Методологический подход к моделированию поведения информационных систем при воздействиях катастрофического характера

Г. П. Акимова, Е. В. Пашкина, А. В. Соловьев

В статье изложен методологический подход к моделированию поведения больших территориально-распределенных информационных систем при воздействиях катастрофического характера.

Обозначения и сокращения

ИС – информационная система
ЦОД – центр обработки данных
ЦКС – центры и каналы связи
ДФ – дестабилизирующие факторы
ОДП – оперативно-диспетчерский персонал
БД – база данных

Введение

Все возрастающий объем обрабатываемой информации и сложность выполняемых функций в современных больших территориально-распределенных информационных системах, существенный, функционально тесно связанный между собой, управленческий аппарат постоянно увеличивающееся количество распределенных по территории страны разнообразных центров обработки данных различных уровней, сервисных центров, узлов коммутации, каналов связи и пр., определяют необходимость создания механизмов, позволяющих оперативно прогнозировать и вычислять вероятность отказов и катастроф при воздействии различных дестабилизирующих факторов, а также выбирать стандартные меры

противодействия и функционирования систем с учетом возможных воздействий катастрофического характера.

Под катастрофами подразумеваются не только пожар, наводнение или землетрясение, но и возможные непредвиденные сбои в работе служб, разрушение данных или повреждение ЦОД, например, в случае разрыва телекоммуникационных линий, возникшего в результате проведения ремонтных работ, умышленной диверсии или саботажа или просто по халатности и ошибочных действий обслуживающего персонала.

Катастрофоустойчивость — способность к восстановлению работы приложений и данных за минимально короткий период времени после катастрофы. В отличие от отказоустойчивых систем, которые должны продолжать функционирование в случае сбоя одного из ее компонентов, катастрофоустойчивая система должна сохранять работоспособность в случае одновременного множественного выхода из строя ее составных частей в результате воздействий непредвиденного характера.

Вследствие этого построение прогноза поведения большой территориально — распределенной информационной системы в условиях катастрофических воздействий требует создания полноценной модели ее функционирования под влиянием различных дестабилизирующих факторов, а также моделирование мер противодействия данным факторам. Процесс создания такой модели будем называть моделированием катастрофоустойчивости информационной системы.

В данной статье предложен общий методологический подход к созданию моделей поведения информационных систем в условиях катастрофических воздействий, а также оговорены основные принципы и допустимые ограничения при построении таких моделей.

1. Основные положения методологического подхода к моделированию катастрофоустойчивости ИС

Основные положения концепции создания комплекса, моделирующего катастрофоустойчивость информационной системы, тесно связаны с общим методологическим подходом, на котором основано проектирование системы.

В рамках данной статьи под элементами информационной системы понимаются ЦОД и ЦКС различных уровней; под узлами системы понимается конкретное оборудование, входящее в ЦОД и ЦКС.

1. В основе концепции лежит моделирование движения информационных потоков во время основного технологического цикла работы

с учетом рисков, т. е. при воздействии на систему дестабилизирующих факторов [9–12].

При моделировании работы временные характеристики движения информационных потоков в модели ИС должны задаваться из учета характеристик оборудования ее элементов (описание узлов ЦОД, ЦКС, их характеристики, принцип действия должны храниться в отдельной БД) и квалификации ОДП.

Движение информационных потоков должно моделироваться с учетом влияния на ИС различных рисков (отказы электропитания, изменение климата внутри помещений ЦОД, пожароопасность, отказы элементов ЦОД, модели умышленного ущерба и влияния человеческого фактора [1, 4–7]). Характеристики рисков, а также сценарии развития катастрофических ситуаций, должны задаваться отдельными параметрическими моделями и храниться в отдельной БД.

Результатом моделирования должно быть вычисление показателей катастрофоустойчивости, надежности [2] и эффективности работы [3], а также качественные выводы о ее готовности к выполнению своих функций при развитии заданных катастрофических событий с анализом причин нарушения устойчивости системы на основе полученной информации.

В отдельной БД должна накапливаться и храниться «история» развития реальных проблем, возникавших при эксплуатации системы, для построения модели ретроспективного анализа развития катастрофических событий и оценки эффективности контрмер.

2. При моделировании катастрофоустойчивости должен применяться сценарный метод («что, если») анализа и прогнозирования поведения информационной системы с учетом влияния дестабилизирующих факторов [11, 12, 14].

   Моделирование поведения информационной системы должно производиться, исходя из предположения, что катастрофическое событие состоялось. Необходимо смоделировать состояние, движение информационных потоков, влияние отказа элемента на поведение всей ИС с учетом времени восстановления элемента.

   Сценарий развития катастрофических событий, степень влияния воздействия дестабилизирующих факторов на ИС должны задаваться отдельными параметрическими моделями, в которых параметрами выступают степень воздействия, вероятность возникновения, наличие средств противодействия ДФ и т. д.

3. При оценке состояния информационной системы и степени ее готовности к выполнению своих функций должно применяться ретроспективное моделирование поведения системы (на основе анализа БД «истории» (ретроспективы) отказов, принципа работы различных конфигураций ИС и т. д.).

   Моделирование отказов элементов информационной системы производится с учетом «истории», а также по случайному закону распределения отказов в ее элементах.

   При оценке состояния готовности системы, а также оценке риска возникновения аварийной или критической ситуации используется анализ «истории» отказов ее элементов и вариантов разрешения проблем (восстановления) с оценкой эффективности контрмер.

4. При анализе поведения ИС под влиянием воздействий на нее рисков должен использоваться принцип имитационного моделирования.

   Должно имитироваться функционирование всех элементов ИС с учетом временных характеристик работы и пропускной способности каналов связи, которые задаются как параметры модели работы ИС.

5. Модель катастрофоустойчивости информационной системы должна быть расширяемой и предусматривать:

   — ввод новых моделей ДФ, их характеристик и функций воздействия на ИС;

   — обработку новых статистических данных по «истории» отказов и изменению конфигурации ЦОД и ЦКС ИС.

6. Модель катастрофоустойчивости информационной системы должна обладать свойством непротиворечивости, т. е. должна соблюдаться непротиворечивость принципам функционирования системы.

2. Ограничения и допущения модели оценки катастрофоустойчивости

При проектировании модели катастрофоустойчивости информационной системы могут быть приняты следующие допущения:

1) все последствия катастрофических воздействий на ИС по причинению ущерба адекватны первопричине (например, пожар, вызванный землетрясением или ураганом и т. п.), поэтому при моделировании катастрофоустойчивости принимается во внимание только первопричина;

2) система обеспечения катастрофоустойчивости ИС проектируется таким образом, что резервные объекты (если таковые имеются), которым переданы функции ЦОД и ЦКС, попавшие под воздействие катастрофы, выполнят поставленную перед ними задачу;
3) риски возникновения и развития катастроф могут иметь такие категории (по их классификации), что передача функций резервным объектам обязательна, независимо от того, что ущерб от катастроф может быть меньше, чем спрогнозирован;
4) восстановление функционирования элементов ИС с заданным уровнем доверительной вероятности (обеспечение достоверности, полноты и своевременности выполнения функций) проводится за время, не превышающее заданное ($T_{ДВ.К.}$).

3. Методология моделирования катастрофоустойчивости ИС

1. В основу методологического подхода моделирования катастрофоустойчивости ИС закладывается предположение, что воздействие катастрофического характера произошло, необходимо оценить влияние его на функционирование системы и определить достаточность дополнительных средств (в том числе средств резервирования) для компенсирования влияния дестабилизирующего фактора, а также действия для компенсации его влияния на ИС [11, 12].

Ограничениями при этом могут выступать надежность, потенциальная пожароопасность, устойчивость связи, энергетическая безопасность (бессбойное электроснабжение) и т. д. для конкретного элемента системы. Через такие ограничения, получаемые на основе исследований или анализа статистических данных функционирования ИС, определяются ее потенциально уязвимые элементы.

2. Определяется важность ЦОД, ЦКС в зависимости от иерархии информационной системы.

Коэффициент важности каждого системы определяется в зависимости от функций, возложенных на ее элементы, значимости, ценности и объема информации. Например, учитывая типы ЦОД и ЦКС, можно ввести обозначения: пусть b_1 соотносится с головным ЦОД (ЦКС), b_{2j} — с j-м региональным ЦОД (ЦКС), b_{3k} — с k-м районным ЦОД (ЦКС) и т. д. Таким образом, в общем случае

$$1 \geqslant b_1 > b_{2j} > b_{3k}. \qquad (1)$$

Назначение приоритетов дает основание считать, что ущерб, нанесенный в результате действия одной и той же катастрофы, для элементов ИС различных приоритетов различен.

3. Модели рисков.

Определяется состав рисков, влияющих на информационную систему, и производится их ранжирование по степени нанесения ущерба.

Все риски разделяются на те, на которые оперативно — диспетчерский персонал, обслуживающий организации, сервисные центры и пр. может повлиять и те, на которые никто повлиять не может (ураган, цунами, землетрясение и т. д.).

Для рисков, на которые можно повлиять в сторону их уменьшения, составляются модели их влияния на систему: создается модель риска, модели воздействия на ИС и модели компенсации или предотвращения последствий.

Для всех рисков необходимо установить, что является объектом риска в каждом конкретном случае (ЦОД, ЦКС в целом или отдельный узел, сервер, канал связи и т. д.).

Для оценки рисков определяются необходимые статистические данные и порядок их сбора (обследование, анкетирование, как один из методов экспертной оценки, получение данных от сервисных центров, подсистем контроля функционирования и т. д.). Затем производится сбор необходимых статистических данных для оценки количественной или даже качественной степени влияния рисков.

По определенным ниже частным показателям производится оценка влияния рисков. Таким образом, вводится количественная оценка (или ограничение, например, по надежности, пожарозащищенности и т. д.) влияния риска на элементы и объекты информационной системы.

Для рисков, последствия которых или степень их влияния определяются только качественно, вводятся (например, путем экспертной оценки или на основе анализа «истории» подобных проблем в ИС) 3 величины: минимальная вероятность возникновения риска («оптимистический» прогноз), максимальная вероятность («пессимистический» прогноз), наибольшая вероятность (например, на основании усреднения двух предыдущих показателей). Данные величины используются в качестве ограничений, определяющих потенциальное состояние элемента ИС. На их основе производится оценка показателей катастрофоустойчивости.

В случае, когда получить количественную оценку влияния риска не предоставляется возможным, на основе экспертной оценки происходит «принятие» или «непринятие» данного риска для информационной

системы. По существу это означает логическое условие: «риск влияет на ИС» или «риск не влияет на ИС».

4. Выбирается основной показатель модели катастрофоустойчивости информационной системы, расчет которого позволяет характеризовать ее устойчивость в целом.

Объектом оценки уровня катастрофоустойчивости является информационная система, поэтому в качестве основного показателя может быть выбран, например, коэффициент доступности ее информационных ресурсов, характеризующий степень доступности (или процент доступных) информационных ресурсов для конечных пользователей системы. В модели может быть определен ряд «критических» информационных ресурсов, отсутствие доступа к которым (хотя бы в течение какого-то времени) приводит к невозможности своевременного выполнения системой своих функций.

Поскольку одним из основных показателей, характеризующих информационную систему, является: $P(T_{ФУНК} \leqslant T_Д)$ — своевременность, определяемая вероятностью выполнения системой своих функций за время, не превышающее $T_Д$ (директивно задано), то в качестве основного показателя, используя допущение, что средства резервирования выполнят свои функции в случае отказа основных средств ИС, может быть выбрано время восстановления после катастрофы ($T_{В.К.}$) с оценкой вероятности его выполнения $P(T_{В.К} \leqslant T_{ДВ.К.})$, исходя из вышеизложенных предположений и допущений. $T_{ДВ.К.}$ — директивно заданное время восстановления после катастрофы или максимальное время простоя ИС.

Основной показатель катастрофоустойчивости может быть рассчитан как для ИС в целом, так и для каждого ее элемента или уровня (головной, региональный, районный и т. д.).

5. Выбираются дополнительные (частные) показатели катастрофоустойчивости информационной системы. На их основе вычисляется основной показатель катастрофоустойчивости, или же частные показатели выступают в качестве ограничений к основному. К таким показателям ИС можно отнести, например:

— коэффициент энергетической безопасности;
— коэффициент пожаробезопасности;
— коэффициент отказоустойчивости (коэффициент готовности);
— предельная пропускная способность информационных каналов;
— коэффициент климатоустойчивости (изменения климатики);
— коэффициент защищенности (от внешних воздействий);
— степень информационной защищенности;

— коэффициент оперативности управления функционированием;
— эффективность функционирования (полнота, достоверность, своевременность получения (сбора, передачи) информации, как функции в зависимости от времени).

6. Разрабатываются модели расчета показателей катастрофоустойчивости (основного и частных) в зависимости от принципа функционирования элементов информационной системы и моделей рисков.

В общем случае ИС представляет собой иерархическую информационную систему, поэтому основной показатель для нее в целом рассчитывается на основе показателей элементов с применением весовых коэффициентов, обозначающих критичность элемента (например, по количеству обслуживаемых пользователей, катастрофобезопасности элемента и т. д.). Для приведенного выше примера (1) критичность головного ЦОД (b_1) будет определяться как 1, критичность регионального ЦОД (b_{2i}) как отношение количества обслуживаемых пользователей к общему пользователей ИС умноженное на коэффициент катастрофобезопасности (см. ниже п. 7) и т. д.

Основной показатель катастрофоустойчивости может быть рассчитан как статический или как изменяющийся в зависимости от времени (например, как коэффициент оперативной доступности информационных ресурсов ИС в данный момент времени).

7. Модели снижения влияния рисков на работу информационной системы.

Для каждого вида рисков разрабатываются модели контрмер, например, на основе собранной статистики или анализа причин возникновения рисков.

При составлении модели должны быть учтены «стоимость» контрмер и оценка «остаточного влияния» риска на ИС в случае принятия данных контрмер. В качестве критерия достаточности контрмеры в модели может выступать соотношение «стоимость/эффективность».

Для составления точной модели оценки времени восстановления объектов информационной системы после катастрофы, а также достаточности моделей контрмер, необходимо провести категорирование объектов ИС по степени катастрофоустойчивости.

Категорирование объектов ИС предполагает два взаимосвязанных процесса:

— анализ уязвимости элементов ИС;
— оценка катастрофоустойчивости конкретных ЦОД и ЦКС.

Анализ уязвимости элементов ИС должен проводиться для наиболее важных (опасных) по степени угроз катастроф:

— по максимальному нематериальному компоненту риска;

— по источнику наибольших материальных потерь;

— по наиболее вероятным угрозам.

Анализ катастрофобезопасности элементов информационной системы должен выявить основные критические элементы, которые под воздействием катастроф и их последствий выходят из строя, теряют работоспособность, что приводит к отказу фрагмента ИС или всей системы в целом. При необходимости вносятся поправки в модель катастрофоустойчивости в части нормирующих коэффициентов важности элементов ИС (b_1, b_2, b_3 и т. д.).

Факторы, которые негативно влияют на эффективность функционирования ЦОД, ЦКС:

— отключение электропитания;

— нарушение условий функционирования средств ЦОД, ЦКС (повышенная влажность, недопустимые колебания температуры, механические повреждения);

— отсутствие ЗИП и обменного фонда;

— нарушение условий для осуществления и продолжения выполнения ОДП своих функций;

— опасность для жизни ОДП.

Таким образом, анализируя воздействие катастроф на критические элементы объекта, можно отметить, что его уязвимость зависит от мощности (категории) катастрофы и наличия средств, нейтрализующих негативные факторы: как средств, находящихся на элементе ИС, так и возможностей оперативной (в течение определенного времени, не превышающего $Т_{ДВ.К.}$) ликвидации последствий катастрофы. Если катастрофа «локализована», то она приводит к минимальному ущербу или вообще не вызывает ущерба. Примером этого может служить возгорание, которое удалось нейтрализовать средствами пожаротушения, находящимися в ЦОД.

В общем случае модель катастрофобезопасности элемента ИС должна учитывать:

— вероятность реализации угрозы катастрофы;

— расчетный нематериальный ущерб;

— расчетный материальный ущерб;

— вероятность выхода из строя критических элементов объекта;

— готовность средств, снижающих уязвимость объекта по отношению к катастрофе.

8. На основании составленных частных моделей рисков, противодействия им, функционирования информационной системы создается общая модель катастрофоустойчивости. На основании данной модели проводятся расчеты и определяются стратегии повышения защищенности элементов ИС.

Идеальным вариантом проведения полноценного моделирования катастрофоустойчивости информационной системы является создание ситуационно-аналитических центров, реализующих модели функционирования ИС (см. [15]). Их использование значительно повышает эффективность функционирования и развития информационной системы в целом.

Заключение

Большие информационные системы все чаще становятся неотъемлемой частью производственного процесса на промышленных предприятиях, коммерческих организациях и в государственных структурах. Чем крупнее организация, тем большая по масштабам информационная система требуется для охвата и управления всем производственным и/или технологическим циклом, но и тем больше риск потери критически важной информации.

Для больших систем, работа которых связана с оперативной обработкой информации, а простой оборачивается большими материальными (или нематериальными: политические, имиджевые и т. д.) потерями, необходимо уделять большое внимание степени защищенности систем от катастрофических воздействий не только природного, но и техногенного, и антропогенного характера. В частности, общепризнано, что основные проблемы создания и внедрения информационных технологий в больших организационных системах сопряжены с влиянием человеческого фактора [1, 4–7]. Это еще раз подчеркивает, что система обеспечения катастрофоустойчивости информационной системы должна быть всесторонне продумана, что бы избежать неучтенных рисков и неоправданных затрат. Необходима разработка модели катастрофоустойчивости системы, ее проверка и совершенствование, тщательное исследование результатов моделирования.

Описанный в статье методологический подход к моделированию катастрофоустойчивости информационной системы был разработан для оценки больших территориально-распределенных информационных систем и применялся при выполнении работ по повышению катастрофоустойчивости Государственной автоматизированной системы Российской Федерации «Выборы».

Литература

1. *Дружинин Г. В.* Человек в моделях технологий. Часть I: Свойства человека в технологических системах. М.: МИИТ. 1996. 124 с.
2. *Акимова Г. П.*, *Соловьев А. В.* Методология оценки надежности иерархических информационных систем // Системный подход к управлению информацией: Труды ИСА РАН. Т. 23. М.: КомКнига/URSS, 2006. С. 18–47.
3. *Акимова Г. П.*, *Соловьев А. В.*, *Яншевский И. М.* Методология оценки эффективности иерархических информационных систем // Системный подход к управлению информацией: Труды ИСА РАН. Т. 23. М.: КомКнига/URSS, 2006. С. 48–66.
4. *Цибулевский И. Е.* Ошибочные реакции человека-оператора. М.: Сов. Радио, 1979. 208 с.
5. *Киреенко В. Е.* Человеческий фактор корпоративных информационных систем (на примере Томского горисполкома) // Вестник Томского государственного университета. 2002. № 275.
6. *Ветлугин К.* Человеческий фактор // Computerworld. 2006. № 11.
7. *Акимова Г. П.*, *Соловьев А. В.*, *Пашкина Е. В.* Методологический подход к определению влияния человеческого фактора на работоспособность информационных систем // Информационно-аналитические аспекты в задачах управления: Труды ИСА РАН. Т. 29. М.: Издательство ЛКИ/URSS, 2007. С. 102–112.
8. Научно-технический отчет. Совершенствование и доработка методического аппарата для оценки эффективности функционирования КСА ГАС «Выборы» // ИСА РАН, 2004.
9. *Завгородний В. И.* Комплексная защита информации в компьютерных системах. М: ВА РВСН им. Петра Великого, 1999.
10. ГОСТ Р51275–99 Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
11. *Постон Т.*, *Стюарт И.* Теория катастроф и ее приложения. М.: Мир, 1980.
12. *Касти Дж.* Большие системы. Связность, сложность и катастрофы. М.: Мир, 1982.
13. *Герасименко А.* Защита машин от биоповреждений. М.: Машиностроение 1984.
14. Актуальные проблемы регулирования природной и техногенной безопасности в XXI веке // Материалы десятой Международной научно-практической конференции по проблемам защиты населения и территорий от чрезвычайных ситуаций. 19–21 апреля 2005 г. / МЧС России. М.: Ин-октаво, 2005. 400 с.
15. *Акимова Г. П.*, *Соловьев А. В.*, *Пашкина Е. В.* Ситуационно-аналитические центры, как способ снижения влияния человеческого фактора на принятие управленческих решений при эксплуатации больших информационных систем // Информационно-аналитические аспекты в задачах управления: Труды ИСА РАН. Т. 29. М.: Издательство ЛКИ/URSS, 2007. С. 113–122.