3 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.005

ВОССТАНОВЛЕНИЕ ДОСТУПНОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ БИЗНЕС-ПРОЦЕССОВ ПОСЛЕ КАТАСТРОФ

С.А. Арустамов

Изложен опыт реализации плана восстановления информационного обеспечения бизнес-процессов после катастроф на примере кредитно-финансовой организации. Приведены основные этапы разработки и внедрения резервной технической инфраструктуры бизнеса, приводятся рекомендации, повышающие качество планируемых мероприятий, предложен формальный критерий качества реализации.
Ключевые слова: доступность информации, информационно-коммуникационная структура, план восстановления бизнеса после катастроф, тестирование и верификация решения.

Введение

Общеизвестно, что уровень информационной безопасности компьютерных систем достигается обеспечением приемлемого уровня рисков нарушения конфиденциальности, целостности и доступности информационных ресурсов. Нарушение доступности информационных ресурсов может произойти в результате следующих событий:

– технический сбой аппаратных либо программных средств;
– умышленная атака на ресурсы со стороны внешних или внутренних злоумышленников;
– физическое уничтожение носителей информации или средств доступа в результате воздействия деструктивных процессов или стихийных природных явлений [1, 2].

Классификация возможных масштабов деструктивных событий приведена в табл. 1.

Уровень	Время простоя	Типичные причины	Доступность территории предприятия	Число лиц, затронутых аварией	Воздействие на предприятие
A	Не более 2 часов	Отказ нескольких рабочих станций	Да	Не более пяти	Низкое
B	Не более 8 часов	Отказ сервера, нарушение работы локальной сети	Да	Более десяти	Умеренное
C	Не более 24 часов	Затопление, длительное отключение энергии	Нет	Около 50 % сотрудников	Значительное
D	Более 24 часов	Землетрясение, наводнение, пожар, террористический акт, война	Нет	Большинство сотрудников	Критическое

Таблица 1. Классификация технических сбоев и катастроф

В настоящей статье изложен опыт автора по разработке, тестированию и внедрению плана мероприятий по ликвидации катастроф (англ. DRP, от Disaster Recovery Planning [3]) класса C и D в российском отделении западной кредитно-финансовой организации (КФО) с численностью персонала в 150 человек.

Предпосылки разработки плана мероприятий по ликвидации катастроф

Необходимым условием успешной реализации плана мероприятий по ликвидации катастроф является признание актуальности и приоритетности такого проекта руководством предприятия и выделение достаточных бюджетных средств на его реализацию.

Одним из главных факторов является удачный выбор расположения резервного офиса по критерию транспортной доступности, с одной стороны, и достаточной удаленности от основного офиса с целью обеспечения независимости его энергообеспечения и выведения его из зоны поражения, с другой. На практике для мегаполиса идеальным расстоянием между основным и резервным офисом следует считать 5–10 км. Меньшая удаленность не гарантирует сохранность резервного офиса при катастрофе, большая вызывает затруднения не только при реализации плана по факту наступления катастрофического события, но и значительно повышает стоимость тестирования решения при его верификации.

Другим фактором является учреждение (подтвержденное приказом по предприятию) комитета по антикризисному управлению (далее – Комитета), в который обязательно должны входить представители руководства в ранге членов совета директоров и руководители отделов, отвечающие за важнейшие направления деятельности. Для кредитно-финансовой организации такими представителями являются коммерческие и операционные отделы, бухгалтерия, ИТ и служба главного инженера.

Аудит информационных ресурсов и определение критического набора бизнес-процессов, необходимых для продолжения деятельности

На этом этапе принципиальным решением является определение минимального набора бизнес-процессов, которые считаются критическими для предприятия. Для КФО таким решением должен стать ответ на вопрос, является ли критичным поддержание услуги управления счетами клиентов через Интернет, можно ли ввести временный мораторий на специфические услуги, такие как отчеты по клиентским транзакциям в нетрадиционном детализированном формате, и т.п. Очевидно, что признание возможным функционирование КФО с предоставлением ограниченного набора банковских услуг в течение оговоренного времени (например в течение 3–4 месяцев, необходимых для восстановления старого офиса или поиска аренды нового) может значительно удешевить стоимость решения.

Другим важным фактором является оценка минимально возможной численности персонала, необходимого для поддержания бизнес-процессов в восстановительный период. Для удешевления проекта приходится допустить работу в две или три смены и несколько ослабить требования безопасности при выполнении бизнес-процедур (например, отказ от привлечения более чем одного сотрудника к выполнению некоторых критических операций). При этом необходимо строго контролировать уровень изменения рисков нарушения двух других компонентов безопасности (конфиденциальности и целостности информационных процессов) и избегать их недопустимого увеличения при решении задачи экономии ресурсов.

На практике при организации резервного офиса рекомендуется организовать 40–60% рабочих мест сотрудников, а также рассмотреть возможность организации двухсменной работы до полного восстановления технической инфраструктуры предприятия.

Планирование информационно-коммуникационной инфраструктуры резервного офиса

Удачная реализация этапа планирования информационно-коммуникационной инфраструктуры (ИКИ) резервного офиса напрямую зависит от качества инвентаризации информационных ресурсов предприятия и от принятия решения о наборе бизнес-процессов, поддерживаемых после начала реализации DRP. Планирование ИКИ должно охватывать два этапа:

– формирование перечня оборудования, включая ПК, серверы, сетевое и оконечное оборудование, учрежденческую АТС (УАТС) с аппаратами, линии передачи данных, осуществляющие связь резервного офиса с партнерами (для КФУ – валютная и фондовые биржи, доступ к системам REUTERS и SWIFT), регуляторами бизнес-деятельности (для КФО – Центральный банк России и налоговые органы), Интернетом, головным офисом (актуально для российских отделений западных КФО) и бизнес-приложениями, размещенных вне территории России.
– разработка политики поддержания актуальности данных (электронных документов, баз данных, содержимого корпоративных почтовых ящиков), необходимых для продолжения бизнеса после наступления деструктивного события.

При формировании перечня оборудования рекомендуется использовать в резервном офисе вычислительные платформы и линии связи с производительностью и пропускной способностью не менее, чем в основном офисе. Более того, заслуживает внимание подход, при котором резервный офис укомплектовывается оборудованием следующего поколения, по производительности превышающим имеющиеся в основном офисе вычислительные мощности. Это позволяет экономить средства на этапе поддержания DRP в актуальном состоянии при плановой смене платформ основного офиса. Следует признать неудачной политику отправки в резервный офис оборудования, списанного в основном офисе в ходе амортизации. Ожидаемая экономия средств на оснащение резервного офиса оборачивается на практике невозможностью обеспечить нормальное функционирование бизнеса после наступления деструктивного события из-за нехватки оперативной памяти, медленного исполнения приложений, несовместимости версий программного и аппаратного обеспечения, сбоев линии связи.

При предварительной настройке рабочих мест в резервной офисе важно соблюдение принципа индивидуальности, учитывающего список локальных приложений и средств доступа к удаленным ресурсам, ориентированных на ведение бизнеса конкретной группы пользователей. При игнорировании этого фактора точная настройка откладывается на период проведения тестирования качества проекта или (что еще хуже) на период после деструктивного события, что задерживает время активации резервного офиса за счет повышения нагрузки на ИТ-специалистов при наличии других неотложных задач.

Политика поддержания актуальности данных резервного офиса должна опираться на классификацию данных по степени важности для бизнеса и частоте их изменяемости. По степени важности для бизнеса данные классифицируются как критические, существенные и некритические, а по частоте изменяемости – как изменяющиеся в реальном режиме времени (динамические), изменяющиеся несколько раз в неделю/месяц (квазидинамические) и изменяющиеся время от времени при наступлении некоторых событий (квазистатические). В зависимости от типа данных применяются различные стратегии их актуализации.

Для критических динамических данных рекомендуется применять технологии переноса изменений, сделанных в основном офисе, в резервный в режиме реального времени, в частности, кластерные решения аппаратного уровня или программные решения, обеспечивающие мгновенную актуализацию (например, пакет Double Take, обеспечивающий «зеркалирование» данных по технологии источник–приемник). При обоих вариантах решения актуальной остается задача создания ежедневных резервных копий данных основного офиса, не связанных с платформами обработки данных (магнитные ленты, внешние диски), для возможности их восстановления при событиях класса A и B, так как технологии зеркалирования не защищают бизнес-пользователей от случайных потерь данных при ошибочных манипуляциях с приложениями.

При реализации программного зеркалирования рекомендуется внедрение двухэтапного процесса: на первом этапе данные зеркалируются с продукционного сервера

на резервный, находящийся в основном офисе (необходимый для восстановления данных после событий класса А и В), а на втором этапе передаются на сервер резервного офиса. При таком подходе удается значительно снизить нагрузку на продукционный сервер, так как при одноэтапном зеркалировании непосредственно через канал связи между продукционным сервером и сервером резервного офиса бизнес-пользователи чувствуют значительное замедление работы приложений продукционного сервера, связанное с замедлениями при удаленной передаче данных от источника к приемнику. При реализации этой технологии немаловажное значение играет обоснованный выбор пропускной способности канала передачи между основным и резервным офисами, который должен осуществляться с учетом объемов данных, передаваемых в реальном режиме времени, и цикличности бизнес-процедур.

Для квазидинамических и квазистатических данных политика актуализации заключается в создании копий на магнитных носителях (ленты, внешние диски) и регулярной их доставке в резервный офис. В ряде случаев приходится идти на разумные компромиссы. Например, несмотря на высокую частоту изменения данных корпоративных почтовых ящиков, которые являются примером динамических данных, их, ввиду среднего уровня критичности, приравнивают к квазидинамическим данным и вместо актуализации в реальном режиме времени применяют еженедельную доставку обновленных копий в резервный офис. Принятие таких компромиссных решений возможно только при условии их утверждения Комитетом с последующим информированием об этом решении бизнес-пользователей. Схема ротации носителей с данными между основным и резервным офисами и их общее количество должна быть строго согласована с принятой политикой восстановления доступности данного типа данных. При этом необходимо помнить об ограниченном ресурсе магнитных носителей при часто повторяющихся процедурах перезаписи и своевременной замене носителей, выработавших свой ресурс.

При оснащении резервного офиса телекоммуникационной инфраструктурой следует руководствовать следующими принципами:

– заказ каналов передачи данных, голосовой связи и оборудования для телефонизации офиса должен производиться с привлечением провайдеров, не задействованных при оснащении основного офиса;
– при организации тендера на подобные проекты предпочтение должно отдаваться провайдерам, использующим альтернативные арендные мощности и узлы коммутации, находящиеся в районах города, удаленных от районов размещения узлов коммутации провайдеров основного офиса. Желательно также затребовать данные, подтверждающие наличие проекта DRP у претендентов на провайдеры. Последнее обстоятельство актуально при проведении тендера на заключение договоров о предоставлении телекоммуникационных услуг и в основном офисе.

Подобная политика преследует цель уменьшения рисков повреждения технической инфраструктуры провайдера при локализации деструктивного события в пределах некоторой зоны. Ярким примером такого события является «блэкаут» (одновременное прекращение энергопитания во многих районах) Москвы, имевший место 25 мая 2005 г.

Документирование процедур DRP и осведомленность бизнес-пользователей

Важным этапом разработки DRP, во многом определяющим его успешную реализацию, является его детальное документирование, включающее описание отдельных процедур, регламентирование ответственности членов Комитета и сотрудников, реализующих процедуры восстановления, и осведомленность бизнес-пользователей в отношении существования такого плана и перспектив восстановления технической инфраструктуры бизнеса после деструктивных событий. При составлении такого документа

важно детально описать процедуры оповещения сотрудников об объявлении активации плана, места сбора и маршрут следования до резервного офиса. Оповещение сотрудников организуется на основе так называемого «дерева вызовов» (call tree), согласно которому первоначально оповещается ограниченное число ответственных сотрудников, которые, в свою очередь, «спускаясь» по дереву вызовов, доводят информацию до своих подчиненных. Документ должен содержать графическую информацию о месте нахождения резервного офиса и детальный маршрут следовании со стрелками, указывающими направление движения. В резервном офисе на каждом рабочем месте необходимо оставить подробную инструкцию, описывающую условия работы в экстремальных условиях на родном языке. Последнее требование специфично для зарубежных организаций, ведущих бизнес на территории России, в которых многие регламентирующие документы составлены на английском языке с целью инспектирования представителями заграничного руководства.

Отдельный документ необходимо подготовить для сотрудников отдела ИТ. В документе необходимо указать последовательность действий по активации ИКИ резервного офиса, которая должна учитывает приоритетность восстановления информации с учетом ее критичности и частоты изменения и способы информирования бизнес-пользователей о готовности отдельных систем к эксплуатации. Особое внимание следует уделить распределению обязанностей и распараллеливанию независимых процессов восстановления данных с целью минимизации времени активации ИКИ и методам быстрого контроля актуальности и целостности данных, переданных в резервный офис по каналу связи, возможности корректного открытия баз данных и других проверок, подтверждающих работоспособность ИКИ.

Тестирование работоспособности плана DRP и верификация корректности его реализации

Отработка основных положений документов для пользователей и служб ИТ проводится в ходе регулярных тестов, имитирующих различные ситуации, возникающие после деструктивных событий. При организации теста отправной точкой является определение модели деструктивного события (например, пожар, уничтоживший все здание). Как это ни парадоксально, отработка тестов по модели полного уничтожения офиса является более простой задачей, чем введение модели частичной деструкции ресурсов (например, затоплен первый этаж, но есть возможность эксплуатации остальных). В последнем случае приходится рассматривать множество вариантов частичного перемещения сотрудников в основной офис и модифицировать бизнес-процессы, объединяющие отделы, оказавшиеся после катастрофы в удалении друг от друга. Это сильно усложняет реализацию единого плана из-за многообразия вариантов частичной деструкции. Практически при тестировании ограничиваются ситуацией полного уничтожения офиса.

Ввиду невозможности совмещения тестирования с повседневными задачами бизнеса тестирование проводится в один из выходных дней, что усложняет задачу проверки процедур взаимодействия с бизнес-партнерами (например, пересылку тестовых платежей в платежную систему ЦБ России). При организации тестирования важно предусмотреть наличие тестовых копий продукционных баз данных с целью исключения искажения бизнес-данных в ходе тестирования, разработать контролируемые процедуры доступа к ним и процедуры возвращения (так называемого «отката») пользователей и ИКИ в обычный бизнес-режим.

В качестве индикатора качества верифицируемого решения можно предложить коэффициент K количества обращений пользователей к службам ИТ по поводу недоступности данных или невозможности реализации отдельных процедур:

$K = L/(P \cdot N)$,

где L – общее число обращений, P – число тестируемых процедур, N – число пользователей, участвовавших в тесте.

Заключение

В работе приведена классификация деструктивных событий, воздействующих на информационное обеспечение бизнес-процедур, разработана методика создания ИКТ резервного офиса, включающая организационные и технические решения, предложен формальный критерий качества решения.

Литература

1. Шаньгин В.Ф.. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.
2. Белов Е.В., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. – М.: Горячая линия – Телеком, 2006. – 544 с.
3. Компания КРОК. План восстановления данных после аварии (DRP) [Электронный ресурс]. – Режим доступа: http://www.croc.ru/solution/it_consulting/drp.php#top, свободный.

Арустамов Сергей Аркадьевич — Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор технических наук, профессор, sergey.arustamov@gmail.com