Три простых вопроса
против одного «синдрома Титаника»

Евгений ПЕПЕЛЯЕВ,
коммерческий директор, SDN

Чудо инженерной мысли – круизный лайнер «Титаник» мог бы стать синонимом образцового BCP, настолько идеально в нем были продуманы все технические детали, организационные моменты, имидж. Но вместо этого он стал одним из самых горьких уроков в истории человечества и, пожалуй, самым убедительным аргументом для тех, кто сомневается, всегда ли нужен DRP. Да, всегда. Потому что любой «непотопляемый» проект рано или поздно становится зависимым от «незначительных» недоразумений.

Прежде чем продолжить разговор, разберемся с аббревиатурой. BCP – Business Continuity Planning – спланированный, документально регламентированный и доведенный до сведения исполнителей комплекс мер и процедур, направленных на обеспечение НЕПРЕРЫВНОСТИ бизнеса путем недопущения сбоя в бизнес-процессах. Иными словами, инструкция о том, как избежать проблем.

DRP – Disaster Recovery Planning – тоже спланированный, регламентированный и доведенный до сведения потенциальных (!) исполнителей комплекс мер, направленных на ВОССТАНОВЛЕНИЕ бизнес-процессов при их нарушении вследствие нештатных ситуаций, т. е. инструкция на случай, если проблемы избежать всё же не удалось

По сути, DRP – часть BCP-программы. Часть, но не одно и то же, хотя многие склонны их отождествлять. Иногда руководство компании отказывается рассматривать DRP, ссылаясь на то, что накануне был подписан BCP. Но ведь в BCP вопросы, связанные с восстановлением работоспособности ИКТ-систем, описаны лишь в общих чертах.

Принято считать, что DRP нужен только высокотехнологичным компаниям, у которых потери от кратковременного простоя измеряются сотнями, миллионами, миллиардами тысяч денежных единиц. Но разве для компаний с не столь мощным ущербом в абсолютных цифрах потеря в критическом для них процентном соотношении с оборотом менее губительна? У каждого своя планка, свои мерки и свои методики. Кому-то достаточно восстановить в памяти картинки противопожарного щита, кому-то – просто перезагрузить компьютер, а кому-то необходимо четко представлять, где лежит файл и/или распечатка с перечнем нужных телефонов и пошаговым описаний действий.

Ориентирами для определения действий на случай непредвиденного инцидента являются два показателя: Recovery Point Objective (RPO) – допустимые потери данных, не подлежащих восстановлению; время восстановления (RTO) – приемлемый промежуток времени, необходимый для восстановления утраченных информационных ценностей и не превышающий максимально допустимого срока срыва бизнес-процессов Maximum Tolerable Period of Disruption (MTPoD). Все эти параметры устанавливаются для каждой компании индивидуально, с учетом критичных для ее бизнеса факторов и зависимостей. В международной практике принято различать семь уровней готовности к восстановлению бизнеса:

уровень 0: время восстановления непредсказуемо, высока вероятность невозможности восстановления данных;

уровень 1: резервное копирование данных в удаленных хранилищах;

уровень 2: резервное копирование на ленточных библиотеках и off-сайтах;

уровень 3: электронная вольтижировка – системная организация резервных данных в удаленных виртуальных или физических кластерах ленточных библиотек;

уровень 4: point-in-time-копии – резервные копии критически важных данных, с высокой степенью частоты обновляемые на удаленных хранилищах;

уровень 5: целостность транзакций – высокий уровень согласованности приложений в основном и резервном центрах хранения и обработки данных, что позволяет сохранять непрерывность всех транзакций, сопоставимую с их качеством в штатном режиме;

уровень 6: нулевая или почти нулевая потеря данных;

уровень 7: высокая степень автоматизации бизнес-интегрированного решения.

Очевидно, что чем выше уровень организации аварийного восстановления данных, тем бóльшего размера инвестиций он требует. Именно поэтому так важно найти допустимый для компании баланс между приемлемыми для нее затратами на то, что может никогда не случиться, и размером потерь и упущенных выгод, которые может повлечь за собой нежелание «лишний раз» подстраховаться. Здесь следует отметить, что, по некоторым экспертным оценкам, каждый доллар, вложенный в DRP, окупается в четырехкратном размере.

ЧТО?

Согласно методологиям разных международных институтов, обладающих экспертизой в сфере управления непрерывностью бизнеса, разработка планов по восстановлению непрерывности бизнеса (Disaster Recovery Plan – DRP) является центральным и, пожалуй, самым значимым звеном в цепочке организационных мер, действий и расчетов, направленных на главную цель – обеспечение устойчивости бизнеса к любым испытаниям со стороны природных стихий, технических катаклизмов, человеческой некомпетентности.

Разработке плана предшествует тщательный анализ целого ряда факторов успешной деятельности компании – от бизнес-процессов, влияющих на качество рыночной услуги/продукта, до состояния инженерной инфраструктуры, поддерживающей нормальный режим работы офиса и ИКТ-систем. На этой стадии существует целая масса нюансов и подводных камней, знание или незнание которых может сыграть решающую роль в процессе организации и финансирования намеченных мер.

Наличие проработанной DRP-программы является жизненной необходимостью для участников кредитно-финансовой отрасли, для телекоммуникационных компаний федерального уровня, для высокотехнологичных предприятий непрерывного производственного цикла, к числу которых относятся, в частности, атомные электростанции.

Этапы программы управления непрерывностью бизнеса (Business Continuity Management – BCM)

АНАЛИТИКА:

- анализ бизнес-процессов (Business Environment Analysis – BEA) – ранжирование действующих в компании бизнес-процессов по степени важности и определение требований к ним по непрерывности;
- выделение ИТ-зависимых бизнес-процессов в отдельную группу;
- анализ рисков (Risk Analysis – RA) – определение рисков, уязвимостей и угроз, способных повлиять на непрерывность бизнес-процессов (в том числе оценка достаточности уже практикуемых организационных и технических мер предупреждения прерываний бизнеса);
- выделение в отдельную группу рисков, влияющих на ИТ;
- оценка воздействия на бизнес (Business Impact Analysis – BIA) – анализ влияния бизнес-процессов на весь бизнес в целом и определение целей восстановления каждого бизнес-процесса вместе с поддерживающей его инфраструктурой, фокус на ИТ составляющую.

ПЛАНИРОВАНИЕ:

- определение стратегии непрерывности бизнеса (Business Continuity Strategy definition) – фиксация целевого времени восстановления (Recovery Time Objective – RTO) и целевой точки восстановления (Recovery Point Objective – RPO) для каждого бизнес-процесса, выбор организационных и технических решений;
- разработка мер по обеспечению непрерывности бизнеса (Business Continuity Plan – BCP) в чрезвычайных ситуациях и пошаговых планов восстановления инфраструктуры в случае нарушения ее штатного режима работы (Disaster Recovery Plan – DRP), документирование соответствующих решений;
- создание технической и организационной систем управления непрерывностью бизнеса;
- формирование программы сопровождения и эксплуатации корпоративной программы BCM, разработка мер и регламентов обеспечения осведомленности персонала на случай возникновения угроз или последствий нештатной ситуации.

Для ряда отраслей разработаны обязательные к исполнению регламенты по обеспечению непрерывности бизнеса, без соблюдения которых само обладание лицензией на право деятельности становится невозможным. Самый известный из них – указание от 5 марта 2009 г. № 2194-У «О внесении изменений в Положение Банка России от 16 декабря 2003 г. № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» – введение в Положение ЦБ РФ от 16.12.2003 № 242-П Приложения № 5 – «Рекомендации по структуре и содержанию плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (далее – План ОНиВД) кредитной организации в случае возникновения непредвиденных обстоятельств, а также по организации проверки возможности его выполнения».

ЗАЧЕМ?

Правильный ответ на этот вопрос определяет успех проекта по планированию и реализации DRP-мер. На данном этапе необходимо определить спектр задач и правильно расставить приоритеты их решения. Не стоит рассчитывать на то, что все инициативы CIO будут безоговорочно поддержаны руководством, финансовой дирекцией и акционерами – как правило, бюджет на защиту от того, что то ли будет, то ли нет, выделяется крайне неохотно. Именно поэтому очень полезно на этапе анализа бизнес-процессов и рисков, угрожающих их непрерывности, заручиться поддержкой или, как минимум, доказательствами заинтересованности со стороны руководителей ключевых бизнес-подразделений. Это поможет сэкономить время и нервы на выяснение, что именно необходимо защитить в первую очередь. Привлечение сторонних аналитиков, обладающих нужными знаниями и опытом, еще больше повысит продуктивность работы и снизит неоправданные затраты.

В общем виде причины, по которым стоит позаботиться о разработке DRP, можно свести к трем основным категориям:

- DRP – непременное условие владения бизнес-лицензией / успешного прохождения аудиторской проверки / подтверждение соответствия бизнеса требуемому уровню ITIL/ITSM;
- организация испытывает осознанную необходимость в мерах по противостоянию последствиям неблагоприятным событиям, вероятность которых в данном регионе/сегменте бизнеса достаточно высока и/или прогнозируема (к примеру, сезонные перегревы, угроза силового воздействия, природные катаклизмы);
- потребность в понимании возможного ущерба бизнесу при простое информационных систем и сопоставления этого ущерба с затратами на профилактику таких ситуаций.

Что и как именно анализировать в конкретной компании – определяется исходя из специфики ее бизнеса и с учетом международных практик в данной сфере.

К окончанию данного этапа должна быть подготовлена матрица, в которой отражены упомянутые в BCP бизнес-процессы (с учетом степени критичности), ИКТ-сервисы, влияющие на них (также с указанием индекса приоритетности). Здесь же должны быть обозначены предполагаемые ресурсозатраты (человеческие, финансовые, технологические) и дан комментарий относительно необходимости тендера по выбору подрядчика или решения.

Еще раз подчеркнем: при подготовке концепции реализации DRP-мер надо быть готовым к тому, что от части задуманного придется отказаться. Решите для себя, с чем именно бизнес может повременить, приготовьтесь идти на уступки там, где возможно, и отстаивать свои позиции там, где это принципиально. Будьте готовы показать и обосновать то, что вы наметили для выполнения на следующем этапе. Будьте реалистичны в оценке своих возможностей и доступных ресурсов – лучше хорошо делать одну часть плана за другой, чем взяться за все и потерпеть неудачу.

После презентации матрицы задач и приоритетов руководству и получения «одобрям-с» на реализацию заявленных мер можно приступать непосредственно к планированию.

КАК?

Итак, акценты расставлены, границы сферы деятельности обозначены. Что теперь? Самое время сформировать управляющий комитет, состоящий из представителей топменеджмента, руководителей бизнес-подразделений, представителей службы безопасности, ИТ и эксплуатации инженерных систем. Если для реализации проекта привлекается внешняя компания, то ее представитель, естественно, тоже входит в управляющий комитет. Возглавлять проект (и комитет) должен опытный профессионал в данной сфере – именно он в итоге будет нести ответственность перед бизнесом и людьми.

Параллельно с формированием комитета должен быть подготовлен разъяснительный документ, информирующий сотрудников компании о вводе в действие BCP&DRP-программы, планируемых мероприятиях, а также разъясняющий значимость нововведения (или устоявшейся уже традиции) для компании. Здесь же должна быть отражена информация о создании и составе управляющего комитета. Наличие данного документа – свидетельство зрелости корпоративной культуры.

В зависимости от результатов решения руководства в отношении концепции DRP и выделенных ресурсов проект разбивается на несколько шагов или самостоятельных подпроектов, согласованных по времени. Если «вдруг» эти подпроекты начинают конкурировать между собой за право получения очередного инвестиционного транша или иных ресурсов (технологических, человеческих и т. д.), необходимо вернуться к взаимному согласованию этапов DRP.

Проработка стратегии восстановления деятельности предполагает описание следующих моментов:

- определение сфер ответственности;
- определение критериев нештатной ситуации/аварии/крушения;
- регламент действий в условиях аварии;
- подготовка шаблонов уведомлений, их ранжирование и процедура рассылки (кому, когда, в какой последовательности);
- правила отключения/неотключения автоматизированных систем;
- процесс запуска вычислительных систем и бизнес-приложений;
- процесс восстановления сети;
- процесс восстановления рабочего места пользователя;
- процесс спасения имущества;
- процесс переезда на новую или временную площадку.

Все разделы плана должны быть четко задокументированы, все контрагенты, которые будут привлечены к реализации DRP-программы, – определены и гарантированно готовы выполнить взятые на себя обязательства. Здесь, кстати говоря, иногда могут возникнуть проблемы, связанные с дорожной ситуацией, неудачным расположением резервного офиса или отсутствием необходимых запчастей и техники на резервном складе. Приведем пример из практики компании SDN. При выборе и проектировании модульного дата-центра в Парголово (Санкт-Петербург), который начнет свою работу в январе 2014 г., было учтено множество факторов, в том числе:

- отказоустойчивая инженерная инфраструктура, обеспечивающая работу серверных ячеек и административно-бытового корпуса, где расположены резервные офисы клиентов;
- удобная транспортная доступность – вдалеке от городских пробок;
- возвышенная местность, не подверженная затоплению в период половодья;
- возможность оперативного перехода на решения высокой вычислительной плотности, предполагающие размещение резервных cloud-хранилищ и репозиториев;
- наличие собственного современного складского помещения, приспособленного для надежного хранения ИТ-оборудования.

В результате этот технологический комплекс позволяет решить целый спектр вопросов корпоративных DRP-программ.

Старайтесь придерживаться намеченного плана, но при необходимости актуализируйте задачи и ресурсы в соответствии с требованиями текущего момента (допустим, некоторые технологические решения подверглись моральному устареванию к моменту их внедрения).

Реализуя план, старайтесь пройти все этапы и обязательно тестируйте

результаты, достигнутые на промежуточных этапах. Проводите регулярные ознакомительные семинары и тренинги. Подобные учебные тревоги и моделирование бедствий позволят выявить упущенные моменты либо диагностировать вновь появившиеся угрозы. А в случае развития неблагоприятных событий – избежать паники и незапланированных потерь из категории «влияние человеческого фактора». Учитывайте особенности человеческой психологии, доводя действия персонала до осознанного автоматизма. Но и не переусердствуйте в своем рвении. График, направленный на отработку важных навыков и рефлексов, не должен ущемлять интересов бизнеса, хотя элементы внезапности в нем, возможно, должны присутствовать.

Ну и наконец, последнее. Сегодня, в эпоху активного развития облачных решений, подходы к составлению BCP&DRP-программ в корне меняются как в пространстве, так и во времени. Размещение данных в территориально распределенных cloud-кластерах существенно повышает уровень катастрофоустойчивости корпоративных информационных систем. Но, как оказалось, рынок не спешит воспользоваться открывшимися возможностями. Согласно опросу ассоциации IT Disaster Recovery Preparedness (DRP) Council, разработавшей единую систему классификации готовности к восстановлению бизнеса после стихийных бедствий и прочих нештатных ситуаций, 72% респондентов (почти три из каждых четырех компаний по всему миру) были причислены к категориям D- или F-класса (наихудшие показатели DRP-готовности). Треть опрошенных призналась в безвозвратной потере важнейших приложений, подлежащих восстановлению в течение нескольких часов. 11% компаний утратили важную информацию, на восстановление которой отводится несколько дней. Ущерб от таких простоев огромен и, по оценкам экспертов, составляет 5000 долл. в минуту. 60% из тех, кто участвовал в опросе, не имеют полностью документированного плана аварийного восстановления. При этом большинство тех, кто такие планы разработал, не считают нужным отрабатывать их на практике – 50% респондентов проводят учения только один или два раза в год, а 13% никогда. Большинство не смогло ответить, действительно ли их компания способна полностью восстановить свои ИТ-системы в случае аварии или длительного отключения электроэнергии. Так что в своей небрежности к DRP-страховке мы не одиноки. Для тех, кто хочет понять собственную ситуацию, адрес теста www.drbenchmark.org. ■

МЕЖДУНАРОДНЫЕ ДОКУМЕНТЫ ПО BCM:

- практики непрерывности бизнеса британского института BCI (Business Continuity Institute), американских институтов DRI (Disaster Recovery Institute) и SANS (SysAdmin, Audit, Network, Security Institute);
- стандарты и спецификации Британского института стандартов (British Standard Institute – BSI); руководства Австралийского национального агентства аудита (ANAO); раздел международного стандарта по информационной безопасности ISO/IEC 27001;
- стандарты и библиотеки COBIT, ITIL, MOF в части непрерывности бизнеса и др.

Алгоритм повышения надежности ИТ-инфраструктуры

Низкий уровень доверия руководителей к надежности ИТ-инфраструктур, используемых в компаниях и госучреждениях, – такой вывод сделала корпорация EMC на основании результатов выполненного по ее заказу независимого исследования Trust in IT. Опрос проводился среди 3200 ИТ-директоров и руководителей высшего звена, представляющих компании разного масштаба из 16 стран. Почти половина (45%) всех участников исследования (в России – 51%) не уверены в том, что имеющаяся ИТ-инфраструктура готова противостоять инцидентам, справляться с их последствиями, т. е. обеспечивать непрерывную доступность, безопасность, резервное копирование и восстановление данных. Указанные характеристики ИТ-инфраструктуры особенно актуальны на фоне доминирующих тенденций в сфере информационных технологий (облака, «большие данные», социальные сети и мобильность). На основании ответов 1600 ИТ-директоров были определены рейтинги ИТ-зрелости организаций, представителями которых они являются. Реализация прогрессивных стратегий, применение передовых технологий, например аналитики «больших данных», свидетельствуют о высоком уровне ИТ-зрелости (по этому показателю всего 8% опрошенных компаний можно отнести к категории «лидеров»). Главным препятствием к внедрению современных решений 52% опрошенных (в России – 62%) назвали ограниченный бюджет. Для создания и развития надежной ИТ-инфрастуктуры EMC предлагает решения, о преимуществах которых журналистам рассказали представители EMC Россия и СНГ в ходе пресс-брифинга, посвященного результатам исследования. Слагаемыми архитектуры защиты данных EMC являются: интеграция с источниками данных; единые сервисы, политики управления защитой данных и система мониторинга; интеграция с платформой защиты данных. Проблему обеспечения непрерывной доступности данных корпорация рекомендует решать на базе системы EMC VPLEX, позволяющей нивелировать сбои на уровне систем хранения, сети и ЦОД. Что касается безопасности данных, то RSA (подразделение корпорации EMC) предлагает решения, обеспечивающие классическую двухфакторную аутентификацию в сочетании с адаптивной на основе анализа «больших данных» (RSA SecurID и RSA Adaptive Authentication), обнаружение, анализ и блокировку сетевых атак и вредоносного ПО (RSA Security Analytics и RSA Sliver Tail), предотвращение утечек конфиденциальных данных (RSA DLP).

www.connect.ru