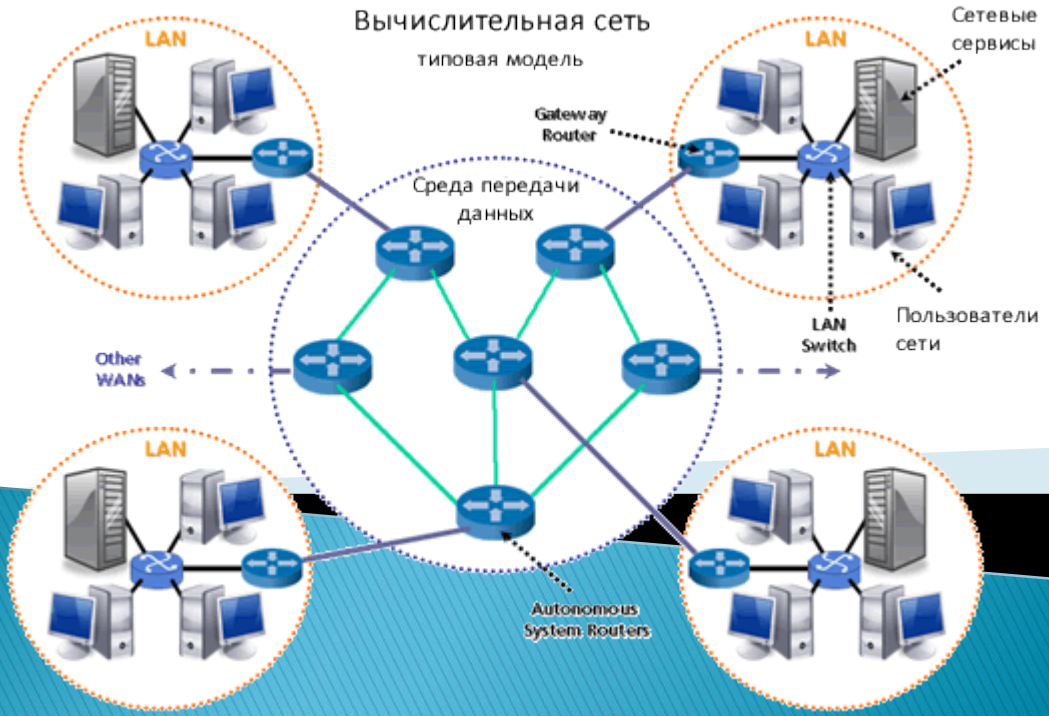
Д„  ”Я

 ” 

Ц 

,#

Послеаварийное восстановление работоспособности сети



Возможность полной потери данных при отсутствии программы послеаварийного восстановления ставит под угрозу деятельность организаций, не располагающих средствами для восстановления работоспособности после катастрофических событий.

Шесть этапов планирования

В терминологии планирования действий в аварийных ситуациях фигурируют два общих понятия:

- **планирование сохранения непрерывности бизнеса (Business Continuity Planning, BCP)**
- **планирование послеаварийного восстановления (Disaster Recovery Planning, DRP).**

Эти понятия, часто используемые как равноценные, представляют различные концепции.

- **BCP** традиционно предусматривает планирование мероприятий, обеспечивающих сохранение деловой активности организации в чрезвычайных ситуациях.

- Сфера ответственности **DRP**, по сути, представляет подмножество BCP и касается восстановления информации и работоспособности систем в случае аварии.

Планирование мероприятий BCP и DRP – дело непростое, и в крупных организациях этим часто занимаются специальные группы.

Однако даже без детального анализа степеней риска и решения прочих сложных вопросов в рамках BCP и DRP в крупных компаниях можно создать программу сохранения целостности бизнеса и послеаварийного восстановления, если придерживаться ниже приведенным этапам.

Этап 1. Определение критически важных деловых операций

Первый шаг планирования в рамках BCP и DRP – определение критически важных деловых операций, т.е. действий, которые должны выполняться в повседневном режиме для сохранения работоспособности организации.

На данном этапе планирования необходимо сотрудничать с главными ответственными лицами организации в определении видов деятельности, важных для сохранения ее работоспособности.

В центре планирования мероприятий в рамках BCP находится сохранение деловой активности организации за счет восстановления этих видов деятельности.

Этап 2. Составление схемы инфраструктуры информационных систем, обеспечивающих выполнение критически важных деловых операций.

Работа отдельного отдела зависит от работоспособности серверов базы данных, где хранятся данные, и приложений, обеспечивающих доступ к этим серверам.

Кроме того, должна функционировать определенная часть центральной сетевой инфраструктуры, чтобы эти критически важные деловые операции могли выполняться.

Перечисленные выше информационные системы необходимо поддерживать в работоспособном состоянии за счет оперативного послеаварийного восстановления.

Этап 3. Модели угроз в виде предсказуемых и вероятных событий

- Практически все катастрофы и аварии, угрожающие целостности бизнеса, являются предсказуемыми с определенной степенью вероятности. Катастрофические события могут быть природными (землетрясение, наводнение) либо механическими (неисправность жесткого диска, разрыв водопроводной трубы и т. д.).

- Определив критически важные системы, можно приступать к моделированию угроз со стороны предсказуемых и вероятных событий.

- Моделирование позволяет реализовать структурный подход к определению потенциальных угроз, несущих в себе максимальную опасность для целостности бизнеса, и ослаблению их негативных последствий.

Этап 4. Разработка планов и процедур сохранения целостности бизнеса

- После составления списка критически важных деловых операций, перечисления информационных систем, обеспечивающих их выполнение, и определения возможных и вероятных событий, способных нарушить работоспособность указанных информационных систем, приступают к выработке превентивных мер, имеющих целью сохранение целостности бизнеса, с использованием моделей угроз.

В рамках BCP существуют четыре категории превентивных мер

- Отказоустойчивость и восстановление после сбоя
- Резервное копирование
- «Холодное» запасное оборудование и помещения
- «Горячее» запасное оборудование и помещения

Отказоустойчивость и восстановление после сбоя

Эта категория превентивных мер предполагает использование резервируемых аппаратных средств, сохраняющих работоспособность при отказе отдельных элементов.

В ИТ для обеспечения отказоустойчивости наиболее широко используются массивы жестких дисков, технологии кластеризации, аккумуляторные и генераторные источники питания.

Резервное копирование

Резервное копирование с использованием внутрисистемных и внесистемных средств занимает центральное место среди превентивных мер в рамках DRP.

В случае утраты данных резервное копирование обеспечивает возможность восстановления и реконструкции информации по последним данным, соответствующим работоспособному состоянию систем.

«Холодное» запасное оборудование и помещения

«Холодное» запасное оборудование — это автономные устройства, которые можно быстро подготовить к выполнению рабочих функций.

В случае аварии можно завершить настройку конфигурации и восстановить либо скопировать данные, необходимые для возобновления работы.

«Холодное» помещение вмещает автономное оборудование, которое можно использовать для возобновления работы в случае аварии на главном оборудовании.

«Горячее» запасное оборудование и помещения

«Горячее» запасное оборудование – это устройства, готовые к немедленной работе в чрезвычайной ситуации.

«Горячее» оборудование позволяет очень быстро возобновлять выполнение операций. Скорость приведения «горячего» оборудования в работоспособное состояние обычно определяется временем, необходимым сотрудникам для прибытия к месту хранения запасного оборудования.

«Горячее» оборудование располагает точными копиями данных в реальном времени (или почти в реальном времени) и всегда работоспособно.

Этап 5. Разработка планов и процедур послеаварийного восстановления

Для серьезных катастроф, в которых возможна полная потеря данных и работоспособности главных систем, необходима разработка планов и процедур восстановления.

Поскольку послеаварийное восстановление относится к стрессовым ситуациям, очень важно иметь под рукой хорошо документированные, проверенные и испытанные на практике процедуры.

Убедиться в работоспособности данных, хранящихся на резервных носителях, можно в режиме имитации работы процедур восстановления.

- Необходимо позаботиться о средствах внесистемного хранения копий процедур, выполняемых в рамках DRP, вместе с проверенными работоспособными резервными копиями.

Этап 6. Проверка работоспособности планов сохранения целостности бизнеса и испытание на практике средств послеаварийного восстановления

- Необходимо проводить планируемые и спонтанные учения для проверки состоятельности стратегий BCP и DRP.
- Можно раз в месяц имитировать отказ кластерных узлов, периодически выполнять восстановление «холодных» запасных серверов либо проводить полномасштабные имитации катастрофических ситуаций с проверкой работоспособности «холодных» и «горячих» средств восстановления.
- Как минимум, следует выполнить восстановление критически важных данных по резервным копиям с хранящихся вне офиса носителей. Хранящиеся вне офиса носители резервных копий – последняя линия защиты от полной утраты данных.