Фалин М. Н.

ПРОБЛЕМА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Адрес статьи: www.gramota.net/materials/1/2008/12/65.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2008. № 12 (19). С. 203-206. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2008/12/

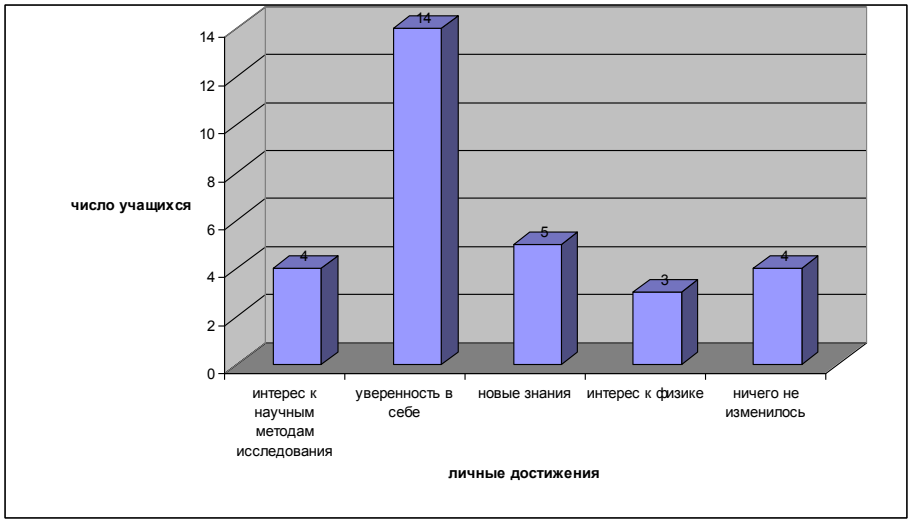

Рис. 2. *Результаты итогового анкетирования школьников*

Если учителю удается пробудить интерес учащихся к своему предмету, это большая профессиональная победа, создающая предпосылки для самостоятельной творческой работы школьников.

ПРОБЛЕМА ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Фалин М. Н.
Московский государственный институт радиотехники, электроники и автоматики (технический университет)

Развитие современных средств вычислительной техники, их внедрение в различные сферы практической деятельности, расширение областей применения автоматизированных систем управления и обработки информации привело к ситуации, когда современный мир невозможно представить без сложных информационных систем, АСОИ, АСУ ТП, автоматических систем, вычислительных комплексов, телекоммуникационных сетей – всего того, что создает информационно-вычислительно-телекоммуникационную среду, обеспечивающую человеку целый спектр сервисных возможностей: от информационной поддержки до автоматического управления процессами и системами.

В применении таких процессов существуют как положительные моменты, такие как, сокращение рутинных действий человека в процессе жизнедеятельности, увеличения его потенциала за счет того, что все большее количество функций передается вычислительным устройствам и системам управления, так и отрицательные стороны, возрастание потенциальной опасности возможных последствий сбоя или отказа в их работе для объекта управления, человека, окружающей среды.

Среди основных опасностей, возникающих при отказе элементов систем выделим следующие [ISO 17799: 1998]:

- физическая потеря объекта управления;
- выдача неправильных или недостоверных данных;
- нарушение управления, приводящее к неуправляемому характеру течения управляемого процесса;
- возникновение смежных деструкционных последствий;
- потери ресурсов, ценностей, продукции.

В результате чего, возможно возникновение следующих последствий, таких как возникновение локальных и глобальных экологических катастроф, возникновение радиологических, химических, биологических и других локальных и глобальных загрязнений, несанкционированное применение средств вооружения, разрушение объектов, катастрофы движущихся объектов, гибель флоры, фауны, человеческие потери.

Таким образом, учитывая широкий спектр применения информационных систем, актуальным является рассмотрение вопросов по обеспечению безопасности функционирования информационных систем, а так же методов позволяющих выявлять появляющиеся сбои и отказы элементов в результате воздействия внешних факторов.

Перед тем как начать рассматривать вопросы по обеспечению безопасности информационной системы дадим ряд определений, которые в дальнейшем помогут дать полную картину.

Система – это множество взаимосвязанных элементов, каждый из которых связан прямо или косвенно с каждым другим элементом, а два любых подмножества этого множества не могут быть независимыми, не нарушая целостность, единство системы.

Элементы системы – это простейшая структурная составляющая системы, которая в рамках данной системы не структурируется.

Под безопасностью функционирования систем понимается, согласно [Тхыонг 1999: 323], свойство системы противодействовать появления аварийных ситуаций, влияющих на жизнедеятельность человека и среду его обитания при функционировании системы в соответствии с целевым назначением.

Под неадекватным поведением системы понимается возникновение одной из следующих ситуаций: отказ одного или нескольких элементов системы, сбой одного или нескольких элементов, сочетание отказа одного или нескольких элементов и сбоя одного или нескольких элементов.

Возникновение ситуации, когда хотя бы один из элементов системы переходит в неисправное и неработоспособное состояние, приводит к отказу.

Система может находиться в следующих видах технического состояния: исправном и неисправном, работоспособном и неработоспособном, правильного и неправильного функционирования.

Причинами сбоя (отказа) в работе системы могут быть:

– закономерные воздействия, вызванные несовершенством конструкции, компоновки, алгоритма обработки, качеством и сроком службы элементов и т.д.;

– случайные воздействия, вызванные неконтролируемыми процессами, происходящими во внешней среде, в самой системе, а также выходом параметров и характеристик элементов системы за пределы нормальных значений;

– случайные и закономерные воздействия, вызванные сознательным целенаправленным воздействием на систему со стороны внешней среды.

В первом случае существуют специальные методики конструирования, проектирования, эксплуатации и сопровождения, которые учитывают возможные недостатки и позволяют их оперативно устранять, не доводя до возникновения неадекватного поведения.

Во втором случае, исключить полностью влияние внешних случайных факторов в полном объеме не представляется возможным, возможно оценить и снизить или исключить полностью влияние выхода параметров и характеристик элементов системы.

В третьем случае, существуют организационно-технические мероприятия, снижающие уровень и вероятность воздействия, однако, не имеется возможности полностью исключить их влияние.

Для повышения безопасности функционирования систем применяются различные методы, классифицируемые по применяемому математическому аппарату [Тхыонг 1999: 323; Петров 2000: 38]:

– методы, основанные на анализе функционирования виде систем уравнений;
– методы, использующие основные теоремы теории вероятности и теории массового обслуживания;
– логико-вероятностные методы;
– топологические методы.

Эти методы направлены на повышение безопасности систем, прогнозирование сбоев и отказов, планирование резервирования отдельных элементов систем.

Чтобы быть готовым к неадекватному поведению элементов, следует проводить специальные мероприятия, рассмотрим один из способов это применение методов анализа систем на предсказуемость поведения.

Для построения систем с предсказуемым поведением в условиях возникновения нештатной ситуации необходимо исключить все возможные действия системы в этих условиях, не относящиеся к выполнению основных и вспомогательных заранее оговоренных функций.

Можно предложить три основных метода решения стоящей задачи:

– метод комплексного анализа (МКА);
– метод приближенного анализа (МПА);
– метод анализа на основе тестирования систем (МАТС).

Метод комплексного анализа (МКА) [Петров 2002: 12] предназначен для осуществления полного комплексного анализа системы на предсказуемость поведения в условиях одиночного или множественного отказа составляющих элементов.

Достоинством данного метода является полное выявление всех возможных последствий отказа. Основным и главным недостатком, препятствующим его практическому использованию, является его трудоемкость, которая возрастает геометрически пропорционально количеству рассматриваемых элементов и для большого их числа является непригодным. Как промежуточный вариант метода комплексного анализа можно предложить вариант, когда система разбивается на достаточно малое количество элементов и число рассматриваемых факторов тоже невелико. При этом необходимая степень детализации обеспечивается последующим разбиением выбранных на первом этапе элементов на субэлементы с применением к каждому такому разбиению приведенного выше метода. Очевидно, что в пределе мы получим такую же трудоемкость, как и при применении метода комплексного анализа к системе в целом. Поэтому выигрыш и практическое применение может быть достигнуто либо при большом объеме однотипных элементов, когда анализ одного из них переносится на остальные, либо при ограничении степени детализации структуры системы.

Метод приближенного анализа (МПА) [Петров 2002: 12] является подмножеством метода комплексного анализа и заключается в том, что вводятся допустимые граничные условия на число и перечень рассматриваемых элементов системы, на число и перечень рассматриваемых функций системы, на точность модели-

рования работы системы. При этом возможно применение дополнительных методов определения перечней элементов, функций и точности моделирования, допустимых для обеспечения требуемой предсказуемости работы системы. Достоинством метода являются меньшие, по сравнению с предыдущим методом, затраты на анализ. Недостатками метода являются вероятность пропуска фактора, влияющего на предсказуемость системы, и его трудоемкость.

Метод анализа на основе тестирования систем (МАТС) [Петров 2002: 12] исходит из предположения, что при анализе необходимо рассматривать не совокупность внешних и внутренних действующих факторов, как это было в двух предыдущих методах, а максимально возможное множество реакций системы и выделять (а затем и исключать, по возможности) действие тех факторов, которые могли бы вызвать такую реакцию, или блокировать возможность появления такой реакции вообще. Данный метод, как видно из предыдущего рассуждения, концентрируется не на перечне внешних воздействий, который может быть сколь угодно большим, а на возможностях технических средств по отработке команд информационно-управляющей системы, которые, во-первых, имеют конечный характер, и их существенно меньше, чем действующих факторов, во-вторых. Таким образом, налицо выигрыш в затратах на анализ и одновременно с анализом выявляется перечень технических возможностей, подлежащих ограничению. К недостатку метода можно отнести то, что он не работает в случае, когда планируемая неадекватная реакция системы находится в поле возможных значений для нормальной работы системы. Например, вследствие какого-либо воздействия летательный аппарат вместо того, чтобы лететь прямо, повернул налево, но параметры полета находятся в нормальных пределах.

Анализируя предлагаемые методы, а также их достоинства и недостатки, можно определить область возможного применения каждого из методов [Петров 2002: 12].

Так, все три метода применимы в случае, когда известна внутренняя структура системы. Это обычно происходит при новой разработке или модификации существующей системы. В этом случае, выбор конкретного метода определяется ресурсными возможностями и необходимой степенью предсказуемости.

В случае, когда неизвестна внутренняя структура системы, возможно применение только первых двух методов. Это происходит в случае, когда внутренняя структура объекта анализа преднамеренно или случайно представляется «черным ящиком», например, объект или его является «know-how» (например, внутренний интерфейс Windows), утеряна документация на систему, объект опечатан или защищен от обратной трансляции, или когда нет непосредственного взаимодействия с объектом (например, АСУВ или АСУО потенциального противника).

Методы позволяют выявлять уязвимость в реализации по отношению к внешним и внутренним воздействующим факторам, выявлять опасности, заложенные в схемных и программных решениях.

Также важным является тот факт, что методы позволяют выявлять возможность появления новых, не планируемых реакций на выходе системы, и, следовательно, прогнозировать возможные дополнительные последствия, возникающие в этом случае.

В любом случае, перед проведением анализа системы на предсказуемость поведения, необходимо понимать потенциальную необходимость такого анализа вследствие дополнительных, и, может быть существенных, затрат на него.

Перечень факторов, принимаемых в рассмотрение, при проведении анализа может быть ограничен или дополнен, в зависимости от полноты рассмотрения. При этом необходимо выделить несколько основных тенденций такого рассмотрения:

- рассмотрение детерминированного внешнего воздействия. В этом случае, рассматривается только поток внешних детерминированных воздействий на систему, исключается детерминированное внутреннее и все виды случайных воздействий и предполагается, что любое воздействие может привести к отказу ЭС;
- рассмотрение совокупного детерминированного внешнего и внутреннего воздействия. В этом случае, рассматривается только поток внешних и внутренних детерминированных воздействий на систему, исключаются все виды случайных воздействий и предполагается, что любое воздействие может привести к отказу ЭС;
- совокупное рассмотрение внешних и внутренних воздействий. В этом случае, весь поток внешних и внутренних детерминированных и случайных воздействий на систему рассматривается как суперпозиция детерминированных внешних и внутренних воздействий с возможным случайным, уровнем самого воздействия, при этом не выделяются значимые или незначимые воздействия и предполагается, что любое воздействие может привести к отказу ЭС;
- рассмотрение случайного совокупного внешнего и внутреннего воздействия. В этом случае, исключается детерминированное внутреннее и внешнее воздействие воздействий и предполагается, что любое воздействие может привести к отказу ЭС. Данный случай полезно рассматривать для случая, когда необходимо оценить степень предсказуемости поведения системы от влияния случайных факторов.

Методы анализа систем на предсказуемость поведения [Тхыонг 1999: 323; Петров 2000: 38] с целью повышения безопасности их функционирования являются ресурсоемкими. Одним из способов решения этой задачи является применение функциональной стандартизации на элементы системы и, может быть, на систему в целом. Рассмотрим подробнее, как это достичь практически.

Для этого должны существовать Реестр сертифицированных продуктов и нормативное обеспечение, обеспечивающее включение объекта в реестр. Реестр должен содержать типовые элементы (программные

модули, схемные решения, типовые алгоритмы) такие, что для них уже выполнена процедура анализа на предсказуемость и определен перечень последствий отказа системы.

Для формирования реестра необходимо, как уже было сказано, наличие нормативного обеспечения. Оно включает в себя нормативные акты, определяющие сертификацию на предсказуемость и методики тестирования. В качестве нормативных актов должны выступать функциональные стандарты (профили) – набор взаимосогласованных и взаимоувязанных стандартов, направленных на достижение конкретной цели. Примером могут служить функциональные стандарты – Профили открытых систем организаций-пользователей. В общем случае, на каждый типовой элемент, входящий в реестр, должен быть разработан функциональный стандарт - Профиль типового элемента, определяющий его характеристики, в том числе, с точки зрения предсказуемости систем.

При практическом применении, в начальный момент осуществляется декомпозиция системы на элементы, но не на любые, а только на те, которые входят в реестр. В том случае, если элемента в реестре нет, для него осуществляется процедура анализа согласно одному из приведенных выше методов. После того, как для всех элементов будут определены перечни возможных последствий отказа, проводится интегральный анализ для системы в целом.

Очевидно, что затраты на анализ предсказуемости системы в условиях отказа снижаются, причем снижение будет тем более ощутимым, чем больше типовых элементов будет в перечне и чем больше их будет применено в конкретной разработке.

Таким образом, можно сделать несколько выводов:

1. Появление новой характеристики системы – предсказуемость поведения в условиях неадекватного поведения элементов системы – повышает качество разработки и эксплуатации системы.
2. Проведение анализа на предсказуемость поведения в условиях неадекватного поведения элементов системы повысит ее безопасность функционирования.
3. Применение методов анализа системы на предсказуемость является ресурсоёмким, поэтому выполнение такого анализа должно быть определено существенным значением фактора предсказуемости для функционирования конкретной системы (автономность работы, опасность техногенной катастрофы и т.д.).
4. Применение функциональной стандартизации может существенно сократить ресурсоёмкость анализа.

Список использованной литературы

1. **Евтихиев Н. Н., Петров А. Б.** Моделирование последствий отказа: обобщенный подход // Вопросы кибернетики: устройства и системы: Межвуз. сб. науч. трудов. – М.: МИРЭА, 1996.
2. **Петров А. Б.** Проектирование информационных систем. Безопасность функционирования: Учебное пособие. – М.: МИРЭА, 2008. – 132 с.
3. **Петров А. Б.** Разработка систем с предсказуемым поведением в условиях отказа элементов системы // Журнал радиоэлектроники. – 2002. - № 12. – С. 12.
4. **Петров А. Б.** Открытые информационные системы: Учебное пособие. - М.: МИРЭА, 2000. – 38 с.
5. **Тхыонг Н. К.** Методы и модели надежности, эффективности и безопасности сложных технических систем в конфликтных ситуациях: Дисс. на соиск. уч. ст. д. т. наук. – М.: ВЦ РАН, 1999. – 323 с.
6. **Харрасов И. А.** Анализ надежности сложных технических систем в процессе их проектирования на основе понятий развивающихся систем. – Уфа: УфГАТУ, 1999. – 163 с.
7. **ISO 17799: 1998. Управление информационной безопасностью. Практические правила.**

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТА В ВИРТУАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ С ЭЛЕМЕНТАМИ САМОДИАГНОСТИКИ[1]

Федосеев В. М., Ягова Е. Ю.

Пензенская государственная технологическая академия

Условия обучения в современном вузе таковы, что они требуют от студента значительно более высокого уровня владения умениями самоуправления учением, чем тот, который имел место в средней школе. Однако, если речь идёт об учебной дисциплине «Математика» для технических специальностей, то, как показывает существующая практика, большинство студентов в этой области не обладает необходимыми навыками и потому испытывает серьёзные трудности с обучением. При этом несформированными, а, следовательно, неприменяемыми являются умения студентов разбивать конечную цель решения задачи на ряд промежуточных; выбирать рациональные способы решения в контексте имеющегося целевого предписания; анализировать причины собственных удач и неудач поисковой деятельности; исправлять свои и чужие ошибки и неточности; умение формулировать задачи и определять, в каком направлении возможно развивать и совершенствовать полученные результаты [5].

[1] Исследование выполнено при финансовой поддержке РГНФ в рамках научно-исследовательского проекта РГНФ «Самодиагностика как средство повышения качества базовых знаний студентов по высшей математике», проект № 08-06-00332а.