УДК 658.012.011.56
ББК 05.25.05

ВЫБОР ОПТИМАЛЬНОГО МЕХАНИЗМА САМОРЕГУЛИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ ОТ АВАРИЙ И КАТАСТРОФ

Гусев В.Б. [1], **Павельев В.В.** [2]
*(Учреждение Российской академии наук
Институт проблем управления РАН, Москва)*
Павельев С.В.[3]
*(Департамент информатизации ОАО «Федеральная сетевая компания Единая энергетическая Система»,
г. Москва)*

Предложена методика выбора оптимального механизма саморегулирования системы защиты от аварий и катастроф выделенного центра обработки данных в территориально-распределенной автоматизированной системе, построенной с использованием каналов глобальных сетей связи.

---

[1] *Владислав Борисович Гусев, кандидат физико-математических наук, (тел. (495) 334-88-21, E-mail: gusvbr@ipu.ru)*
[2] *Владимир Васильевич Павельев (тел. (495) 334-88-21, E-mail: pavvvs@ipu.ru)*
[3] *Сергей Владимирович Павельев, (тел (495) 921-76-07, E-mail: pavelyev-sv@rao.elektra.ru)*

Ключевые слова: центр обработки данных, глобальные сети связи, оптимальный механизм саморегулирования системы защиты.

1. 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. Одним из основных подходов, применяемых в настоящее время для оптимизации затрат на системы безопасности, является анализ и управление рисками. Простейшей мерой риска является пара: вероятность Q неблагоприятного события и последствия (ущерб) W при его наступлении. Оба показателя могут быть мультипликативным образом объединены в один: $R = Q * W$, что позволяет сравнивать ситуации с различными последствиями и вероятностями их наступления. 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 саморегулирования системы защиты от них центров обработки данных.

2. Обеспечение требуемого уровня доступности информационных ресурсов в территориально-распределенных it-инфраструктурах.

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].

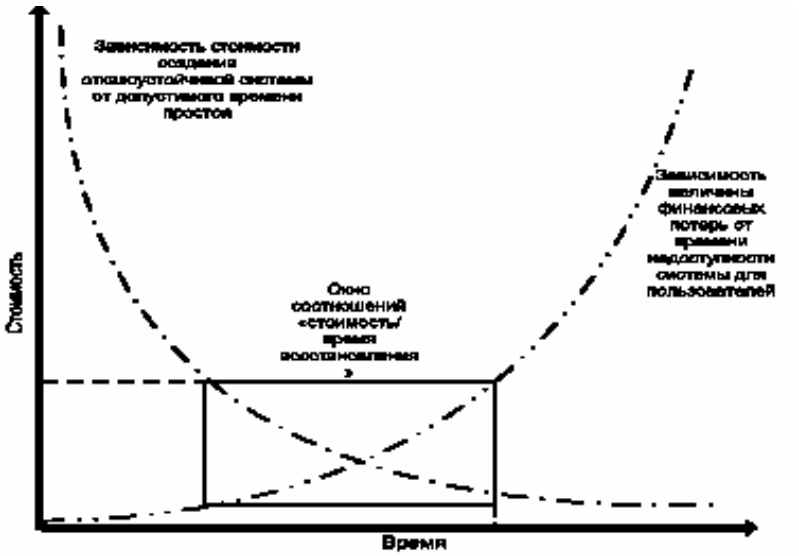

Рис. 1. Зависимость финансовых потерь из-за недоступности IT-сервисов от времени их недоступности и стоимости создания системы высокой доступности от величины допустимого времени простоя.

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

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

3. 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 лучшей схемы защиты из 10 наиболее распространенных и обеспеченных программными и техническими средствами.

4. Выбор наилучшего варианта защиты центра обработки данных от аварий и катастроф.

Широко распространенные методики выбора лучших вариантов в качестве целевой функции используют аддитивную линейную свертку значений частных показателей с учетом коэффициентов их относительной важности. Под весовым коэффициентом показателя понимается нормированное приращение значений целевой функции, приходящееся на единицу приращения значения этого показателя, инвариантное относительно фиксированных уровней значений остальных показателей. Большинством разработчиков методик комплексного оценивания, использующих метод аддитивной линейной свертки частных показателей, данное требование инвариантности считается автоматически выполняющимся при любых условиях. В действительности, в задачах разработки гармоничных сбалансированных систем, имеющих практический смысл, приращение целевой функции, приходящееся на единицу приращения значений одного показателя, обычно зависит от того, на каком уровне зафиксированы значения остальных показателей. Таким образом, значения весовых коэффициентов показателей, как правило, будут меняться в зависимости от того, на каких участках шкал

производится их соизмерение. Кроме того, линейная монотонная функция свертки требует допустимости взаимной компенсации худших оценок по одним показателям лучшими оценками по другим показателям, что на практике далеко не всегда возможно.

Методика целенаправленного выбора лучшего варианта, использующая метод векторной стратификации [2-4], позволяет преодолеть перечисленные трудности. В основе целенаправленного выбора лежит следующий принцип: комплексное оценивание должно обеспечивать измерение степени соответствия объекта оценки сформулированному целевому назначению. В соответствии с этим принципом путем дихотомической конкретизации и детализации формулировки заданной цели формируется бинарная древовидная структура показателей комплексной оценки объекта выбора.

Значения частных показателей определяются следующим образом.

Путем опроса экспертов или на основании имеющейся статистики определяются вероятности реализации опасностей в отношении выделенных групп объектов опасности в случае отсутствия мероприятий по защите ЦОД от аварий и катастроф.

Производится расчет ущерба в случае реализации опасностей при отсутствии мероприятий по защите ЦОД от аварий и катастроф.

Расчет суммарного риска нарушения доступности информационных ресурсов при отсутствии мероприятий по защите ЦОД от аварий и катастроф производится по следующей формуле:

$R_{\sum} = \sum_i P_i W_i$, где P_i - вероятность реализации опасностей в отношении i-й группы объектов опасности;

W_i - ущерб в случае реализации опасностей в отношении i-й группы объектов опасности.

Соответственно каждой группе объектов опасности будет соответствовать риск $R_i = P_i W_i$

Расчет затрат на реализацию каждого варианта для имеющегося перечня вариантов защитных мероприятий производится по следующей формуле:

$C_n = \sum_i C_{ni}$, где n – номер рассматриваемого варианта;

i – статья затрат в соответствии с деревом затрат.

Из перечня рассматриваемых вариантов исключаем все варианты, не соответствующие следующему условию:

$$C_n \le kR_{\sum} \quad (3.1.)$$

где $R_{\sum}$ - суммарный риск нарушения доступности информационных ресурсов при отсутствии мероприятий по защите ЦОД от аварий и катастроф;

k - коэффициент, отражающий склонность лица, принимающего решения (ЛПР) к риску.

Производится расчет значений рисков для каждой группы объектов опасности для каждого из рассматриваемых вариантов (после исключения вариантов, не соответствующих условию 3.1.):

$$R_{ni} = P_{ni} W_{ni} ,$$

где n – номер варианта;

i – номер группы опасностей, воздействующих на определенную группу объектов опасностей.

Производится расчет величины снижения риска. Для каждого из рассматриваемых вариантов вычисляем величины снижения риска для каждой группы объектов опасности по сравнению с величинами рисков, рассчитанных для случая отсутствия мер защиты по формуле:

$$. \Delta R_{ni} = R_i - R_{ni}$$

. Для каждого из рассматриваемых вариантов получаем относительные оценки по показателям, расположенным на концевых вершинах дерева оценок. Значения величин снижения риска и постатейных расходов на создание систем защиты, характери-

зующих каждый из рассматриваемых вариантов, преобразуются в вербально-числовую шкалу Харрингтона из пяти градаций и далее в соответствующую пятибалльную шкалу.

Для каждого узла древовидной структуры показателей лицо, принимающее решение, или эксперты заполняют матрицы логической свертки частных оценок в обобщающую оценку размерности 5×5. Строки матрицы соответствуют значениям оценок по одному из объединяемых показателей, столбцы – значениям оценок по второму показателю. Значения оценок варианта по обобщающему показателю проставляются на пересечении столбцов и строк. Их определяет эксперт или лицо, принимающее решение с учетом относительной значимости оценок по объединяемым показателям.

По комплексному критерию (решающему правилу, состоящему из совокупности матриц логической свертки) все рассматриваемые варианты оцениваются по 5-бальной шкале, упорядочивающей их по предпочтительности. Самые лучшие, обеспечивающие полное достижение заявленной цели, будут отнесены к 5-й страте, самые худшие (бесполезные для достижения цели) – к 1-й страте. Если в некоторой страте окажется несколько объектов оценки, то лучший из них выбирается с помощью дополнительной информации об условиях их применения.

5. Механизм саморегулирования системы защиты центра обработки данных

Затраты на эксплуатацию системы защиты Центра обработки данных возрастают в связи с возникновением новых угроз, необходимостью парирования их, инфляцией и другими факторами. Сравнивая потери от нарушения доступности данных и затраты на содержание системы защиты Центра обработки данных и ее развитие, можно найти оптимальный уровень защиты, обеспечивающий наименьшие общие издержки.

Рассмотрим экономический механизм оптимизации системы защиты Центра обработки данных от вероятных угроз,

позволяющий достигать минимальных значений целевой функции $s = (f + q) \rightarrow \min$, где

f — затраты на защиту Центра обработки данных от вероятных угроз,

q — ущерб от реализации угроз.

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

Для этой цели будем использовать принцип действия пропорционально-интегрального регулятора [7]. В качестве значения невязки процесса регулирования выбрана предельная сумма общих издержек Ms. Обратная связь в системе с саморегуляцией осуществляется по следующему закону: q = 0+k* Ms+l*I, где q – ущерб от реализации угроз, q0 – 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 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.

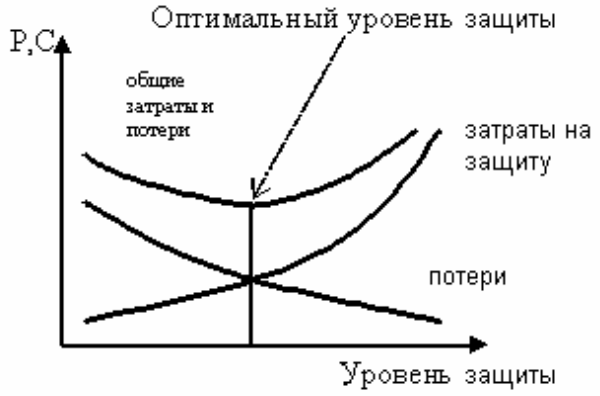

Рис.2. Экономические последствия мер защиты данных

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 определением $Ms(t)=(s(t) – s(t-1))/(q(t) – q(t-1))$,
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 q0, определяемых структурой системы защиты. Имитация результатов работы регулятора в условиях роста эффективных затрат с темпом инфляции приведена на рис 6.

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.

Рассмотренные модели индикативных регуляторов позволяют признать перспективность их использования [8]. 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. 7)

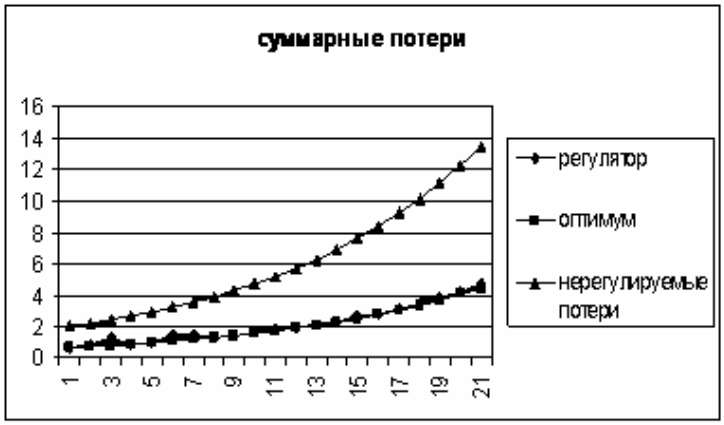

Рис. 4. Сравнение общих издержек при наличии механизма оптимизации и без него

- Упрощается процесс достижения целей в актуальных сферах деятельности
- Организация таких регуляторов требует: разработки индикативных показателей обратной связи, настройки численных параметров обратной связи, периодич-

ного пересмотра состава показателей и механизма регулирования.

6. 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 органи-

зационных 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. 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
8. 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.

CHOICE OF THE OPTIMAL MECHANISM OF SELF-REGULATION OF THE DATA-PROCESSING PROTECTION SYSTEM FROM FAILURES AND ACCIDENTS

Vladislav Gusev, Russian Academy of Sciences Institute of Control Sciences (ICS RAS) Moscow, Russian Federation, Cand.Sc. (E-mail: gusvbr@ipu.ru)
Vladimir Pavelyev, Russian Academy of Sciences Institute of Control Sciences (ICS RAS) Moscow, Russian Federation (E-mail: pavvvs@ipu.ru)

Sergey Pavelyev, Department of information of Open Society "Federal network company of UNIFORM POWER SYSTEM" Moscow, Russian Federation (E-mail: pavelyev-sv@rao.elektra.ru).

Abstract: The technique of a choice of the optimum mechanism of self-regulation of system of protection against failures and accidents of the allocated data-processing centre in the territorially-distributed automated system constructed with use of channels of global communication networks is offered.

Keywords: mechanism of self-regulation, protection, failures and accidents, allocated data-processing center, global communication networks