

### «Хочешь мира — готовься к войне»

Если произошла авария в основном офисе, то одного только восстановления данных обычно бывает недостаточно. Ведь главное — это обеспечение непрерывности ведения бизнеса. Задача это комплексная, следовательно, и решать ее надо комплексно...

Многие компании наверняка оказывались в ситуации, когда им приходилось переезжать на другое место: офис, этаж, да хотя бы комнату. Если этот процесс запланирован, тогда еще ничего. Можно спокойно переехать, без особых потерь для бизнеса. А как быть, если переезд не запланирован? Если, например, произошла авария: обрушилось перекрытие, затопило серверную комнату, неожиданно сработала система пожаротушения (или наоборот не сработала, и весь офис сгорел дотла L). В общем, может произойти множество неприятностей, которые способны остановить сердце любого бизнеса — ИТ-инфраструктуру. Не факт, что подобные неприятности когда-нибудь обрушатся на вашу голову, однако к ним надо быть всегда готовым! Надо всегда оставаться в тонусе.

Когда приходит сигнал об аварии, неподготовленные просто впадают в панику. Много вопросов и мало ответов, вероятность человеческой ошибки велика. Куда бежать? Что брать? А если нужных ресурсов нет? Где резервные копии? А они вообще были? Когда последний раз выполнялось резервное копирование? Кто за что отвечает? В итоге — полный хаос и неразбериха. Бизнес стоит. И восстановить его в такой ситуации уже не просто.

Чтобы такая ситуация не возникла ни при каких обстоятельствах, ответы на перечисленные вопросы стоит найти заранее. Конечно, в каждом конкретном случае детальные инструкции на случай аварии являются сугубо индивидуальными для каждой компании. Однако из опыта системных интеграторов можно выделить некоторые общие моменты организации действий в штатных ситуациях.

Выбор резервной площадки. Первоочередная задача и, вместе с тем, одна из самых трудных. Хорошо, если у вас уже есть один или несколько территориально удаленных филиалов, между которыми уже налажено взаимодействие. А если нет?

В этом случае можно прибегнуть к одному из следующих вариантов:

- 1) Создать резервный офис (со всеми вытекающими последствиями).
- 2) Выделить в филиале места для главного офиса. То есть в случае аварии главный офис переезжает в один из филиалов на заранее подготовленную площадку. Этот метод имеет значительное преимущество перед первым, поскольку в случае переезда «пострадавшие» сразу оказываются в реально работающем офисе. Так или иначе, но филиал функционирует и может на какое-то время «приютить» «погорельцев» (работников главного офиса).
- 3) Обратиться в компанию, которая представляет услуги по обеспечению непрерывности бизнеса (по западной терминологии business recovery solution или BRS). Такой подход получил большое распространение на Западе (что не удивительно в «эру аутсорсинга»). В Украине также есть ряд компаний, готовых «за умеренную плату» содержать для вашей организации резервную площадку, и в случае аварии обеспечить всем необходимым для продолжения ведения бизнеса — от серверов и каналов связи до рабочих столов и канцелярских принадлежностей (все зависит от суммы контракта). Кроме этого фирма, предоставляющая услуги BRS, может предоставить заказчику также и квалифицированный персонал: специалистов, консультантов и др. (для достижения максимально короткого времени восстановления бизнеса).

Подготовка инфраструктуры. Для нормальной работы резервной площадки ее надо подготовить, создать подходящую инфраструктуру. Что же там должно быть? Воображение рисует сначала технику. Но ведь кроме техники там надо восстановить бизнес! Что для этого нужно?

1) Первое и главное — это коммуникации: резервные каналы с АТС, Интернетом, связь с другими филиалами и т.д. Здесь проявляется еще одно преимущество создания резервного центра в собственном филиале. Все эти «запасные» каналы могут в этом случае не простаивать (как при создании «законсервированной» резервной площадки), а использоваться для работы филиала, в случае аварии их просто «уступают» вновь прибывшим работникам.

2) Критическое оборудование. Это серверы, системы хранения данных, коммутаторы, маршрутизаторы, модемы и т.д.

3) Инфраструктура для персонала. Тоже немаловажная часть. Она включает столы, стулья, тумбочки, шкафчики и другие предметы, необходимые для работы.

Ответственный персонал. Это самое главное в деле восстановления после аварии, без него никто ваш бизнес не восстановит. Ответственные должны быть всегда (хотя бы для того, чтобы с кого-то спросить за последствия аварии).

Если организация достаточно крупная и в штате не десять человек, а сотни или даже тысячи, на резервной площадке всем может элементарно не хватить места. А если даже и хватит, все равно сложно наладить слаженную работу достаточно быстро. Поэтому необходимо выбрать некоторое количество квалифицированных сотрудников, которые могут поддерживать функционирование бизнеса и его восстановление до подхода «основных сил» или до момента восстановления основного офиса. Второй важный аспект — тотальное документирование. Персонал должен иметь четкие инструкции по работе на случай аварии. Каждый работник должен знать, за что конкретно он отвечает, как надо действовать в случае аварии, где его временное рабочее место, с кем он должен контактировать по каким вопросам и т.п.

Доставка персонала. Обязательно должен быть план доставки персонала до нового места работы: каким транспортом это будет осуществляться, сколько времени будет затрачено на дорогу, где быстро взять новых работников (если те, что есть, пострадали) и т.д. Кроме этого должен быть план возврата на старое место работы (ведь компании не вечно работать на резервной площадке).

Детальный временной план, описывающий все действия с момента наступления аварии до момента полного восстановления бизнеса. После стольких затраченных усилий нельзя допустить, чтобы что-то пошло «не так», поэтому следует провести тестирование «аварийного» плана — провести учения. То, что у нас есть план, это хорошо. Но не протестировав его, мы не сможем убедиться в том, что он действительно работает. Тестирование помогает выявить скрытые недостатки и пути их устранения, проверить работоспособность или что-то улучшить.

Так или иначе, но общий подход к организации любого катастрофоустойчивого решения сводится к одному предложению: «чем меньше время восстановления, тем меньше убытки», из него и следует исходить.

*Автор:*

*Александр НОВАК,*

*начальник отдела продаж IBM System p и TotalStorage ООО «System Integration Service»*

*Опубликовано в журнале «СЕТИ И БИЗНЕС» № 2 (21) 2005*

---