало улучшению ее качества.

Авторы заранее выражают признательность всем читателям, которые готовы сообщить свое мнение о данной книге. Вы можете отправлять свои письма по адресу издательства «ДМК-Пресс» (orders@dmkpress.ru), выпустившего книгу.

С уважением,
CISO Сергей Петренко
CISO Андрей Беляев
Санкт-Петербург – Москва, 2010 год.