

Резервный центр как инструмент обеспечения непрерывности бизнеса



↑
Марк КУПЕРМАН,
ЗАО «Информсвязь Холдинг»



↑
Дмитрий АВЕРЬЯНОВ,
ЗАО «Информсвязь Холдинг»

Практически все крупные ведомства и корпорации имеют информационно-телекоммуникационные системы, обеспечивающие доступ к коллективным информационным ресурсам и коммуникационным сервисам. Для ряда таких систем вопросы надежности носят принципиальный характер. Однако резервирования важнейших узлов путем установки резервного комплекта рядом с основным не всегда достаточно для обеспечения непрерывности их работы.

Непрерывность бизнеса

Воздействие внешних факторов на ИТ-инфраструктуру компании, возникновение различных нештатных ситуаций несут в себе постоянную угрозу остановки бизнес-процессов компании. Поэтому тема управления непрерывностью бизнеса (Business Continuity Management, BCM) имеет давнюю историю. Управление доступностью, непрерывностью и мощностями, оценка рисков остановки бизнес-процессов, планы обеспечения непрерывности деятельности компании и восстановления после аварии – эти и другие подобные мероприятия описываются международными, национальными стандартами и рекомендациями, включены в фирменные методики ведущих ИТ-компаний и даже в банковские нормативные акты. Однако ISO/IEC 20000, ITIL, COBIT, BS 25999 и аналогичные документы не отвечают на вопрос: как построить ИТ-инфраструктуру, гарантирующую необходимый уровень непрерывности бизнеса?

Обеспечение непрерывности бизнеса, как правило, тесно связано с резервированием. Но пока нет полной ясности, в каких случаях необходимы резервные компоненты, каковы требования к ним, как их классифицировать по степени отказоустойчивости. Как известно, «нельзя управлять тем, что нельзя измерить» – следовательно, при отсутствии методик количественной оценки непрерывности бизнеса как-то странно говорить о BCM. Даже обоснование коэффициента готовности отказоустойчивых систем сегодня остается ско-

рее философским вопросом, нежели математической задачей (см. «Правда «пяти девяток», «ИКС» №6, с. 84). Ясно одно: если от простоя информационных (платежных, телекоммуникационных и т.д.) систем компания несет убытки, для защиты ее критически важных бизнес-процессов необходим резервный центр.

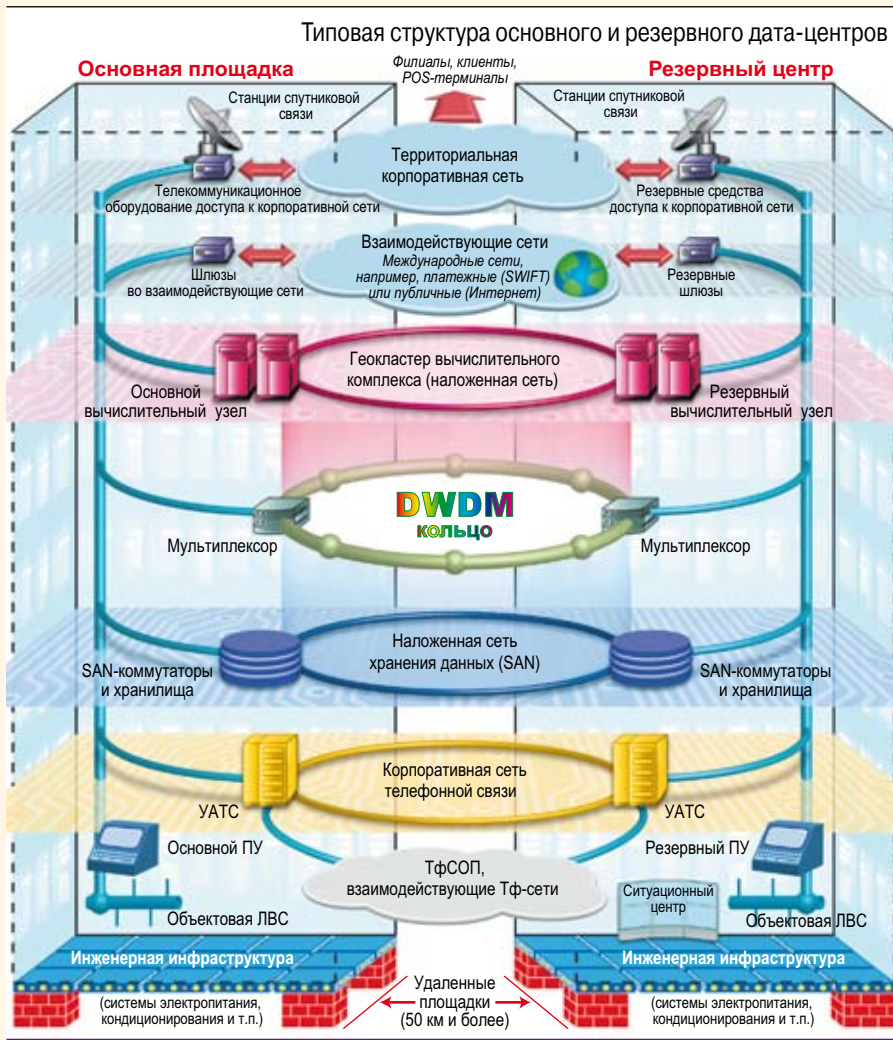
Катастрофоустойчивые ЦОДы

В обеспечении бизнес-процессов корпораций и государственных организаций фактор надежности корпоративной сети и информационных систем вносит основную долю рисков, связанных с потерей данных или недоступностью информационных сервисов. Чтобы обеспечить стабильность управления госструктурами или непрерывность бизнеса коммерческих организаций, помимо основных информационных систем предусматриваются резервные. Основу их составляют резервные центры обработки данных (ЦОДы), или дата-центры.

На резервный ЦОД возлагается основная задача обеспечения непрерывности вычислительного процесса при выходе из строя основных систем. Чтобы обеспечить толерантность базовых сервисов ИТ- и коммуникационных систем к различным аварийным ситуациям, на резервной площадке размещают дублирующий комплект серверов и телекоммуникационного оборудования; необходимы также механизмы переключения информационных нагрузок и механизмы репликаций для поддержания актуальной копии данных.

Централизация, повышение эффективности вычислений, рост объемов информации наряду с ужесточением требований к уровню ее сохранности и непрерывности процесса обработки – всё это обусловило сочетание двух подходов: консолидации информационных ресурсов в составе ЦОДа и структурного резервирования их аппаратно-программных комплексов. Повышенный интерес к резервным центрам объясняется, прежде всего, необходимостью обеспечить катастрофоустойчивость ядра ИТ-инфраструктуры организации. Типовое решение этой задачи – территориальное разнесение узлов обработки и хранения данных. Поэтому в целом наиболее эффективным будет резервирование совместно с территориальным разнесением ЦОДов. Это обеспечивает максимальный уровень живучести системы под воздействием как локальных деструктивных факторов (отказы аппаратуры, сбои программного обеспечения, случайные ошибки или злонамеренные действия пользователей), так и внешних угроз (террористический акт, пожар, затопление, авария в сетях энергоснабжения или сетях передачи данных провайдера, другие техногенные катастрофы и стихийные бедствия).

Таким образом, резервный центр, удаленный от основной площадки, обеспечивает не только отказо-, но и катастрофоустойчивость, определяющую максимальный уровень живучести ядра информационно-телекоммуникационной системы (ИТКС) и, следовательно, минимальный риск остановки бизнес-процессов организации.



Обеспечение катастрофоустойчивой конфигурации ИТКС организации (ведомства) – весьма непростая и затратная задача, поэтому такие конфигурации имеют смысл лишь для ответственных применений. Широкое распространение резервные центры получили в банковском секторе, где бизнес, включая вопросы репутации, находится в прямой зависимости от доступности информационной системы. В данном случае высокая цена простоя платежных систем способна оправдать строительство резервного центра.

Обычно серьезные проблемы в банковских ИТ-системах тщательно скрывают, поскольку они могут отразиться на лояльности клиентов и престиже банка в целом. Поэтому примеры зависимости эффективной работы финансовых учреждений от качества функционирования ИТ-систем приходится брать из практики крупнейших зарубежных

бирж, где факты простоев в результате остановки информационных систем широко известны. В апреле 2000 г. в течение восьми часов (почти всю торговую сессию) были парализованы торги на Лондонской фондовой бирже (LSE) из-за ошибок в работе программного обеспечения. Заметим, что на бирже эксплуатировались наиболее надежные FT-системы того времени с коэффициентом готовности свыше 99,999%. Убытки составили несколько миллионов фунтов. В сентябре 2008 г. снова на LSE был зафиксирован сбой, повлекший за собой остановку ее работы на четыре часа. Кроме прямых потерь – а около 40% дохода биржи приходится на продажу информации о курсах акций в режиме реального времени, – сбой на LSE сыграл на руку ее конкурентам. Известны случаи крупных аварий, в результате которых были остановлены критически важные

сервисы, на других торговых площадках, включая Токийскую фондовую биржу и NASDAQ.

В нашей стране резервные центры имеют Банк России, Альфа-Банк, Банк ВЕФК, Московский кредитный банк, подразделения Сбербанка и другие банки. Резервные центры широко распространены в Министерстве обороны и других силовых ведомствах; например, крупный резервный ЦОД внедряется в интересах пограничной службы для обработки данных биометрических загранпаспортов граждан России.

Структура основного и резервного центров

Чтобы создать системы, толерантные к серьезным авариям и катастрофам, используют территориальное разнесение вычислительных платформ и информационных хранилищ, организуя кампусные, метро- и континентальные кластеры. Для катастрофоустойчивых геокластеров разнесение узлов, как правило, составляет не менее 50 км. На рисунке представлена типовая структура основного и резервного центров, основанная на геокластерах. В ней выделены три основных элемента обеспечения катастрофоустойчивости:

- протяженная скоростная магистраль, соединяющая обе площадки (в данном случае в виде DWDM-кольца);
- вычислительный геокластер (с узлами кластера на основной и резервной площадках);
- геокластер систем хранения (Storage Area Network, SAN).

Чтобы обеспечить непрерывность вычислений, резервный центр обычно работает в режиме горячего резервирования. При этом подразумевается, что резервный узел всегда имеет актуальную информацию (путем репликации информации с основного узла) и готов незамедлительно переключиться на обслуживание задач.

Структура и элементы дата-центра на рисунке даны обобщенно, для каждого вертикального рынка можно подставить свои конкретные элементы. Например, для банковского сектора «шлюз в другие сети» может означать шлюз в международную сеть SWIFT.

Кроме ядра резервного центра – резервного ЦОДа, который обеспечивает основные операции автоматического обнаружения отказов, переконфигурирования системы для снятия нагрузки с неисправных комплексов и переключения ее на резервные, – важную роль играют и другие подсистемы. Даже в штатном режиме требуется постоянный детальный мониторинг всех систем (который обычно ведут системы управления телекоммуникационным оборудованием и вычислительными комплексами), например, в целях анализа сетей или вычислительных процессов для их оптимизации и прогнозирования нештатных ситуаций. Кроме того, при эскалации проблем необходим переход на автоматизированное или ручное управление; при этом требуется знание предварительной обстановки и возможных сценариев устранения проблем. Заранее должны быть решены организационные задачи, предусматривающие ряд оперативных мероприятий для обнаружения и нейтрализации нештатных ситуаций, включая разработку аварийного плана действий (disaster recovery plan), в том числе для переключения информационных сервисов и восстановления работоспособности основного узла. Следует иметь в виду, что даже самая надежная вычислительная платформа, например, класса Permanent Availability, не сможет функционировать при отказе инженерной инфраструктуры, включая системы энергоснабжения и кондиционирования, а также системы их мониторинга и управления ими.

В задачи системы эксплуатации резервного центра входит контроль и поддержка работоспособности

аппаратно-программных средств центра в зависимости от наличия нештатной ситуации или степени ее опасности. Для системы эксплуатации можно предусмотреть переменный количественный состав, который легко оперативно нарастить из штатного состава служб эксплуатации основной площадки.

При возникновении чрезвычайных ситуаций или длительного восстановления основной площадки может оказаться недостаточно переключения на аппаратно-программные резервные элементы. Для обеспечения непрерывного управления ИТ-системой организации, поддержания ее штатной функциональности силами резервного центра предусматривают заблаговременно подготовленные рабочие места для руководства и технического персонала, а также других структурных подразделений. Степень развертывания этих элементов увеличивается по мере эскалации проблем и деградации элементов основной площадки. Учитывая особенность работы резервного центра, целесообразно включать в его состав элементы, способствующие более эффективному решению управленческих задач в сложной обстановке и в условиях дефицита времени. Одним из таких элементов является ситуационный центр. Он позволяет повысить качество принимаемых решений путем визуализации информационного потока, а также результатов анализа, моделирования и прогнозирования развития нештатных ситуаций.

Развертывание перечисленных выше подсистем, на первый взгляд, может показаться излишним даже для крупного банка. Однако энергетиче-

ский коллапс в Москве в мае 2005 г. показал уровень толерантности эксплуатируемых систем. Торги на биржах были остановлены, многие банки вынуждены были прекратить работу части офисов и филиалов. Некоторые даже выступили с официальным обращением к гражданам о «возможных временных затруднениях в обслуживании клиентов банка».

Учитывая, что сегодня банковские системы, как правило, ведут централизованную обработку платежной и другой информации, даже наличие автономных источников электроэнергии на основной площадке не гарантирует им связь с внешними объектами (филиалами, клиентами, другими платежными сетями). Нет гарантий работоспособности всей цепочки операторов связи в проблемном регионе. Кроме того, работа руководства и структурных подразделений организации на основной площадке в таких условиях будет затруднена дефицитом энергии из-за повышенного энергопотребления резервных источников. От способности безболезненно переносить подобные коллапсы и любые другие катаклизмы зависит, например, финансовая устойчивость и престиж банка. Поэтому все более широкое применение находят резервные центры, позволяющие нивелировать последствия не только технических аварий и ошибок обслуживающего персонала, но и крупных пожаров, обрушения зданий, заражения опасными программными вирусами, террористических актов (и ложных сообщений о них) и прочих чрезвычайных ситуаций. ИКС

Холодоснабжение и кондиционирование дата-центров от проекта до технического обслуживания на базе оборудования RC Group



Реклама



RC GROUP

ВЕНТСПЕЦСТРОЙ
VENTCONSTRUCTION

www.ventss.ru • info@ventss.ru • (495) 775-37-91