МЕХАНИЗМ САМОНАСТРОЙКИ СИСТЕМЫ ЗАЩИТЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

В.Б. Гусев, В.В. Павельев
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., д. 65
E-mail: gusvbr@ipu.ru, pavvvs@ipu.ru

Предложена методика выбора механизма саморегулирования в процессе эксплуатации системы защиты от аварий и катастроф выделенного центра обработки данных в территориально-распределенной автоматизированной системе, построенной с использованием каналов глобальных сетей связи. Механизм ориентирован на достижение оптимального режима эксплуатации в смысле минимизации комплексной оценки ущерба и затрат при выполнении технических требований к системе.

THE SELF-REGULATION MECHANISM FOR THE PROTECTION SYSTEM OF DATA PROCESSING CENTER / V.B. Gusev, V.V. Pavelyev (Institute of Control Sciences of RAS, 65 Profsoyuznaya st., Moscow, 117997, Russia). The procedure of the selection of the mechanism of self-regulation in the process of operating the system for protection from emergencies and catastrophes of the chosen data processing center in the territorial-distributed automated system, built with the use of channels of global communication networks is proposed. Mechanism is oriented to reaching of the optimum regime of operation in the sense of the minimization of the integrated assessment of damage and expenditures with fulfilling of technical requirements for the system.

Введение

В настоящее время многие организации начали целенаправленно внедрять технологии обеспечения непрерывности бизнеса в непредвиденных ситуациях (BCP — business continuity planning). Учитывая, что затраты на внедрение и эксплуатацию таких технологий составляют значительную долю ресурсов многих организаций, важное значение приобретает проблема оптимизации этих затрат. Принятие ответственных решений по выбору схемы защиты от аварий и катастроф центров обработки данных требует комплексной оценки рассматриваемых вариантов. При этом в качестве основных критериев выступают следующие показатели:

- возможный ущерб от нарушения нормальной работы автоматизированной системы в результате выхода из строя центра обработки данных;
- вероятность наступления событий, наносящих существенный ущерб;
- затраты (капитальные и эксплуатационные) на мероприятия по защите центров обработки данных от аварий и катастроф.

В связи с этим, актуальной является задача разработки методики анализа потенциальных угроз и оптимального механизма самонастройки системы защиты от них центров обработки данных.

При эксплуатации любых автоматизированных систем всегда существует определенная вероятность разрушения информационных массивов (ИМ) и программных модулей (ПМ). При использовании каналов глобальных сетей связи и децентрализованном хранении резерва возможно быстрое возобновление работы при выходе из строя одного из узлов, содержащего рабочие информационные массивы и программные модули. Зависимость финансовых потерь, которые несет организация из-за недоступности IT-сервисов, от времени их недоступности приведена на рис. 1. Здесь же приведена зависимость стоимости создания системы высокой доступности от величины допустимого времени простоя. Величина финансовых потерь, как правило, растет нелинейно, нелинейная зависимость наблюдается и у величины затрат на мероприятия по обеспечению непрерывности IT-сервисов от гарантированного времени восстановления.

Оптимальное решение обычно лежит в области, которая на рисунке обозначена как окно соотношений «стоимость/время восстановления» [1].

Основными технологиями, обеспечивающими защиту данных в чрезвычайных ситуациях, являются:

- резервное копирование и архивирование данных на удаленной площадке (Crossite backup) с размещением их на внешних накопителях;
- различные способы репликации данных на удаленную площадку с размещением их на дисковых массивах.

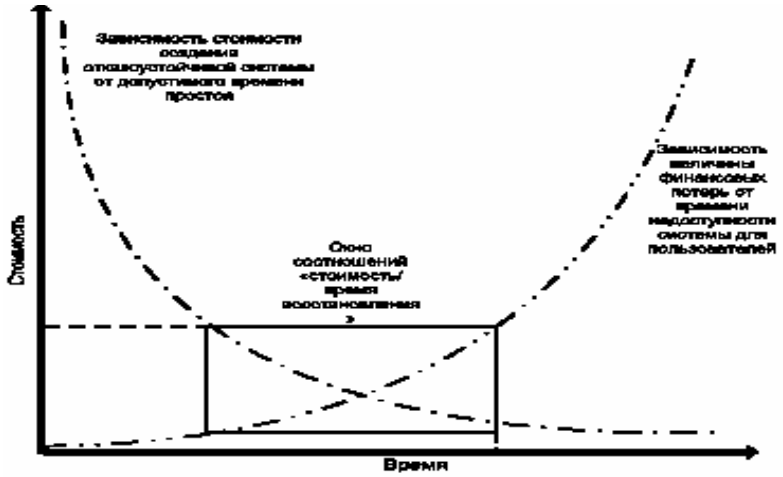


Рис. 1. Зависимость финансовых потерь из-за недоступности IT-сервисов от времени их недоступности и стоимости создания системы высокой доступности от величины допустимого времени простоя.

1. Основные схемы организации резервирования информационных массивов и IT-сервисов в территориально-распределенных системах.

При проектировании IT-инфраструктуры современных территориально-распределенных автоматизированных систем в настоящее время обычно используются архитектуры, предусматривающие создание одного или нескольких центров обработки данных (ЦОД), иногда находящихся на значительном расстоянии друг от друга. Приняв за основу 7-ми уровневую (0…–6) классификацию построения систем резервирования и управления данными и доработав ее на основе российского и международного опыта построения территориально-распределенных IT-архитектур с выделенными центрами обработки данных [1-6] предлагается выделить 10 наиболее распространенных схем организации резервирования информационных массивов и IT-сервисов в территориально-распределенных IT-инфраструктурах с выделенными центрами обработки данных:

1. Производится регулярное резервное копирование ИМ и ПМ с хранением резервных копий в том же помещении/здании.
2. Производится регулярное резервное копирование с хранением резервных копий в отдельном помещении/здании.
3. Используются технологии резервного копирования и архивирование данных на резервную площадку .
4. Используются технологии резервного копирования и архивирования наиболее критичных данных на резервную площадку по каналам связи .
5. Репликация данных на резервную площадку в асинхронном режиме (с небольшим запаздыванием).
6. Репликация данных на резервную площадку в синхронном режиме.
7. Оперативное резервирование. Режим постоянной готовности. Репликация данных на резервную площадку осуществляется в синхронном режиме.
8. Вычислительный центр распределен по нескольким площадкам, находящимся на удалении не более 50 км (в пределах одного города). В этом случае из нескольких площадок можно создать единый вычислительный центр, рассматривая их просто как разные комнаты в одном здании.
9. Вычислительный центр распределен по нескольким площадкам, находящимся на существенном удалении (в несколько тысяч километров).
10. Вычислительный центр состоит из нескольких площадок, расположенных в пределах одного города, плюс одна или несколько площадок на существенном удалении (в другом регионе). Между площадками в пределах города организована синхронная репликация, на удаленные площадки осуществляется асинхронная репликация.

Ставится задача выбора лучшего варианта схемы защиты из 10 наиболее распространенных и обеспеченных программными и техническими средствами.

В качестве показателей комплексной оценки рассматриваемых вариантов схем защиты используются:

– показатели, определяющие снижение риска ущерба при использовании мер защиты;
– показатели, определяющие размер затрат на создание системы защиты.

К показателям, определяющим снижение риска ущерба при использовании мер защиты относятся:

- Оценка снижения риска ущерба от недоступности средств обработки данных по причине неработоспособности основного производственного оборудования или персонала вследствие природных негативных факторов.
- Оценка снижения риска ущерба от недоступности средств обработки данных по причине неработоспособности основного производственного оборудования или персонала вследствие негативных техногенных воздействий.
- Оценка снижения риска ущерба от недоступности средств обработки данных по причине неработоспособности основного производственного оборудования или персонала вследствие возникновения неприемлемых социальных условий (локальный вооруженный конфликт, общественные беспорядки, нарушения договорных обязательств на пользование зданием (помещением) ЦОД и т.д.).

К показателям, определяющим размер затрат на создание системы защиты, относятся:

- Оценка затрат на закупку оборудования и организацию каналов связи основной производственной площадки.
- Оценка затрат на закупку оборудования и организацию каналов связи резервной площадки.
- Оценка затрат на оборудование помещений производственной площадки.
- Оценка затрат на оборудование помещений резервной площадки.

- Оценка текущих затрат на эксплуатацию системы, находящейся в производ-ственном режиме.
- Оценка текущих затрат на эксплуатацию системы, находящейся в резерве
- Оценка затрат на оплату труда персонала.

При проектировании или модернизации Центра обработки данных механизм выбора варианта защиты может использовать комплексную оценку варианта защиты Центра от аварий и катастроф [7] при достаточно размытых данных о предполагаемых условиях эксплуатации. В процессе эксплуатации данные о внешних условиях применительно к фиксированному отрезку времени становятся более определенными. В связи с этим значительный эффект может дать механизм самонастройки системы защиты центра обработки данных в процессе эксплуатации. Объектами управления при самонастройке системы в процессе эксплуатации будут число резервных копий, режимы копирования и репликации, протоколы обмена данными.

2. Механизм самонастройки системы защиты центра обработки данных

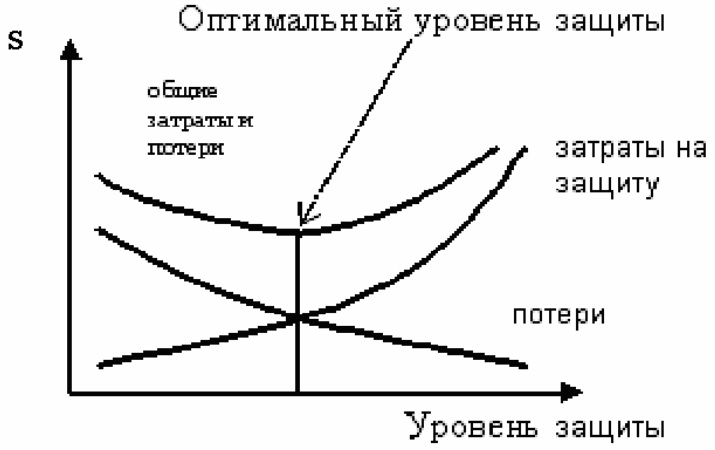
Затраты на эксплуатацию выбранного варианта системы защиты Центра обработки данных могут изменяться (как правило, возрастать) в связи с возникновением новых угроз, необходимостью парирования их, инфляцией и другими факторами. Предполагается, что выбранная система защиты в процессе эксплуатации допускает необходимые действия по рациональному реагированию на изменения условий её функционирования (например, наращиванию и модификации защитных свойств системы за счёт увеличения числа копий, частоты производимой репликации, изменения протокола обмена данными и пр.). При этом, каждое такое действие соизмеряется как с производимыми затратами, так и с изменением потерь от нарушений в системе, измеренных в стоимостных показателях. Сравнивая потери от нарушения доступности данных и затраты на содержание системы защиты Центра обработки данных и ее развитие в пределах выбранной архитектуры, можно найти оптимальный уровень защиты, обеспечивающий наименьшие общие издержки в процессе эксплуатации.

Рассмотрим механизм оптимизации режимов функционирования системы защиты Центра обработки данных от вероятных угроз на основе обратной связи, позволяющий достигать минимальных значений целевой функции $s = (f + q) \rightarrow \min$ (рис. 2), где

q — оценка затрат на защиту Центра обработки данных от вероятных угроз,

f — оценка ущерба от реализации угроз,

s — общие издержки, вызванные затратами на создание защиты Центра обработки данных от вероятных угроз и ущербом, наносимым при реализации этих угроз.



ёРис.2. Механизм оптимального выбора мер защиты данных

Для этой цели в условиях эксплуатационного режима будем использовать принцип действия пропорционально-интегрального регулятора [8].

В качестве модели затрат, аппроксимирующей зависимость общих затрат от затрат на реализацию защитных мероприятий, рассмотрим зависимость

$s=a/exp(q/r)+q,$

где q – затраты на реализацию защитных мероприятий, a – максимальный ущерб от реализации угроз, r – эффективность мер защиты. Поскольку процесс регулирования развивается во времени t, параметры a и r изменяются с темпом инфляции p. Численные значения параметров модели следующие: p=1,02; a=2 p^t; r=0,2 p^t; t=0,1,…,21.

В отличие от классического регулятора, в качестве значения невязки процесса регулирования выбрана предельная сумма общих издержек $M_s=ds/dq$. Обратная связь в системе с саморегуляцией осуществляется по следующему закону:

$q = q_0+k\, M_s+l\, I,$

где q_0 – постоянные затраты, k – коэффициент пропорциональной связи, l – коэффициент интегральной связи, I – интеграл (накопленная сумма) предельных издержек. При соответствующем подборе коэффициентов обратной связи (в рассматриваемой численной реализации модели были выбраны значения q_0=0,5; k=0,02; l = 0,1) процесс находился вблизи оптимального режима при (минимальном) значении общих издержек. Графики основных параметров процесса саморегулирования приведены на рис. 5 и 6.

Интерпретация результатов моделирования позволит реализовать организационный механизм, обеспечивающий минимизацию общих издержек.

Основным звеном этого механизма является измеритель предельных общих издержек на каждом шаге цикла в соответствии с конечно-разностным приближением

$M_s(t)=(s(t) – s(t-1))/(q(t) – q(t-1))$,

где t – текущий цикл регулирования. В стационарном режиме, как не трудно видеть, уровень предельных издержек равен нулю. Значение достигаемого уровня суммарных потерь зависит как от «эффективности» регулятора системы защиты Центра обработки данных, так и постоянных издержек q_0, определяемых структурой системы защиты. Имитация результатов работы регулятора в условиях роста эффективных затрат с темпом инфляции приведена на рис 3.

Рис. 3. Динамика основных параметров процесса саморегулирования

Результаты расчетов показывают, что, несмотря на неточное приближение динамики затрат к оптимальному уровню, уровень общих издержек практически совпадает с минимально достижимым (оптимальным) уровнем.

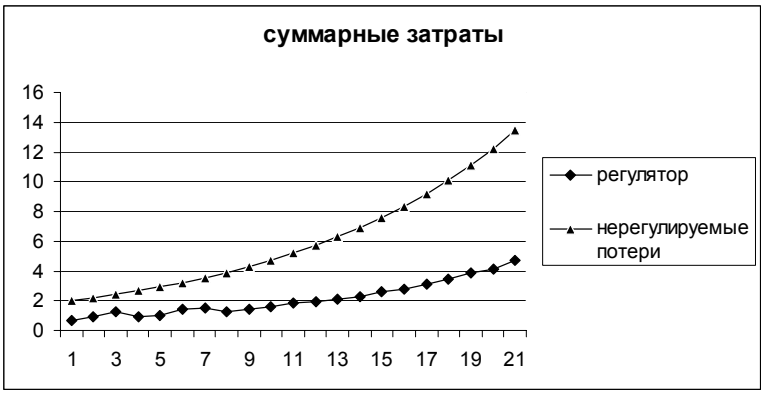


Рис. 4. Сравнение общих издержек при наличии механизма оптимизации и без него

Рассмотренные модели индикативных регуляторов позволяют признать перспективность их использования [9]. Важной чертой представленных регуляторов является то, что они не требуют знания модели регулируемого объекта. Необходимо иметь только элемент, измеряющий текущее состояние критериального показателя, алгоритм расчета управляющего воздействия и канал обратной связи.

При этом:

- Индикативные регуляторы позволяют обеспечить близкие к требуемым (в т.ч. оптимальным) параметры состояния объекта управления
- Эффект от применения механизмов оптимизации, как правило, весьма значителен (рис. 4)
- Упрощается процесс достижения целей в актуальных сферах деятельности
- Организация таких регуляторов требует: разработки индикативных показателей обратной связи, настройки численных параметров обратной связи, периодичного пересмотра состава показателей и механизма регулирования.

Заключение

Рассмотрены основные стратегии обеспечения доступности информационных ресурсов и обеспечения непрерывности IT-сервисов в случае аварий и катастроф.

Разработана методика выбора наилучшего варианта системы защиты центров обработки данных с использованием метода векторной стратификации и экономического механизма оптимизации системы защиты Центра обработки данных от вероятных угроз, позволяющего достигать минимальных значений целевой функции.

Предлагаемая методика позволяет увязать методы экспертного оценивания с моделированием рассматриваемых объектов и процессов. Благодаря этому появляется возможность получать эффективные решения при рациональном сочетании исходной информации, полученной от экспертов и объективной информации, полученной в результате измерений и сбора статистики (по результатам испытаний технических средств, результатам проведенных организационных мероприятий и др.).

Литература

1. *C. Warrick, C. Beretta, R. Ghem, L. Hilliard, S. Kamonthipsukon, S. Rolandi, J. Sing, G. J. Tarella, C. Leung* Ibm Total Storage Business Continuity Solutions Guide, International Technical Support Organization, Ibm Redbooks Sg24-6547-02, August 2005.
2. *Павельев В.В*. Формирование системы критериальных свойств при комплексной оценке сложных объектов.- В Кн.: Механизмы Функционирования Организационных Систем. Вып. 29. – М., Институт Проблем Управления, 1982.
3. *Глотов В. А., Павельев В. В.* Векторная стратификация. – М.: Наука, 1984

4. Анохин А.М., Гусев В.Б., Павельев В.В. Комплексное оценивание и оптимизация на моделях многомерных объектов. М., - 2003 (Научное Издание / Институт Проблем Управления им. В.А. Трапезникова РАН).
5. *А. Морозевич, В. Гаврилюк.* Управление данными или ilm по ibm: опыт практической реализации. "Storage News", №3, 2006.
6. *Павельев С.В.* Методы обеспечения сохранности информации пользователей в сети интернет. // Теория Активных Систем / Труды Международной Научно-Практической Конференции (17-19 Ноября 2003 Г., Москва, Россия). Общая Редакция - В.Н.Бурков, Д.А.Новиков. Том 2. –М.: ИПУ РАН, 2003.
7. *Гусев В.Б., Павельев В.В., Павельев С.В.* Выбор оптимального механизма саморегулирования системы защиты центра обработки данных от аварий и катастроф. Сборник Трудов "Управление Большими Системами" М.:ИПУ РАН, 2009.
8. *John Shaw*. The Pid Control Algorithm: How It Works, How To Tune It, And How To Use It. 2nd Ed. 62pp. Http://Learncontrol.Com/Pid/Description.Htm
9. *Левинталь А.Б., Ефременко В.Ф., Гусев В.Б., Пащенко Ф.Ф.* Расчет показателей индикативного планирования для программ развития региона. Научное Издание. – М.: Институт Проблем Управления РАН, 2006, 54 с.