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]
(ОАО «Федеральная сетевая компания
Единая энергетическая система», 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.

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

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

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: $R = QW$, математическое ожидание ущерба, 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 (ЦОД) 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 ЦОД;

– вероятность наступления событий, наносящих существенный ущерб;

– затраты (капитальные и эксплуатационные) на мероприятия по защите ЦОД от аварий и катастроф.

В связи с этим, актуальной является задача разработки методики анализа потенциальных угроз на этапах проектирования и эксплуатации системы, а также оптимального механизма саморегулирования системы защиты от них ЦОД на этапе ее эксплуатации.

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 рациональных 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 ленточных накопителях;

– различные способы репликации данных на удаленную площадку с размещением их на дисковых массивах.

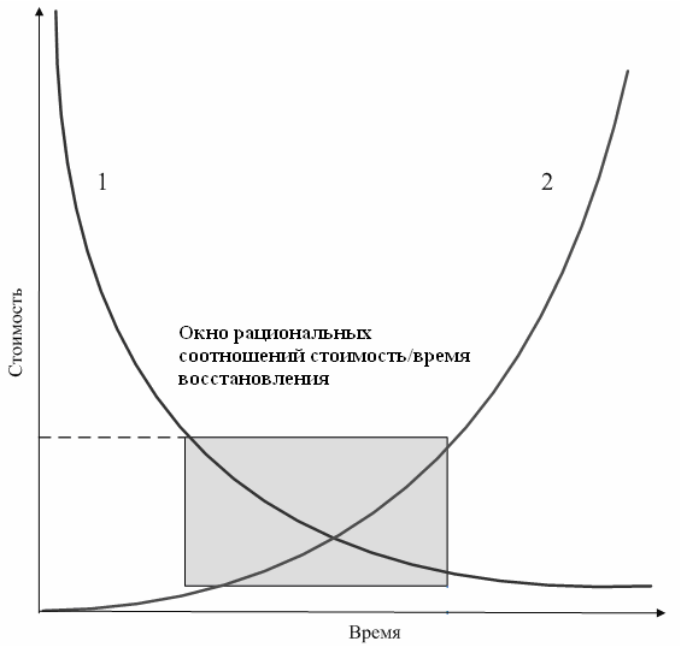

Рис. 1. Зависимость финансовых потерь (2) из-за недоступности информационных ресурсов от времени их недоступности и стоимости (1) создания системы высокой доступности от допустимого времени простоя

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 ЦОД, иногда находящихся на значительном расстоянии друг от друга. Приняв за основу семиуровневую (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 ЦОД [4, 6, 8] предлагается выделить 10 наиболее распространенных схем организации резервирования информационных массивов и IT-сервисов в территориально-распределенных IT-инфраструктурах с выделенными ЦОД:

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 син-

хронная репликация, на удаленные площадки осуществляется асинхронная репликация.

Ставится задача выбора лучшего варианта схемы защиты, формируемого как комбинация из 10 наиболее распространенных и обеспеченных программными и техническими средствами схем защиты.

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, не постоянны и зависят от того, на каких участках шкал производится их соизмерение. Кроме того, монотонная линейная 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 [4-6], 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.

Комплексная оценка варианта защиты ЦОД от аварий и катастроф формируется в виде бинарного дерева, содержащего две группы оценок. Группа П1 – показатели, определяющие снижение риска ущерба при использовании мер защиты; группа П2 – показатели, определяющие размер затрат на создание системы защиты.

В таблице 1 в качестве примера приведена часть показателей группы П1 и группы П2.

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 верхней оценки 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-ой группы объектов опасности; W_i – ущерб в

случае реализации опасностей в отношении i-ой группы объектов опасности.

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

Табл. 1. Фрагменты показателей группы П1 и группы П2

Код показателя	Наименование показателя
	Группа П1
1.1	Оценка снижения риска ущерба от недоступности средств обработки данных вследствие природных пожаров, наводнений и прочих негативных природных факторов
1.2.1	Оценка снижения риска ущерба от недоступности средств обработки данных вследствие аварий на опасных производствах
1.2.2	Оценка снижения риска ущерба от недоступности средств обработки данных вследствие прочих негативных техногенных воздействий
	Группа П2
2.1.1.1	Оценка затрат на закупку оборудования и организацию каналов связи производственной площадки
2.1.1.2	Оценка затрат на закупку оборудования и организацию каналов связи резервной площадки
2.1.2.1	Оценка затрат на оборудование помещений производственной площадки
2.1.2.2	Оценка затрат на оборудование помещений резервной площадки
2.2.1.1	Оценка текущих затрат на эксплуатацию системы, находящейся в производственном режиме
2.2.1.2	Оценка текущих затрат на эксплуатацию системы, находящейся в резерве
2.2.2	Оценка затрат на оплату труда персонала

Свяжем каждую группу объектов опасности с мероприятием, парирующим эти опасности. Некоторые мероприятия носят избыточный характер, воздействуя на несколько групп объектов опасности. Расчет верхней оценки затрат на реализацию каждого варианта защиты для имеющегося перечня вариантов защитных мероприятий производится по следующей формуле:

$$C_n = \sum_i C_{nj},$$

где n – номер рассматриваемого варианта; j – статья затрат, соответствующая мероприятию по защите.

Из перечня рассматриваемых вариантов на предварительном этапе целесообразно исключить все варианты, не соответствующие субъективному условию рациональности затрат на реализацию варианта защиты:

(1) $C_n \le kR_{\sum}$,

где k – коэффициент, отражающий склонность лица, принимающего решения (ЛПР) к риску. Если для значения k порядка 1 находится хотя бы один вариант защиты, удовлетворяющий условию (1), то принимается решение, что задача выбора варианта имеет смысл.

Расчет значений рисков производится для каждой группы объектов опасности для каждого из рассматриваемых вариантов:

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

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 у каждой группы объектов опасности по сравнению с величинами рисков, рассчитанных для случая отсутствия мер защиты по формуле:

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

Использование оценок снижения рисков для принятия решений путем суммирования ΔR_{ni} по номерам групп опасностей i некорректно, поскольку реализации опасностей группы i при

варианте защиты n не являются независимыми событиями. Степень влияния групп опасностей определяется экспертным путем методом векторной стратификации. Как указывалось выше, существенным достоинством этого метода является возможность учета нелинейности вклада отдельных факторов в результирующую оценку.

В соответствии с рассматриваемым методом, для каждого из вариантов защиты получаем относительные оценки по показателям, расположенным на концевых вершинах дерева оценок. Для этого значения величин снижения риска и постатейных расходов на создание систем защиты, характеризующих 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 пятибальной шкале, упорядочивающей их по предпочтительности. Самые лучшие, обеспечивающие полное достижение заявленной цели, будут отнесены к 5-ой страте, самые худшие (бесполезные для достижения цели) – к 1-ой 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 выбранного варианта системы защиты ЦОД 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 производимых репликаций, 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 ЦОД и ее развитие в пределах выбранной архитектуры, можно находить и отслеживать оптимальный уровень защиты, обеспечивающий наименьшие общие издержки в процессе эксплуатации.

Рассмотрим механизм оптимизации режимов функционирования системы защиты ЦОД от вероятных угроз на основе обратной связи, позволяющий достигать минимальных значений целевой функции $s = (f + q) \rightarrow \min$ (рис. 2), где q — затраты на защиту ЦОД от вероятных угроз; f — ущерб от реализации угроз; s — общие издержки, вызванные затратами на создание защиты ЦОД от вероятных угроз и ущербом, наносимым при реализации этих угроз.

Для этой цели в условиях эксплуатационного режима будем использовать принцип действия пропорционально-интегрального регулятора [7]. Статистические данные о произведенных затратах на мероприятия по защите, а также оценки ожидаемых или реализованных потерь периодически собираются и используются для расчета оптимальных уровней планируе-

мых затрат на защиту в процессе эксплуатации информационной системы. Предлагаемый механизм не требует явного задания зависимости общих издержек от составляющих, поскольку использует только регулярно производимые замеры реальных издержек и эксплуатационных затрат.

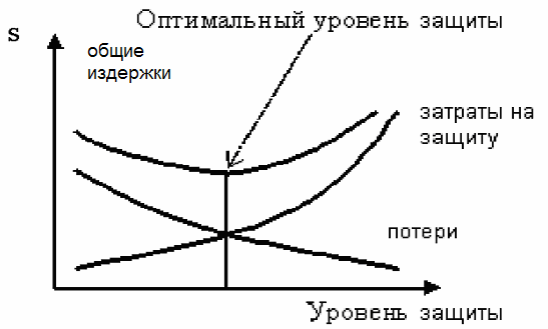

Рис.2. Механизм оптимального выбора мер защиты данных

Для иллюстрации в качестве модели затрат, аппроксимирующей зависимость общих издержек от вероятных угроз и 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 – стоимость «эффективных» мер защиты. Поскольку процесс регулирования развивается во времени t, параметры a и r изменяются с темпом инфляции p. Численные значения параметров модели были выбраны следующими: $p = 1{,}02$; $a = 2p^t$; $r = 0{,}2p^t$; $t = 0, 1, \ldots, 21$.

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

$$q = q_0 + k\,M_s + lI,$$

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).

Для подбора параметров регулятора использовалась процедура многомерной минимизации усредненного по времени значения полных издержек. Для практических приложений можно использовать процедуру многомерной минимизации апостериорного прогнозируемого значения полных издержек на основе статистических данных, относящихся к предыстории. Правомерность такого подхода при выборе параметров регулирования q_0, k, l основывается на предположении о том, что в процессе эксплуатации системы источники сбоев и угроз сохраняют свою природу и необходимо только учитывать уточненные характеристики риска. Возникновение непредвиденных угроз требует корректировки архитектуры информационной системы по методу, описанному в предыдущих разделах.

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 (оптимальном) режиме, как не трудно видеть, уровень предельных издержек равен нулю. Значение достигаемого уровня суммарных потерь зависит как от «эффективности» регулятора системы защиты ЦОД, так и постоянных издержек q_0, определяемых структурой системы защиты. Результаты имитации работы регулятора в условиях роста эффективных затрат с учетом инфляции приведены на рис 3. Для сравнения на этом рисунке

приведена кривая для оптимальных значений затрат на организацию защиты, вычисленных аналитически:

$$q(t) = r(t) \cdot \ln {r(t)}/{a(t)} \cdot$$

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.

Рассмотренная модель может быть отнесена к модели индикативных регуляторов [1]. Важной чертой представленных регуляторов является то, что они нацелены на достижение оптимального уровня контролируемого параметра и не требуют ни знания этого уровня, ни 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);

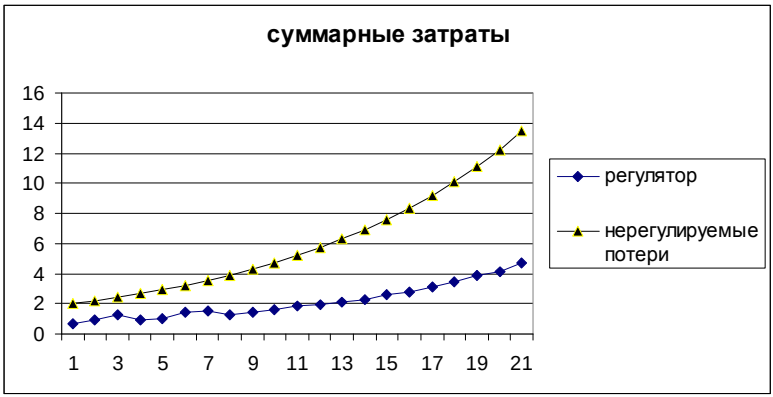

Рис. 4. Сравнение общих издержек при наличии механизма оптимизации и без него

– упрощается процесс достижения целей в актуальных сферах деятельности;

– организация таких регуляторов требует: разработки индикативных показателей обратной связи, настройки численных параметров обратной связи, периодичного 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 ЦОД с использованием метода векторной стратификации и экономического механизма оптимизации системы защиты ЦОД 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.).

Результаты моделирования позволяют признать перспективность использования предложенного метода саморегулирования системы защиты ЦОД от аварий и катастроф.

Литература

1. АНОХИН А. М., ГУСЕВ В. Б., ПАВЕЛЬЕВ В. В. *Комплексное оценивание и оптимизация на моделях многомерных объектов*. – М.: ИПУ РАН, 2003.
2. ГЛОТОВ В. А., ПАВЕЛЬЕВ В. В. *Векторная стратификация*. – М.: Наука, 1984.
3. ЛЕВИНТАЛЬ А. Б., ЕФРЕМЕНКО В. Ф., ГУСЕВ В. Б., ПАЩЕНКО Ф. Ф.. *Расчет показателей индикативного планирования для программ развития региона. Научное издание*. – М.: ИПУ РАН, 2006.
4. МОРОЗЕВИЧ А., ГАВРИЛЮК В.. *Управление данными или ILM по IBM: опыт практической реализации* / "Storage News".– 2006. – №3 (28).
5. ПАВЕЛЬЕВ В. В. *Формирование системы критериальных свойств при комплексной оценке сложных объектов*. – В кн.: Механизмы функционирования организационных систем. Вып. 29. – М.: ИПУ РАН, 1982.
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). Под ред. В. Н. Буркова, Д. А. Новикова. Том 2. –М.: ИПУ РАН, 2003. – С. 140-142.
7. SHAW J. *The PID Control Algorithm: How It Works, How To Tune It, and How to Use It*. – 2nd Ed. – 62 p. – URL: http://learncontrol.com/pid/description.htm
8. WARRICK C., BERETTA C., GHEM R., HILLIARD L., KAMONTHIPSUKON S., ROLANDI S., SING J., TARELLA G. J., LEUNG C. *IBM Total Storage Business Continuity Solutions Guide*, International Technical Support Organization, IBM Redbooks SG24-6547-02, August 2005.

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. (gusvbr@ipu.ru)
Vladimir Pavelyev, Russian Academy of Sciences Institute of Control Sciences (ICS RAS) Moscow, Russian Federation (pavvvs@ipu.ru)
Sergey Pavelyev, Department of information of Open Society "Federal network company of Uniform Power Systems" Moscow, Russian Federation (pavelyev-sv@rao.elektra.ru).

Abstract: The technique is proposed of a choice of the optimum mechanism for 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.

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

Статья представлена к публикации
членом редакционной коллегии А.И. Орловым.