Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 05 (168)/2007

Непрерывность бизнеса

Подходы и решения

КОРПОРАТИВНЫЙ МЕНЕДЖМЕНТ

Непрерывность бизнеса
Подходы и решения

Константин Мусатов,
ИТ-консультант отдела проектирования вычислительных комплексов

СОДЕРЖАНИЕ

Введение

История обеспечения непрерывности деятельности началась в 50-х гг. XX века. Именно тогда компании столкнулись с проблемой аварийного восстановления деятельности и начали хранить дубликаты критичных данных в электронной и бумажной форме в удаленных помещениях. Первое время такие действия предпринимались отдельными предприятиями и организациями от случая к случаю, но в 70-х гг. их необходимость стала очевидной, применяться они стали довольно часто, и появились специализированные компании, предлагавшие услуги по хранению данных. Позже закономерно возник рынок резервных «горячих» вычислительных центров (ВЦ). Аварийное восстановление окончательно сформировалось в 80-х гг., когда в одних только Соединенных Штатах Америки услуги по предоставлению «горячих» резервных вычислительных центров предлагали более ста компаний. «Горячий» резервный ВЦ стал очень популярным решением среди финансовых организаций с централизованной ИТ-инфраструктурой, которые очень сильно зависели от наличия и доступности данных.

В 90-е гг. бурное развитие компьютерной индустрии привело к кардинальным переменам: на смену вычислительным центрам пришли вездесущие персональные компьютеры, соответственно этому изменились подходы к аварийному восстановлению информационных систем. Большинство организаций отказались от единого центрального мейнфрейма, заменив его большим количеством серверов и пользовательских мест, распределенных по всей организации. Децентрализация информационно-вычислительной инфраструктуры и, как следствие, большое количество разнообразных комбинаций неисправностей аппаратного и программного обеспечения существенно повысили сложность аварийного восстановления ИС.

Во второй половине 90-х на смену термину «аварийное восстановление» пришел термин «непрерывность бизнеса». Причиной этому послужил тот факт, что профессиональные составители планов аварийного восстановления старались уменьшить количество уязвимостей (начиная с человеческого фактора, продолжая недоступностью компьютерных сетей, сетевыми атаками и заканчивая авариями телекоммуникаций), которые возникли благодаря децентрализованной архитектуре. Термин «аварийное восстановление» стал использоваться для описания традиционных информационно-технологических вопросов, связанных с резервным копированием и восстановлением данных, тогда как о «непрерывности бизнеса» говорят в связи с бесперебойной деятельностью всей организации, включая производственное оборудование, средства коммуникации и персонал.

Развитие законодательной базы в мире

Помимо развития технологий, на деятельность организаций, особенно в финансовой сфере и области здравоохранения, стали оказывать все большее влияние нормативные требования и индустриальные стандарты. Хотя правительственные директивы носили расплывчатый характер, тем не менее они подстегнули проявление инициативы самими организациями и способствовали становлению дисциплины обеспечения непрерывности бизнеса.

С 1983-го года финансовые институты США должны были иметь планы восстановления, записанные на бумаге. Поскольку законодательные требования не отличались излишней конкретностью, считалось, что они относились в основном к резервному копированию и восстановлению баз данных. Для соответствия нормативным актам достаточно было увозить магнитные ленты с резервными копиями в удаленные хранилища. Более четкие законодательные требования к содержанию и уровню детализации, поддержанию в актуальном состоянии и тестированию планов аварийного восстановления появились лишь в 1989-м году.

В 1988 г. в США был основан Международный институт аварийного восстановления. Перед его членами были поставлены такие задачи:

- создание базы знаний по вопросам планирования аварийного восстановления и обеспечения непрерывности;
- сертификация людей, имеющих высокую квалификацию и большой опыт в данных областях;
- повышение профессионализма сертифицированных специалистов и уровня доверия к качеству их услуг.

В 1994 г. в Великобритании был основан Институт непрерывности бизнеса (Business Continuity Institute). Эта некоммерческая организация помогла объединить усилия специалистов в области аварийного восстановления и обеспечения непрерывности бизнеса и выработать единый набор рекомендаций в данной области.

В 1996 г. Департамент здравоохранения и социального обеспечения США (U.S. Department of Health and Human Services) начал разрабатывать «Акт об учете и перерегистрации страхования здоровья» (Health Insurance Portability and Accountability Act (HIPAA)), который требовал от компаний в области здравоохранения организовать процессы, гарантирующие сохранность личной информации пациентов. Здесь имелись в виду доступ, отслеживание, резервное копирование, передача и восстановление данных о клиенте, а также необходимо было разработать планы аварийного реагирования, обеспечения непрерывности деятельности и безопасности. Этот документ приобрел статус закона в 2001 году, а с 2003-го были ужесточены требования к его соблюдению.

В 1997 г. Объединенная комиссия по аккредитации организаций здравоохранения США (Joint Commission on Accreditation of Healthcare Organizations (JCAHO)) опубликовала руководство, в котором рассматривались вопросы информационной безопасности, готовности к чрезвычайным ситуациям и аварийного восстановления в области здравоохранения. Все организации, желающие быть аккредитованными, обязаны отвечать данным требованиям.

В том же году Федеральный совет по надзору за финансовыми учреждениями США (Federal Financial Institutions Examination Council (FFIEC)) объявил, что за отсутствие планов аварийного восстановления распределенных компьютерных сетей несут ответственность советы директоров организаций. Позднее FFIEC расширил их зону ответственности дополнительно к планам в области компьютерного оборудования, включив в нее планы обеспечения непрерывности бизнеса всей организации.

В 2000 г. американская Национальная ассоциация пожарных (National Fire Protection Association) опубликовала стандарт аварийного управления и программ обеспечения непрерывности (NFPA 1600), определив тем самым требования в таких областях программ обеспечения непрерывности, как оценка риска, анализ влияния на бизнес, снижение ущерба и тестирование. Этот стандарт был утвержден Американским национальным институтом стандартов (American National Standards Institute (ANSI)), после чего стал часто цитируемым руководством при разработке различных инициатив в области обеспечения непрерывности бизнеса.

В 2001г. в США вступил в силу Акт Грамма-Лича-Блайли (Gramm-Leach-Bliley Act), обязывающий организации соблюдать процедуры, обеспечивающие конфиденциальность информации клиентов. Организации, на которые распространяется действие Акта Грамма-Лича-Блайли (к ним относятся не только финансовые институты, но и сети розничной торговли, страховые компании, агентства недвижимости и налоговые консультанты), также обязаны удостове-

риться, что их поставщики услуг или товаров, в свою очередь, также защищают личные сведения клиентов.

В 2002 г. в США был принят Акт Сорбейна-Оксли (Sarbanes-Oxley Act), обеспечивающий более высокое качество корпоративного управления при подготовке финансовой отчетности для инвесторов. Он требует от высшего руководства подтверждать точность финансовых отчетов, а также раскрывать любые изменения, относящиеся к финансовому положению организации или ведению операций. (Несмотря на то, что этот документ не содержит конкретных ИТ-требований, из его положений вытекает ряд ограничений и условий, которым должна удовлетворять информационная система организаций).

В 2004 г. Комиссия по ценным бумагам США (Securities and Exchange Commission (SEC)) одобрила два документа: «Правило 3510 Национальной Ассоциации дилеров ценных бумаг» (National Association of Securities Dealers (NASD) Rule 3510) и «Правило 446 Нью-Йоркской фондовой биржи» (New York Stock Exchange (NYSE) Rule 446), требующие от организаций-членов создания и поддержания в актуальном состоянии планов обеспечения непрерывности бизнеса. Правила также рекомендуют ежегодно пересматривать планы, постоянно поддерживать их актуальность и в обязательном порядке информировать клиентов о способах реагирования на возможные перерывы в деятельности.

В 2002 г. британский Институт непрерывности бизнеса опубликовал первую версию «Руководства по применению рекомендуемых методов» (Good Practice Guidelines). На их основе в начале 2003 г. Британский институт стандартов совместно с Институтом обеспечения непрерывности разработал общедоступную спецификацию PAS56. В этом документе описывались процесс, общие принципы и терминология управления непрерывностью бизнеса. Что еще более важно, в нем описывались действия, выполняемые в рамках процесса управления непрерывностью бизнеса, и результаты, достигаемые после внедрения этого процесса. Кроме того, документ содержал описание проверенных на практике наилучших методов выполнения этих действий.

28 августа 2003 г. Международный институт аварийного восстановления и британский Институт непрерывности бизнеса опубликовали свод знаний, которыми должны обладать те, кто профессионально предоставляет услуги в области аварийного восстановления и обеспечения непрерывности деятельности организации. Этот свод знаний состоял из 10 пунктов, каждый из которых описывал один из этапов разработки, внедрения и развития процесса управления обеспечением непрерывности бизнеса. Наличие этого свода знаний позволило унифицировать требования, предъявляемые при сертификации специалистов, найме на работу и заключении контрактов.

В 2003 г. Объединенным комитетом стандартов Австралии и Новой Зеландии была опубликована первая версия «Справочника по управлению обеспечением непрерывности бизнеса» (Handbook Business Continuity Management). В документе рассматривались такие угрозы непрерывности бизнеса, как стихийные бедствия, крах компаний, военные действия и терроризм. В следующем году после существенной переработки и дополнения в свет вышла вторая версия этого справочника.

25 июля 2003 г. Банк Японии выпустил документ под названием «Планирование обеспечения непрерывности в финансовых организациях» («Business Continuity Planning at Financial Institutions»). Это был третий документ, посвященный проблеме обеспечения непрерывности критичных операций в финансовых институтах. Первый — «Разумные меры по управлению обеспечением непрерывности деятельности финансовых институтов при подготовке к разрушению рабочих помещений» («Sound Practices on Business Continuity Management of Financial Institutions in Preparation for Disruption of Operational Sites») — был опубликован в марте 2002 г., а второй — «Результаты опросного изучения управления обеспечением непрерывности деятельности» («Results of a Questionnaire Study on Business Continuity Management») — в феврале 2003-го. Но только в третьем (июльском) документе, наконец, появилось подробное описание «разумных мер» по разработке и внедрению планов обеспечения непрерывности деятельности.

В ноябре 2004 г. Главный информационный департамент Федеральной канцелярии Австрии подготовил «Справочник по информационной безопасности» (Handbook of IT-Security), версия 2.2. (Первая версия увидела свет еще в 1998 г.). Австрийский справочник подробно описывает процесс управления информационной безопасностью, анализ рисков, разработку концепции безопасности, порядок внедрения планов безопасности и последующие действия, а также содержит большой список мер по обеспе-

чению безопасности. Первоначально документ предназначался только для правительственных организаций, но новая версия подходит для любых организаций. Этот документ соответствует международным стандартам информационной безопасности ISO/IEC IS 13335 и, частично, ISO/IEC IS 17799, и он тесно связан с процессами обеспечения непрерывности и управления изменениями.

22 сентября 2005 г. Бизнес-федерация Сингапура совместно с Советом по стандартам, продуктивности и инновациям Сингапура (Standards, Productivity and Innovation Board (SPRING)) и при поддержке Совета по экономическому развитию Сингапура официально объявила о вступлении в действие стандарта управления обеспечением непрерывности деятельности. Он получил название Technical Reference TR19:2005. В стандарте описаны требования, предъявляемые к организациям, задавшимся целью защититься от событий, которые могут прервать ход выполнения штатных бизнес-операций, и получить возможность быстро восстанавливать эти операции, а также оговариваются требования к поддержанию готовности реагировать на чрезвычайные события. Однако в нем нет описания того, каким образом организации должны добиваться выполнения требований данного документа. В качестве обоснования утверждается, что деятельность каждой организации носит уникальный характер и постоянно меняется вслед за развитием технологий, изменениями в бизнес-среде и необходимостью удовлетворять нормативным и законодательным актам. Также в стандарте не рассматриваются вопросы управления проектом написания планов обеспечения непрерывности, такие как инициация проекта и получение поддержки со стороны высшего руководства организации. Отметим, что ряд компаний, расположенных в Сингапуре и в других странах, уже сообщили об успешном прохождении сертификации на соответствие этому стандарту.

В конце 2005 г. правительство Японии опубликовало первую редакцию «Руководства по обеспечению непрерывности бизнеса» («Business Continuity Guidelines»). В то время как лидеры в области обеспечения непрерывности — Великобритания и США — в качестве основной угрозы рассматривают терроризм, главное внимание японских компаний сосредоточено на минимизации воздействия стихийных бедствий, например, землетрясений. Тем не менее структура и содержание этого руководства соответствует документам, имеющим международное признание. Важной отличительной особенностью последствий стихийных бедствий является их большой масштаб, из чего вытекает невозможность восстановления деятельности одной отдельно взятой компании или организации. Поэтому данный документ содержит требования к организации объединять усилия по восстановлению как с расположенными поблизости компаниями, так и с важными партнерами по осуществлению прерванной деятельности. Япония выступила с инициативой о включении этого положения в будущий международный стандарт ISO. В настоящее время правительство Японии совместно с десятью промышленными группами разрабатывает узкоспециализированные руководства по обеспечению непрерывности бизнеса в различных отраслях.

В июне 2006 г. Объединенным комитетом стандартов Австралии и Новой Зеландии опубликован документ HB 292-2006 «Руководство по управлению обеспечением непрерывностью деятельности для практического применения» («A practitioners guide to business continuity management»). В нем описывается ряд общепринятых, а также новых практических методов, применяемых в США, Великобритании и ряде других стран. Особенность управления непрерывностью деятельности заключается в том, что методы, хорошо зарекомендовавшие себя в одной организации, могут не подойти для другой, поэтому очень большое внимание должно быть уделено выбору аспектов управления обеспечением непрерывности, которые будут реализованы в конкретной организации. Структура этого руководства основана на второй версии «Справочника по управлению обеспечением непрерывности бизнеса». Однако содержание документа существенно расширено и дополнено большим количеством пояснительной информации.

4 июля 2006 г. Базельский комитет по банковскому надзору опубликовал новые соглашения о достаточности капитала (Базель II). Эти рекомендации не являются обязательными к выполнению, однако учитываются при разработке законодательных актов. Работы по внедрению этих рекомендаций ведутся более чем в ста странах. Их выполнение обеспечит стабильность международной финансовой системы даже в том случае, если прекратится деятельность одного или нескольких банков. Достижение этой цели осуществляется путем наложения строгих требований на процессы управления рисками и капиталом и в том числе затрагивает процессы оценки рисков и влияния на бизнес, написания

планов обеспечения непрерывности деятельности и т.д. В августе 2006 г. Базельский комитет выпустил специальный документ, посвященный теме непрерывности бизнеса: «Высокоуровневые принципы обеспечения непрерывности деятельности» («High-level principles for business continuity»).

В ноябре 2006 г. Британский институт стандартов опубликовал первую часть стандарта BS 25999-1 Business Continuity Management — Code of practice. К моменту написания этой статьи завершилось публичное обсуждение чернового варианта второй части данного стандарта. Официальная публикация второй части, намеченная на 30 октября 2007 года, позволит организациям получать сертификат соответствия требованиям этого стандарта.

Летом 2007 г. канадская ассоциация по стандартизации представила для публичного обсуждения Стандарт Z1600 аварийного управления и программ обеспечения непрерывности деятельности. Сбор предложений и комментариев заканчивается 17 сентября 2007 г.

Состояние дел в России

Конечно, проблема сохранения жизни людей и сохранности важной информации в условиях аварийных ситуаций волновала не только западный мир. В нашей стране в каждой организации обязательно существовали регламенты действий при пожаре, штаб гражданской обороны и даже иногда проводились учебные тревоги. Для обеспечения сохранности важного программного обеспечения, например, в некоторых организациях делались полные распечатки текстов компьютерных программ, которые хранились в удаленном хранилище.

В качестве угроз с точки зрения гражданской обороны рассматривались, главным образом, риски вооруженного нападения на государство, поэтому гражданская оборона представляла из себя систему общегосударственных оборонных мероприятий, проводимых в мирное и военное время в целях защиты населения и обеспечения устойчивой работы народного хозяйства. Общее руководство осуществлялось правительством, а на местах — местными органами власти. В качестве мер реагирования предусматривалась организация эвакуации населения из городов, из районов возможного затопления в результате разрушения крупных гидротехнических сооружений в безопасные районы, укрытие населения в убежищах и других защитных сооружениях. Другая важная задача гражданской обороны, помимо эвакуации населения, состояла в обеспечении устойчивой работы народного хозяйства. В этих целях проводились различные организационные и инженерно-технические мероприятия; создавались запасы сырья, оборудования и средств для восстановительных работ. В полном соответствии с теорией и здравым смыслом для успешного решения задач гражданской обороны проходила подготовка населения и (иногда) проводились учения. Но после распада Советского Союза мероприятия в рамках гражданской обороны практически перестали осуществляться.

В последние несколько лет в России стали появляться коммерческие центры обработки и хранения данных, такие как DATA FORT, M1, Stack, WideXs, обеспечивающие компаниям возможность продолжать предоставление услуг клиентам в случае выхода из строя или перерыва в работе собственного вычислительного центра.

В 2003 г. Центральный банк Российской Федерации принял Положение ЦБР от 16 декабря. N 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах». Пункт 3.7 этого положения гласит: «Кредитная организация должна иметь разработанные планы действий на случай непредвиденных обстоятельств с использованием дублирующих (резервных) автоматизированных систем и (или) устройств, включая восстановление критических для деятельности кредитной организации систем, поддерживаемых внешним поставщиком (провайдером) услуг. Внутренними документами должен быть определен порядок проверки этих планов в части их выполнимости в случаях возникновения непредвиденных обстоятельств, а также перечень непредвиденных обстоятельств, в отношении которых разрабатываются планы действий».

С первого января 2006 г. вступила в действие новая редакция Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2006. Раздел 9.6 целиком посвящен обеспечению непрерывности бизнеса (деятельности) и восстановлению после прерываний. В тексте

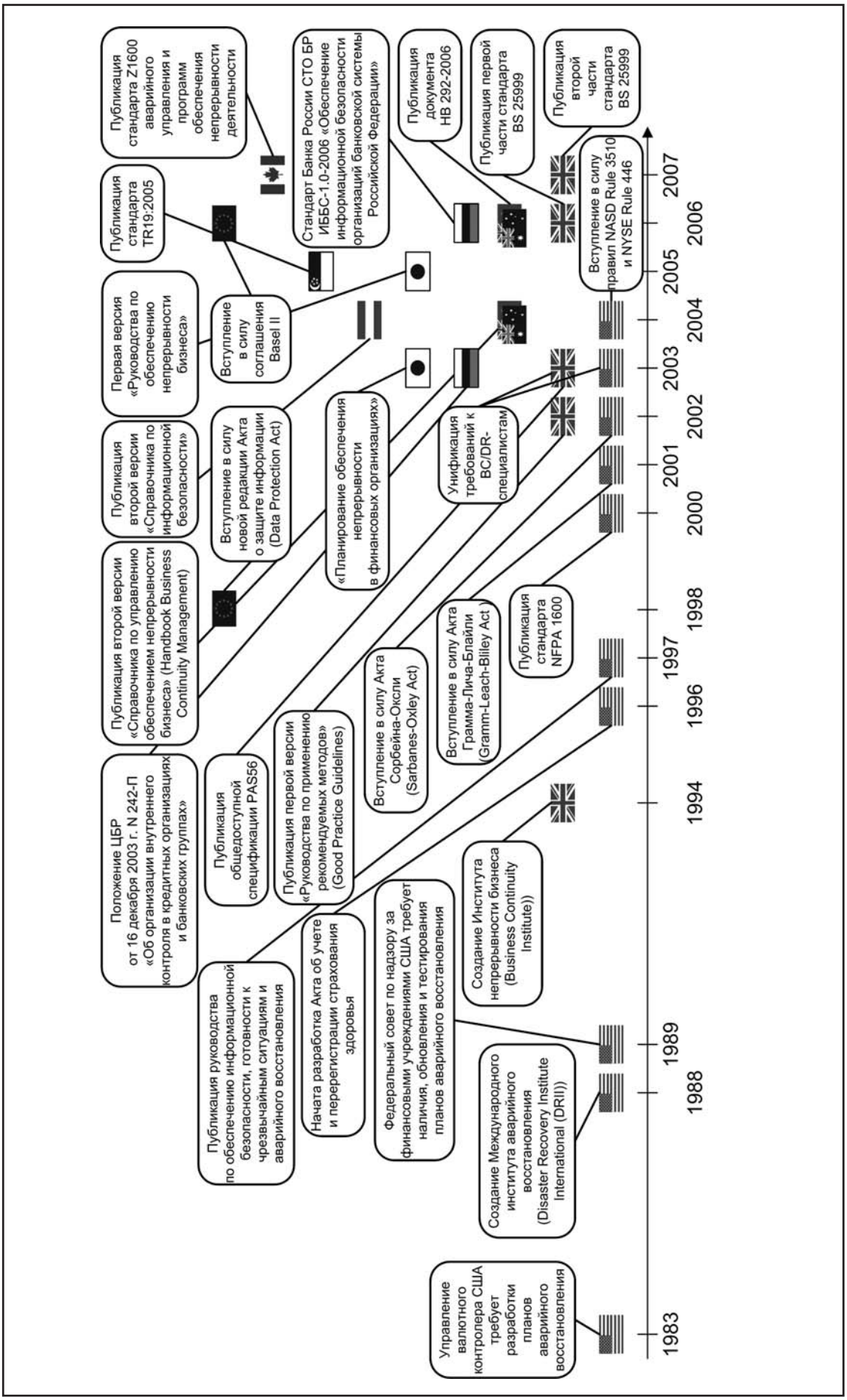

Рис. 1 Хронология международного законодательства, регулирующего аварийное восстановление и управление обеспечением непрерывности деятельности организаций

стандарта явно указано, что в качестве методологической основы при разработке планов могут быть использованы общепринятые международные стандарты, регулирующие вопросы менеджмента непрерывности бизнеса (например, BSI PAS-56).

Аналогичные законодательные акты появились в США и Великобритании в 80-х гг. Таким образом, можно заключить, что в законодательном плане мы отстаем примерно на два десятка лет. Так же, как в США и Великобритании 20 лет назад, сейчас в России вопросы, связанные с обеспечением непрерывности бизнеса, рассматриваются, в основном, как проблемы информационной безопасности или часть задач ИТ-инфраструктуры. Однако ситуация будет быстро меняться, причем в первую очередь на финансовом и телекоммуникационном рынках. Это определяется различными факторами.

На российский рынок приходят крупные финансовые корпорации. Высокие стандарты их работы, в том числе требования к наличию процесса обеспечения непрерывности бизнеса, заставят сначала поглощенные или приобретенные, а затем и все остальные отечественные финансовые институты позаботиться о сохранности своего бизнеса. Другими побудительными мотивами могут послужить стремление выйти на западные фондовые рынки и, следовательно, необходимость соблюдать законодательные нормы других стран, необходимость соответствовать разнообразным международным стандартам (одним из требований в ряде которых является наличие планов обеспечения непрерывности бизнеса); желание получить конкурентное преимущество в глазах партнеров или клиентов, которым необходима уверенность в надежности того, чьими продуктами/услугами они предполагают воспользоваться.

Прогноз – возникновение устойчивости бизнеса

Учитывая множество уже действующих нормативных актов и еще большее количество готовящихся к принятию, следует признать, что обеспечение непрерывности постепенно превращается в дисциплину, которая должна охватывать весь бизнес. Необходимо обеспечивать непрерывность операций, а также защиту сотрудников, клиентов, инвесторов. В защите нуждаются средства производства, инфраструктура, информация, торговая марка. Если прежде подходы к обеспечению непрерывности были специфичными для каждой области деятельности, и зачастую каждое подразделение занималось этой проблемой независимо от остальных, то сегодня необходим единый подход к проблеме сохранения устойчивости бизнеса организации в целом.

Обеспечение непрерывности бизнеса превращается в обеспечение его устойчивости, при которой гибкая ИТ-инфраструктура позволяет организации восстановить работу после любых сбоев в режиме реального времени. Такая инфраструктура предоставит всем сотрудникам, партнерам и другим заинтересованным сторонам доступ к любой информации, необходимой для выполнения важных бизнес-операций. В случае чрезвычайной ситуации удаленный доступ, гетерогенные коммуникационные среды, беспроводные технологии немедленно превратятся из средств поддержания штатной работы в средства, поддерживающие функциональность организации в период аварии или сбоя. Подобное свойство является ключевым для обеспечения нулевого времени простоя, а это требование становится все более распространенным в сегодняшнем быстро меняющемся, высоко конкурентном мире бизнеса.

О преимуществах

Какие же преимущества получают организации, внедряющие процесс управления непрерывностью своей деятельности?

Внедрение этого процесса имеет много положительных сторон. Например, оно дает владельцам и акционерам гарантии сохранности вложенных средств. Более того, речь может идти не просто о сохранности. Согласно исследованию «The Impact of Catastrophes on Shareholder Value» Rory J. Knight и Deborah J. Pretty, кумулятивный доход сверх нормы (Cumulative Abnormal Return — сумма различий между ожидаемой и реальной стоимостью акций) компаний, успешно восстановивших деятельность после крупномасштабной аварии, спустя год составляет примерно 10% (Рис.2).

Менеджерам процесс обеспечения непрерывности выгоден тем, что повышает управляемость организации, сотрудникам — обеспечивает надежность и уверенность в будущем, поскольку снижается вероятность внезапного исчезновения компании-работодателя. Но следует отметить еще и то, что преимущества получает не только сама организация. При наличии этого процесса в компании ее клиенты и партнеры приобретают уверенность в том, что продукты или услуги будут получены ими в срок вне за-

Рис. 2 Диаграмма, иллюстрирующая превышение кумулятивного дохода сверх нормы компаний относительно расчетного

висимости от обстоятельств. Это становится важным конкурентным преимуществом на современном рынке. Еще одним преимуществом является то, что страховые компании будут назначать цену страхования бизнеса в зависимости от того, есть ли в организации планы аварийного восстановления или нет. Подобная практика широко распространена на Западе и без сомнения в скором времени начнет применяться и в России.

Преимуществом может стать соблюдение рекомендаций ЦБ РФ по обеспечению непрерывности бизнеса и аварийного восстановления деятельности кредитных организаций после прерываний; эти рекомендации описаны в представленных ниже документах.

Стандарт Банка России СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», вступивший в действие 1.1.2006, пункт 9.6. «Обеспечение непрерывности бизнеса (деятельности) и восстановление после прерываний». Организации следует разработать и внедрить план обеспечения непрерывности бизнеса (деятельности) и восстановления после прерываний. Данный план и соответствующие процессы восстановления должны пересматриваться на регулярной основе и своевременно обновляться (например, при существенных изменениях в операционной деятельности, организационной структуре, бизнес-процессах и автоматизированных банковских системах). Эффективность документированных процедур восстановления необходимо периодически проверять и тестировать (как минимум на полугодовой основе). С планом должны быть ознакомлены все сотрудники, отвечающие за его выполнение и вовлеченные в процессы восстановления.

Положение ЦБР от 16 декабря 2003 г. N 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», пункт 3.7. «Кредитная организация должна иметь разработанные планы действий на случай непредвиденных обстоятельств с использованием дублирующих (резервных) автоматизированных систем и (или) устройств, включая восстановление критических для деятельности кредитной организации систем, поддерживаемых внешним поставщиком (провайдером) услуг. Внутренними документами должен быть определен порядок проверки этих планов в части их выполнимости в случаях возникновения непредвиденных обстоятельств, а также перечень непредвиденных обстоятельств, в отношении которых разрабатываются планы действий».

Наличие планов BCP/DRP является обязательным условием в случаях, когда:

- организация, заботясь о повышении уровня информационной безопасности (ИБ), планирует получить сертификат соответствия собственной системы управления ИБ требованиям стандарта BS ISO/IEC 27001:2005;
- организация стремится повысить уровень управления ИТ-сервисами и планирует получить сертификат соответствия процесса управления ИТ-сервисами требованиям

стандарта ISO/IEC 20000:2005, одной из неотъемлемых частей которого является управление непрерывностью ИТ-сервисов.

Наличие планов BCP/DRP важно для создания репутации надежной организации, что имеет значение для выхода на зарубежные фондовые рынки.

В процессе создания и обновления планов появляется возможность:

- оценить угрозы/чрезвычайные ситуации, с которыми может столкнуться банк, и детально изучить их возможные последствия;
- оценить существующие уязвимости ИТ-инфраструктуры (управление рисками);
- формализовать и перенести на бумагу существующие неформальные процедуры и процессы (управление знаниями);
- повысить осведомленность сотрудников и руководства о проблеме обеспечения непрерывности деятельности за счет их вовлечения в процесс поддержания планов в актуальном состоянии;
- сократить время неразберихи и хаоса в случае наступления ЧС, тем самым уменьшить размер ущерба и ускорить процесс восстановления;
- внушать уверенность заинтересованным сторонам (особенно персоналу и заказчикам) в своей способности справиться с нештатной ситуацией;
- повышать устойчивость компании с течением времени, обеспечивая учет результатов процесса при принятии решений на всех уровнях;
- минимизировать вероятность нештатных ситуаций и их воздействие на деятельность организации.

Почему организация должна реализовать процесс управления непрерывностью деятельности?

Процесс управления непрерывностью деятельности представляет собой важный элемент надлежащего управления деятельностью организации, предоставления услуг и предпринимательской расчетливости.

Менеджеры и владельцы несут ответственность за поддержание способности организации к бесперебойному функционированию. Организации постоянно должны поставлять продукты и услуги, т.е. они заключают контракты и иным способом повышают ожидания заказчиков. Все организации имеют моральные и социальные обязательства, особенно если они обеспечивают помощь в чрезвычайных ситуациях или занимаются предоставлением общественных или добровольных услуг. В некоторых случаях обязанность организации реализовать процесс управления непрерывностью деятельности устанавливается в законодательном или нормативном порядке.

Деятельность всех организаций подвержена угрозе возникновения нештатных ситуаций, например, в случае, террористических актов, технологической аварии, наводнения, отключения электропитания и др. Наряду с обеспечением благополучия и безопасности, процесс управления непрерывностью деятельности обеспечивает способность адекватно реагировать на подобные нештатные ситуации.

В настоящее время управление непрерывностью деятельности необходимо рассматривать не как дорогостоящий процесс планирования, а как процесс, который повышает стоимость организации.

Преимущества эффективной программы управления непрерывностью деятельности

Преимущества эффективной программы управления непрерывностью деятельности состоят в том, что организация:

- имеет возможность проактивно идентифицировать возможные последствия нештатной ситуации;
- имеет разработанную процедуру эффективного реагирования на нештатные ситуации, позволяющую минимизировать воздействие таких ситуаций на организацию;
- имеет возможность управлять рисками, не подлежащими страхованию;
- содействует совместной работе различных групп;
- способна продемонстрировать эффективность процедур реагирования посредством их тестирования;
- может улучшить свою репутацию;
- может получить конкурентное преимущество, которое дает продемонстрированная способность обеспечивать непрерывность поставок.

Результаты реализации эффективной программы управления непрерывностью деятельности

Реализация эффективной программы управления непрерывностью деятельности позволяет добиться следующих результатов:

- идентифицированы и защищены основные продукты и услуги, что гарантирует непрерывность их поставки;
- используются средства управления инцидентами, что позволяет обеспечить эффективное реагирование;
- надлежащим образом собраны, документированы и проанализированы основные сведения о самой организации и ее отношениях с другими организациями, необходимыми регулирующими органами или правительственными учреждениями, местными органами власти и аварийными службами;
- персонал обучен эффективно реагировать на инциденты или нештатные ситуации с помощью надлежащего тестирования;
- требования заинтересованных сторон проанализированы и могут быть выполнены;
- в случае нештатной ситуации персонал получает надлежащую поддержку и необходимые контакты;
- обеспечивается надежность цепочки поставок организации;
- обеспечивается защита репутации организации;
- обеспечивается выполнение организацией правовых и нормативных обязательств.

Что подразумевается под процессом управления непрерывностью деятельности (BCM)?

К настоящему моменту наибольшее распространение в мире получил стандарт BS 25999 Business Continuity Management. С высокой долей вероятности именно он послужит основой для международного стандарта управления непрерывностью деятельности, который, несомненно, появится в скором будущем. По этой причине дальнейшее изложение в данной статье будет опираться, в основном, именно на этот стандарт.

В этом стандарте приведено следующее определение процесса управления непрерывностью деятельности: *«Целостный процесс управления, в рамках которого идентифицируются потенциальные угрозы деятельности организации, оцениваются возможные воздействия на бизнес-операции в случае осуществления этих угроз, а также создается основа для обеспечения способности организации восстанавливать свою деятельность и эффективно реагировать на инциденты, что позволяет гарантировать соблюдение интересов заинтересованных сторон, обеспечить защиту репутации, бренда и создающих стоимость операций».*

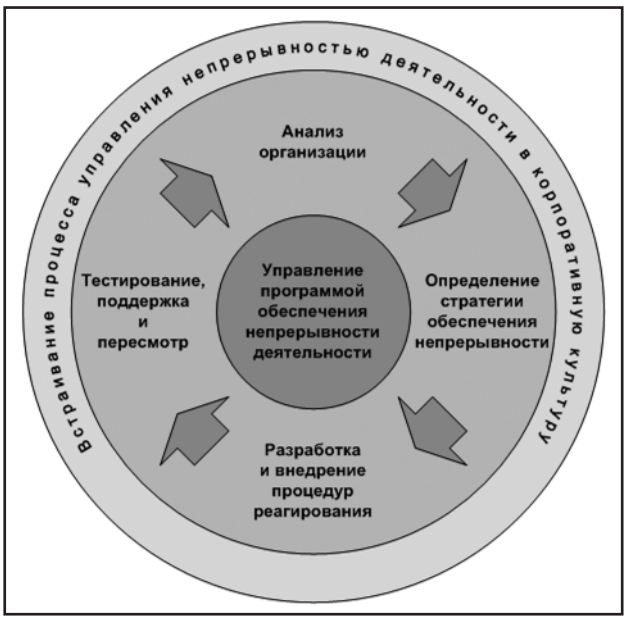

Рис. 3 Жизненный цикл процесса управления непрерывностью деятельности согласно стандарту BS25999

Этот процесс нельзя свести к аварийному восстановлению, или к кризисному управлению, или к управлению рисками, или восстановлению технической архитектуры. К нему нельзя относиться как к области деятельности узкой группы специалистов. Напротив, инициатором и движущей силой этого процесса должно быть высшее руководство организации. Управление непрерывностью деятельности охватывает все стороны деятельности организации и тесно связано с самым широким кругом дисциплин менеджмента.

Приведем описание **жизненного цикла** процесса управления непрерывностью деятельности. Цикл включает шесть элементов, которые могут быть реализованы организациями любого масштаба, функционирующими в любом секторе экономики: государственном, частном, некоммерческом, образовательном, производственном и т.д. Хотя область применения и структура программы построения процесса управления непрерывностью деятельности могут варьироваться, а объем затраченных усилий будет зависеть от потребностей конкретной организации, указанные шесть элементов всегда должны присутствовать.

Этап 1. Управление программой построения процесса обеспечения непрерывности деятельности

Согласно определению, программой называется план деятельности, совокупность действий и мероприятий для достижения намеченной цели.

Рис. 4 Области деятельности организации, охватываемые процессом управления непрерывностью

В данном случае правильнее говорить не об отдельном проекте, а именно о программе, поскольку построение процесса обеспечения непрерывности деятельности является широкомасштабной задачей, охватывающей самые различные области деятельности организации, многие подразделения и разные уровни руководства. Управление программой абсолютно необходимо рассматривать как отдельную важную задачу. Недостаток внимания к вопросам управления приведет к тому, что действия в рамках программы окажутся нескоординированными, и в результате станет невозможно оценивать эффективность выполнения работ и значимость достигнутых результатов, достоверно проверять работоспособность реализованных мер, своевременно модернизировать используемые решения и проверять готовность сотрудников к действиям в чрезвычайной ситуации. Если руководители компании считают работу в рамках данной программы излишней обузой, то чего же тогда можно ожидать от рядовых сотрудников? Если процессом не руководить, участники быстро теряют интерес и всякое желание принимать участие в проектах, появившихся в рамках программы.

Опыт множества проектов свидетельствует, что одной из первых задач на этом этапе является формализация целей организации в области обеспечения деятельности и составление политики обеспечения непрерывности. В этом документе отражается степень важности, которую придает обеспечению непрерывности высшее руководство организации, и общие принципы, в соответствии с которыми должна обеспечиваться непрерывность деятельности.

Для того чтобы оценить качество управления программой обеспечения непрерывности деятельности в организации, следует ответить, например, на ряд следующих вопросов:

- чувствуют ли менеджеры организации собственную ответственность за обеспечение непрерывности своей деятельности?
- выделяется ли собственный бюджет на деятельность в рамках программы?
- отслеживается ли влияние происходящих в организации изменений на возможность обеспечения непрерывности деятельности?
- есть ли в компании налаженный процесс составления отчетов о состоянии дел с обеспечением непрерывности деятельности?
- есть ли информационная система, в которой фиксируется и хранится вся информация, относящаяся к внедрению, поддержанию и модернизации процесса обеспечения непрерывности деятельности?
- существуют ли процедуры, гарантирующие соответствие организации договорным

обязательствам и требованиям законодательства и нормативных актов?
- участвует ли в программе внутренняя служба аудита?
- отражаются ли происходящие в организации изменения в планах аварийного восстановления?

Если положительный ответ можно дать не на все вопросы, значит, есть над чем работать.

Следует заметить, что в рамки управления входят как процесс восстановления деятельности в случае наступления чрезвычайной ситуации, так и процесс создания и постоянного обновления организационных и технических мер, обеспечивающих возможность этого восстановления.

Этап 2. Анализ организации

Действия, выполняемые на данном этапе, обеспечивают сбор информации, которая позволяет расставить приоритеты среди продуктов и услуг, предоставляемых клиентам организации, а также определить первоочередные действия, необходимые для предоставления этих продуктов и услуг.

Собираемая информация должна помочь ответить на следующие вопросы:
- какие бизнес-цели, стоящие перед организацией, расцениваются как самые важные?
- какие продукты, услуги появляются в результате достижения этих бизнес-целей?
- какие внешние и внутренние ресурсы, технологические или бизнес-процессы необходимы для достижения важных бизнес-целей?
- за какой период времени или с какой периодичностью требуется достигать выбранных бизнес-целей?
- какой уровень риска организация считает для себя приемлемым?

Решение о приемлемом уровне риска должно быть не интуитивным, а осознанным. Руководство организации должно четко осознать масштаб и серьезность существующих рисков перед тем, как документально подтвердить свою готовность рисковать.

Кроме того, для каждого бизнес-процесса организации, непрерывность которого должна быть обеспечена, определяются количественные параметры его восстановления. К таким параметрам относятся:
- RTO (Recovery Time Objective, целевое время восстановления) — промежуток времени с момента наступления чрезвычайной ситуации, за который выполнение критичного бизнес-процесса должно быть восстановлено. Сегодня уровень развития технологий позволяет обеспечить почти мгновенное восстановление, по крайней мере, технической инфраструктуры, поддерживающей данный бизнес-процесс. Однако надо принимать во внимание, что стоимость таких решений весьма высока и может превышать ценность самого бизнес-процесса;
- RPO (Recovery Point Objective, целевая точка восстановления) — промежуток времени, предшествующий наступлению чрезвычайной ситуации, данные за который могут быть утрачены. Например, если резервная копия данных создается один раз в сутки, то в случае наступления ЧС все данные, поступившие после последнего создания резервной копии, будут утрачены. Сегодня существуют технические возможности свести к нулю потери данных в случае возникновения критической ситуации. Как и в предыдущем пункте, необходимо тщательно изучить все сильные и слабые стороны применения таких технологий;
- LBC (Level of Business Continuity) — уровень непрерывности бизнеса. Этот параметр

Рис. 5 Параметры, количественно описывающие процесс восстановления

восстановления описывает, какую долю штатной нагрузки должен обеспечивать бизнес-процесс в случае ЧС. Возможен случай, когда в кризисной ситуации будет достаточно восстановить только 50% производительности в штатном режиме.

Полученные ответы на следующем этапе позволят определить выбор такой стратегии обеспечения непрерывности деятельности, которая наилучшим образом будет соответствовать политике обеспечения непрерывности.

Этап 3. Определение стратегии обеспечения непрерывности деятельности

Стратегия обеспечения непрерывности должна предусматривать решение целого ряда задач:

- обеспечение безопасности сотрудников;
- обеспечение персонала рабочими помещениями;
- обеспечение техническими средствами;
- обеспечение доступа к необходимой информации;
- обеспечение необходимыми материалами;
- обеспечение взаимодействия с бизнес-партнерами, подрядчиками, поставщиками, клиентами и другими заинтересованными сторонами.

Для решения каждой из этих задач вырабатывается собственная стратегия, нацеленная на достижение параметров восстановления, определенных на предыдущем этапе.

Работы по обеспечению непрерывности в случае наступления чрезвычайной ситуации можно условно разбить на три фазы:

- реагирование на событие — эвакуация персонала и оборудования, вызов аварийных служб;
- обеспечение непрерывности критичных бизнес-процессов — продолжение выполнения наиболее важных бизнес-процессов в кризисных условиях, например, в новом помещении;
- восстановление штатного выполнения всех бизнес-процессов — возвращение в старое помещение или восстановление бизнеса на новом месте в полном объеме.

Для каждой из этих фаз может потребоваться разработка своего набора стратегий.

Этап 4. Разработка и внедрение процедур реагирования

Результатом разработки и внедрения процедур реагирования процесса управления непрерывностью деятельности является создание инфраструктуры управления и структуры управления инцидентами, планов обеспечения непрерывности деятельности и планов восстановления деятельности, в которых подробно определяются действия, которые необходимо предпринять во время или после инцидента для поддержки или восстановления функционирования.

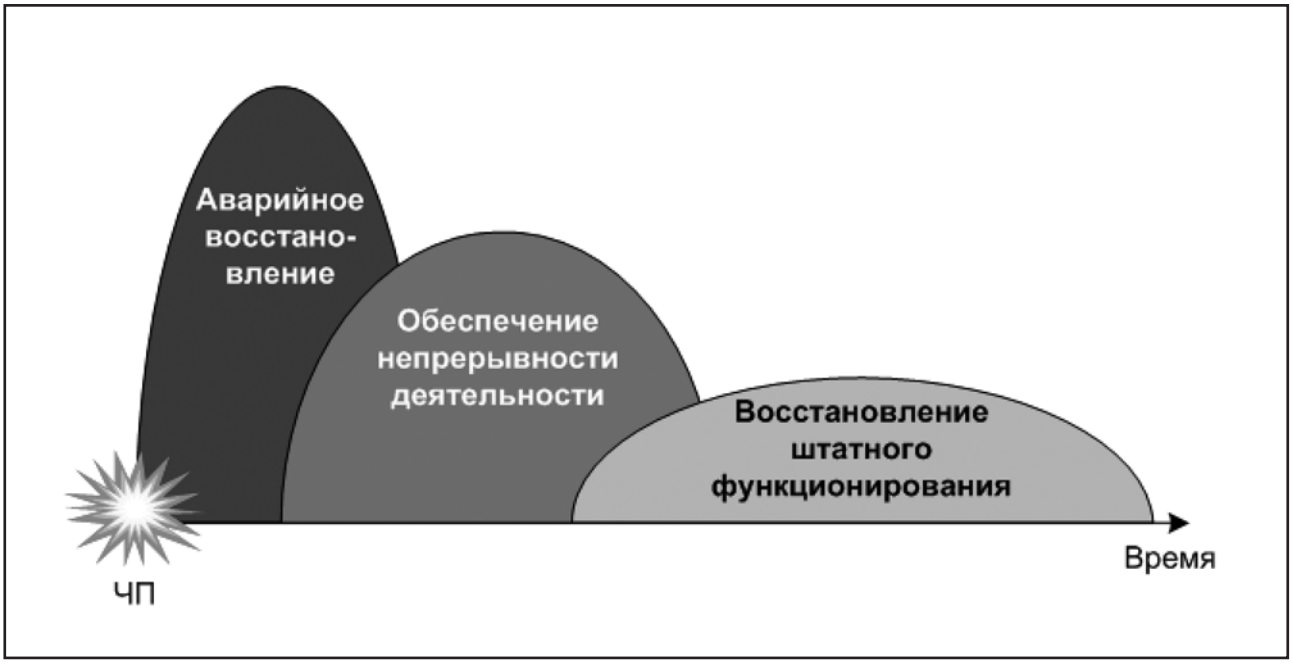

Рис. 6 Этапы восстановительных работ в случае чрезвычайного происшествия

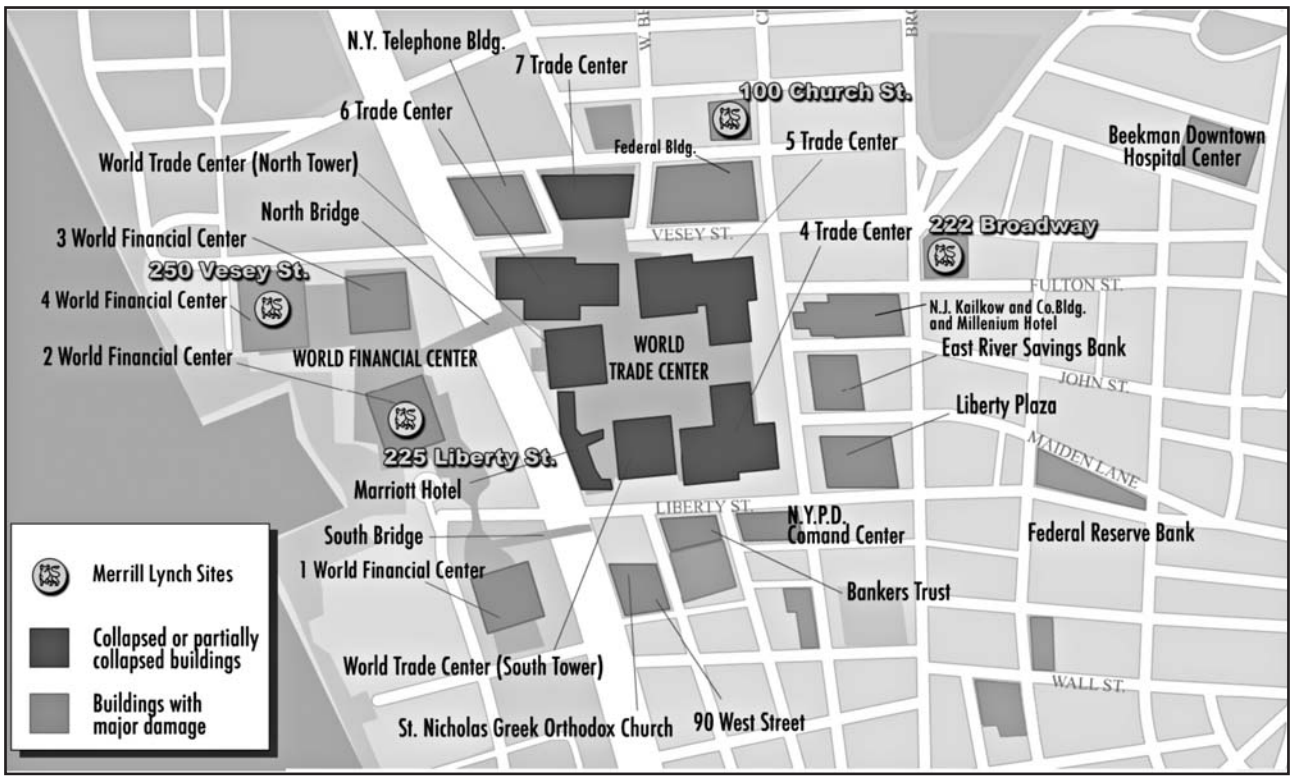

Рис. 7 Схема расположения зданий компании Merill Lynch и степень их разрушения

Природа инцидента может оказаться столь неожиданной, что организация окажется неподготовленной именно к такому развитию событий, даже если она предусмотрела тщательно проверенные ответные меры против ожидаемого уровня ущерба. Поэтому крайне важно, чтобы руководство организации и вспомогательные структуры не следовали бездумно существующему плану, а принимали решения в зависимости от обстоятельств. План обеспечения непрерывности деятельности никогда не заменит решений квалифицированных и компетентных специалистов.

В качестве примера можно привести американскую корпорацию Merill Lynch, центральные офисы которой находились в непосредственной близости от башен Всемирного торгового центра. За несколько месяцев до 11 сентября 2001 года корпорация проводила масштабные учения, в ходе которых имитировалась недоступность зданий штаб-квартиры в результате аномальных снегопадов. Мысль о том, что здания могут быть полностью или частично разрушены, конечно, никому не могла прийти в голову. Однако благодаря тому, что процесс управления обеспечением непрерывности был внедрен в компании, а все, кто мог, участвовали в восстановительных работах, испытаниях и тестах, деятельность компании была восстановлена в течение недели, и перерыв оказал минимальное влияние на бизнес (Рис. 7).

Этап 5. Тестирование, поддержка и пересмотр мероприятий процесса управления непрерывностью деятельности

Тестирование, поддержка, пересмотр и аудит системы управления непрерывностью деятельности обеспечивают для организации возможности, представленные в таблице 1 (см. стр. 18).

Этап 6. Встраивание процесса управления непрерывностью деятельности в культуру организации

Внедрение процесса управления непрерывностью деятельности в культуру организации дает много положительных моментов. В ряде высокотехнологичных отраслей, таких как телекоммуникации, непрерывность деятельности является не просто потребностью бизнеса, но и требованием законодательства. Временное непредоставление услуг вне зависимости от причин, вызвавших этот перерыв, может привести к отзыву лицензии и, следовательно, полному прекращению деятельности. Изменение корпора-

Описание	Преимущества	Недостатки
Настольная проверка проводится в виде диалога между автором и, как правило, еще одним участником. Она также может быть применена к техническим компонентам, таким как таблицы конфигурации, и индивидуальным планам восстановления.	Настольная проверка обычно выявляет в проверяемом документе серьезные дефекты или неверные допущения и является быстрой, простой и дешевой.	Из-за небольшого количества участников и отсутствия проверки на практике не могут быть выявлены более мелкие изъяны.
Сквозной анализ является более тщательной проверкой и выполняется большим количеством участников. Тестирование может иметь форму: • чтения; • рецензирования; • диалога/проверочных вопросов; • разбора определенного сценария (если это возможно). Сквозной анализ является минимальным уровнем тестирования для документации и планов аварийного восстановления, предназначенных для групп.	Выявляет все серьезные дефекты или неверные допущения. Допускает введение сценария, т.е. принимается набор условий (сценарий) и содержание документа тестируется в предположении реализации этих условий.	В тестировании принимают участие не все, кто будет применять документ на практике, оно осуществляется виртуальным образом, поэтому не позволяет выявить мелкие недочеты и несогласованность действий большого количества людей.
Имитация предназначена для создания псевдоаварийной ситуации для одного конкретного элемента ИТ-инфраструктуры, например, путем отключения одного сервера. Именно так тестируются прикладные системы, ОС и физические компоненты ИС, а также документы, описывающие их восстановление. Данный тип тестирования позволяет доказать, что компоненты ИС могут действовать в соответствии с требованиями, предъявляемыми после возникновения аварии.	Позволяет использовать блочный подход, т.е., когда сначала могут быть протестированы базовые (небольшие) компоненты, которые затем будут встроены в более крупные, более сложные системы и среды. Данный тип тестирования может послужить хорошей основой для тестирования управления в кризисной ситуации, т.е. когда планы и действия управляющих в кризисной ситуации тестируются в предположении реализации некоторого набора условий.	Данный тип тестирования не всегда полностью доказывает абсолютную работоспособность, т.к. отсутствуют стресс и жесткие временные рамки аварийной ситуации и, таким образом, он не позволяет протестировать человеческий фактор.
Функциональное тестирование При данном типе тестирования, как правило, одна из бизнес-функций целиком восстанавливается и выполняется на резервном оборудовании/резервной площадке.	Позволяет доказать работоспособность и достаточный уровень взаимодействия: • команд аварийного восстановления ИТ-сервисов; • компонентов ИС; • сетевых соединений; • процессов инициации; • планов аварийного восстановления ИТ-сервисов; • связей с процессом управления в кризисной ситуации.	Данный тип тестирования может быть дорогостоящим, а отделение одной бизнес-функции от остальных не всегда возможно. Связанные с функциональным тестированием проблемы могут иметь разрушительные последствия.
Полное тестирование Имитируется полная потеря вычислительного центра/здания/офиса и тестируется весь процесс восстановления. При данном типе тестирования, как правило, все бизнес-функции будут восстановлены на резервном оборудовании/в РВЦ. Также могут быть протестированы/натренированы связи процесса инициации и управления в кризисной ситуации.	Позволяет убедиться в полной интеграции всех ИТ-компонентов, команд аварийного восстановления, планов аварийного восстановления и услуг по поддержке/поставкам со стороны третьих компаний.	Данный тип тестирования может быть очень дорогостоящим и очень разрушительным. Кроме того, риск провала может значительно превышать преимущества выполнения полного тестирования.

Таблица 1.

тивной культуры является длительным и сложным процессом. Написания стратегий и планов будет явно недостаточно.

Для достижения успеха на этом этапе действовать надо в нескольких направлениях. Во-первых, до сотрудников следует донести смысл и важность работ по обеспечению непрерывности. Причем это обучение необходимо проводить регулярно. Одновременно с этим необходимо тренировать навыки, которые потребуются сотрудникам в случае наступления ЧС.

Вторым важным компонентом успеха служит явная активная поддержка работ по внедрению и поддержанию этого процесса со стороны менеджмента ***всех уровней***. Поддержка со стороны только высшего руководства — есть необходимое, но не достаточное условие успеха. Пассивное сопротивление со стороны руководителей среднего звена и рядовых сотрудников, на кого ляжет существенная доля нагрузки по внедрению процесса, может стать непреодолимым препятствием на пути к успешному внедрению.

Третьим важным соображением является то, что даже в технологических компаниях процесс обеспечения непрерывности деятельности не должен рассматриваться как задача исключительно ИТ- или других технических подразделений. Необходимо регулярно проводить работу по донесению до бизнес-подразделений мысли, что задача обеспечения непрерывности бизнеса не может быть решена без их участия.

Перед тем как принимать решение о внедрении в организации этого процесса, в числе прочего руководству придется подумать о том, следует ли привлечь к этой работе внешних консультантов, или постараться справиться собственными силами. Наличие ресурсов и опыт внедрения подобных программ, масштаб организации и сложность ее бизнес-процессов — эти и множество других факторов должны быть взвешены и учтены. Каждая ситуация уникальна, поэтому невозможно дать однозначную рекомендацию, которая подошла бы всем и каждому. Выскажем лишь несколько общих соображений, которые могут оказаться полезными.

Какие еще вопросы предстоит решать в ходе работ по обеспечению непрерывности деятельности организации?

Помощь консультантов может оказаться полезной в том случае, если:

- собственный опыт в нужной области отсутствует или является недостаточным;
- не хватает ресурсов, скорее всего — свободных рук, для выполнения работ самостоятельно;
- хочется организовать работу/ построить процесс в соответствии с лучшими отраслевыми или мировыми практиками.

Внешние консультанты могут:

- руководить командой, направлять и координировать усилия сотрудников заказчика в нужном направлении;
- тренировать, обучать, передавая свой опыт, полученный в сходных проектах;
- планировать дальнейшие шаги благодаря владению методикой и наличию опыта;
- выполнять все работы, которые не могут быть выполнены сотрудниками заказчика (здесь следует отметить, что речь не идет о том, чтобы «увиливать» от выполнения договорных обязательств или «перекладывать» работу на других участников проекта. Одна из задач проектов по внедрению процесса управления обеспечением непрерывности деятельности состоит в передаче консультантами знаний и навыков, необходимых для поддержания этого процесса, сотрудникам заказчика);
- проверять результаты выполненных работ;
- исправлять допущенные ошибки, неверные предположения и планы, которые могут привести к проблемам в будущем. Среди наиболее распространенных ошибок можно упомянуть переоценку или недооценку рисков, делегирование задачи управления проектом внедрения BCM руководителям без необходимых полномочий, недооценка скорости изменений, происходящих в компании.

Задача привлечения консультанта тесно связана с задачей построения команды. Тот, на кого падет выбор, должен усилить команду, если она уже существует, или обязан соответствовать представлению о том, как должна выглядеть такая команда. Необходимо четко сформулировать для себя, какие задачи необходимо решить консультантам, после чего удостовериться, что их понимание поставленных задач совпадает с вашим. Однако возможна ситуация, когда одной из задач, стоящих перед консультантами, окажется та самая формулировка целей. В таком случае, ваш взгляд на цели и пути их достижения, вероятно, изменится с учетом рекомендаций консультантов.

Желательно, чтобы консультант обладал большим и успешным опытом предоставления услуг, которые планирует оказывать. Совсем хорошо, если его квалификация подтверждена сертификатами международных организаций, специализирующихся в предоставлении услуг подобного рода.

Будьте реалистичны в своих ожиданиях. При всем желании консультанты не сделают за вас всю работу, как и тренер не будет выступать вместо спортсмена, режиссер не будет играть вместо актера, а учитель не будет решать задачи вместо ученика. Для достижения поставленных целей требуется совместная работа, поэтому консультант нуждается в кооперации с вашей стороны не меньше, чем вы в его помощи.

Рис. 8 Кадры из ставшего уже историческим фильма о пожаре в компании «Инфосистемы Джет»

Опыт компании «Инфосистемы Джет»

Вот уже больше 15 лет компания «Инфосистемы Джет» предоставляет услуги системной интеграции. С годами клиенты компании стали проявлять все больший интерес к разнообразным консультационным услугам, в том числе к обеспечению отказоустойчивости информационных комплексов и непрерывности их деятельности, аварийному восстановлению функционирования и информационной безопасности. В пользе наличия процессов обеспечения непрерывности деятельности компания убедилась на собственном опыте, пережив в 2003-м году пожар и успешно пройдя все шаги восстановления бизнеса.

Приобретя практический опыт, специалисты компании «Инфосистемы Джет» занялись активным расширением теоретических и методических основ обеспечения непрерывности бизнеса. Работа в совместных проектах с западными консультантами, изучение специальной литературы, посещение международных выставок, участие в конференциях, посвященных аварийному восстановлению и обеспечению непрерывности, — все это гарантирует высокое

качество работ по обеспечению непрерывности на уровне лучших международных образцов.

Усилия по повышению качества предоставляемых услуг закономерно привели к тому, что ряд сотрудников компании стал членами британского Института непрерывности бизнеса (Business Continuity Institute). На сегодня это учреждение является лидером в области BCM, членами этой организации являются более 4000 специалистов из более чем 85 стран мира. На момент написания статьи более четверти всех сертифицированных этим институтом российских специалистов являются сотрудниками компании «Инфосистемы Джет». На их счету много реализованных проектов в области обеспечения высокой доступности сервисов, аварийного восстановления, обеспечения непрерывности деятельности в крупных российских финансовых и телекоммуникационных компаниях. Ниже приведены описания некоторых из этих проектов.

ОАО «Вымпелком»

Зависимость бизнеса от качества и доступности ИТ-сервисов вызвала необходимость разработать и внедрить стратегию обеспечения непрерывности предоставления ИТ-услуг, которая является частью стратегии обеспечения непрерывности бизнеса.

Для решения этой задачи к проекту были подключены команда компании «Инфосистемы Джет» и специалисты Symantec Consulting Services, выделенного коллектива консультантов компании Symantec.

По масштабу и бюджету это одна из крупнейших в мире программ послеаварийного восстановления и обеспечения непрерывности ИТ-услуг, позволяющая ОАО «ВымпелКом» снизить уровень рисков для бизнеса, защитить активы и минимизировать последствия аварий.

На первом этапе проекта было проведено подробное обследование информационных систем ВымпелКома с точки зрения их влияния на бизнес. Разработана общая стратегия восстановления ИТ-услуг и высокоуровневый план реализации проекта.

Далее работы велись в двух направлениях. Во-первых, специалисты компании «Инфосистемы Джет» спроектировали и внедрили технические решения, обеспечивающие реализацию разработанной стратегии восстановления ИТ-услуг: построили и оснастили резервный центр, за счет кластеризации обеспечили бесперебойность работы критических бизнес-приложений, с помощью синхронной репликации — высокую доступность данных, с помощью удаленного резервного копирования — сохранность данных. Во-вторых, были разработаны методики и планы обеспечения непрерывности предоставления ИТ-услуг в соответствии со спецификацией PAS56.

Обеспечение непрерывности ИТ-услуг — это одна из важнейших задач, решаемых ИТ-дирекцией ВымпелКома. Проводится регулярное обновление планов и методик, тестирование компонентов, обеспечивающих непрерывность предоставления ИТ-услуг. Проект развивается, и в настоящее время идет разработка всеобъемлющей стратегии обеспечения непрерывности бизнеса. В этот процесс будут вовлечены техническая дирекция компании и ее бизнес-подразделения. Реализация проекта позволит гарантированно восстанавливать предоставление бизнес-услуг в согласованное время при наступлении чрезвычайной ситуации.

В главном вычислительном центре (ГВЦ) работают около 300 RISC-серверов Sun Microsystems, объединенных сетью хранения данных с дисковыми массивами. В этой среде емкостью более 300 ТБ работает большинство основных приложений ВымпелКома, включая такие критически важные, как система самообслуживания клиентов, системы биллинга и управления взаимоотношениями с клиентами и партнерами. Резервный вычислительный центр (РВЦ) спроектирован таким образом, чтобы обеспечить резервирование всех критичных для бизнеса систем и приложений.

В рамках проекта специалисты компании «Инфосистемы Джет» спроектировали и построили новую сеть хранения (SAN) ГВЦ с полным дублированием сетевого оборудования и магистралей (более 2000 портов) и распределенную сеть хранения ГВЦ-РВЦ, распределенную систему резервного копирования на более чем 300 серверов с общей емкостью копируемых данных более 1ПБ, высокоскоростную транспортную сеть между ГВЦ и РВЦ на основе технологии DWDM, обеспечивающую синхронную репликацию более 20ТБ данных; более 10 распределенных кластеров для бесперебойного функционирования наиболее критичных бизнес-приложений (биллинг, CRM и др.), инженерную и ИТ- инфраструктуру РВЦ.

Для обеспечения антикризисного управления для персонала ВымпелКома консультантами Symantec были разработаны практические процедуры, тренинги и документация, основывающиеся на спецификации PAS56 и передовом мировом опыте.

ОАО «Межрегиональный ТранзитТелеком»

Целью проекта в ОАО «МТТ» стала разработка стратегии обеспечения непрерывности и плана аварийного восстановления ИТ-сервисов центрального офиса ОАО «МТТ».

В соответствии с требованиями заказчика, организация должна была получить разработанные планы действий на случай непредвиденных обстоятельств, а также процедуры и политики, обеспечивающие восстановление критических для деятельности организации систем, поддерживаемых внешним поставщиком (провайдером) услуг. Внутренними документами должен был быть определен порядок проверки этих планов в части их выполнимости в случаях возникновения непредвиденных обстоятельств, а также перечень непредвиденных обстоятельств, в отношении которых разрабатываются планы действий.

В рамках данного проекта были выполнены следующие работы:

1) составлен перечень непредвиденных обстоятельств, которые могут вызвать длительный перерыв в деятельности;
2) составлен список критичных ИТ-сервисов центрального офиса ОАО «МТТ», необходимых для обеспечения деятельности заказчика, в предоставлении которых длительный перерыв недопустим;
3) представлено описание ИТ-инфраструктуры и дана оценка реальных значений показателей RTO/RPO для существующей ИТ-инфраструктуры;
4) описан порядок действий персонала заказчика при выходе из строя отдельных ИТ-сервисов и отдельных серверных помещений;
5) описана стратегия тестирования плана аварийного восстановления и элементов ИТ-инфраструктуры.

Результатами данного проекта стали разработанная стратегия и планы аварийного восстановления. Проведенные тренинги послужили начальным шагом по внедрению процесса обеспечения непрерывности в корпоративную культуру ОАО «МТТ».

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем