Сборник докладов на XXIII межведомственной НТК “Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем”, 5-7 июля 2004 г., г. Серпухов, ВИ РВ, часть 4, С. 242-246.
УДК 681.5
ББК 39.5

ктн доцент Белов В.П., дтн профессор Голяков А.Д.

Научно-исследовательский институт точной механики, г. Санкт-Петербург

АНАЛИЗ МЕТОДОВ ОЦЕНИВАНИЯ БЕЗОПАСНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ

Современный этап развития отечественной промышленности характеризуется, с одной стороны, остаточными явлениями, которые обусловлены последствиями произведённых в нашей стране “реформ”, а, с другой стороны, жёсткими требованиями, которые предъявляются к качеству производимых изделий. В условиях рыночных отношений требования к качеству изделий подразделяются на обязательные и рекомендательные. В соответствии с действующим законодательством (в частности, в соответствии с законом “О техническом регулировании”) к обязательным относятся требования, направленные на обеспечение:

- безопасности жизни, здоровья и имущества, охраны окружающей среды;
- технической и информационной совместимости, взаимозаменяемости изделий;
- единства методов их контроля и маркировки.

Все остальные требования носят рекомендательный характер. В состав этих требований входят основные потребительские (эксплуатационные) требования, а также требования, которые предъявляются к методам их оценивания и контроля, требования к упаковке, маркировке, транспортировке, хранению, применению и т.п.

Корректное решение задач установления требований по безопасности к сложным техническим системам и последующего подтверждения этих требований возможно при наличии методологических основ теории безопасности. Однако до настоящего времени работы по формированию такой методологии находятся на недостаточно высоком уровне. Свидетельством этому является тот хаос, который наблюдается в современной терминологической базе теории безопасности.

С вступлением в силу Федерального закона “О техническом регулировании”, имеющего известные недостатки [1], факт отсутствия согласованного понятийного аппарата теории безопасности стал очевидным. Существенные лишь в каком-то одном отношении дефиниции, приведённые в Законе РФ “О безопасности”, стали абсолютизироваться в других нормативно-правовых документах. В результате возникли разного рода парадоксы и затруднения.

Это, в первую очередь, относится к такому основополагающему понятию, как “безопасность”. В соответствии с Законом РФ “О безопасности” под этим термином понимается состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Признание понятия “безопасность” как “состояния” применительно к социальным системам являлось, по всей видимости, удобным решением в тот период времени и в тех условиях, в которых создавался и принимался закон “О безопасности”. Действительно, состояние – это качественное, а не количественное понятие, так как система может либо находиться, либо не находиться в некотором состоянии. Кроме того, особенность термина “безопасность государства”, определённого как “состояние”, заключается в том, что в другом состоянии, при котором оно не способно противостоять внутренним или внешним угрозам, государство существовать не может. Этим, по всей видимости, и объясняется отсутствие в Федеральном законе “О безопасности” даже упоминания о состоянии, противоположном состоянию безопасности.

Другая ситуация складывается при решении задач построения основы новой системы технического регулирования. Эта система, как известно, должна в максимальной степени снизить технические барьеры и повысить конкурентоспособность отечественной продукции путём установления соответствующих показателей безопасности в технических регламентах. При этом возникает необходимость измерения (оценивания) риска, выступающего в роли показателей безопасности. Следовательно, безопасность технической системы – это “свойство”, которое в отличие от “состояния”, относится к количественным понятиям.

Основные подходы к построению методологии теории безопасности применительно к системам ракетно-космической техники и системам движения поездов метрополитена предложены в монографии “Надёжность и безопасность информационно-управляющих систем (методы оценивания и контроля)”, которая написана сотрудниками НИИ “Точной механики” [2].

В этой монографии под безопасностью понимается свойство системы, характеризующееся её способностью противостоять внутренним и внешним угрозам, сохраняя безопасное состояние в течение заданного времени и в определённой области пространства. В качестве количественных показателей безопасности выбраны характеристики функции распределения ущерба, в частности, её квантиль, математическое ожидание, среднее квадратическое отклонение, также вероятность перехода системы из безопасного состояния в опасное, т.е. значение приемлемого (допустимого) риска.

Для оценивания показателей безопасности на практике используются качественные и количественные методы.

В группу качественных методов входят хорошо зарекомендовавшие себя на начальных этапах жизненного цикла технических систем методы “Проверочного листа”, “Что будет, если…?”, “Анализ вида и последствий отказов”

(АВПО), метод изучения угроз (опасностей) и работоспособности (HAZOP - Hazard and Operablity Research) и т.п.

Эти методы отличаются простотой анализа и могут быть реализованы специалистами практически любой квалификации при исследовании безопасности сложных технических систем. С помощью качественных методов в ряде случаев удаётся выявить так называемые “проблемные области”, например, виды одиночных отказов, которые могут привести к “опасному” отказу системы, элементы или подсистемы, требующие введения дополнительных средств защиты от внутренних и внешних угроз, и т.п. Наибольший эффект при этом достигается в результате использования всей совокупности качественных методов.

С помощью методов этой группы решаются следующие задачи:

выявляются виды угроз безопасному состоянию системы (в том числе виды опасных отказов), изучаются их причины, механизмы и условия возникновения и развития с целью определения возможности принятия оперативных решений или соответствующих мер защиты;

проводится качественный анализ последствий отказов путём качественного оценивания возможного ущерба при его возникновении;

определяются критичные элементы, т.е. такие элементы, отказ которых может стать опасным, т.е. способным при неблагоприятных обстоятельствах перевести систему из безопасного состояния в опасное;

анализируются правила поведения персонала в аварийных ситуациях, обусловленных возможными отказами системы, предусмотренные эксплуатационной документацией, вырабатываются предложения по их совершенствованию или внесению соответствующих изменений в эксплуатационную документацию при их отсутствии;

проводится анализ возможных ошибок персонала при эксплуатации, техническом обслуживании и ремонте системы, оценивается их возможные последствия, вырабатываются предложения по совершенствованию человеко-машинных интерфейсов и введению дополнительных средств защиты от ошибок персонала, по совершенствованию инструкций по эксплуатации, техническому обслуживанию и ремонту.

Основой этих методов является анализ ситуаций, которые способны привести к опасному событию. В частности при использовании метода изучения угроз и работоспособности (HAZOP) определяется перечень параметров, при отклонении которых от заданных значений возникают или развиваются опасные процессы. Контролю подвергается по очереди каждая составная часть технической системы. В ходе такой проверки ставится ряд вопросов, сформулированных на основе ключевых слов. Ключевые слова используются для того, чтобы с помощью разработанных на их основе вопросов можно было бы изучить все возможные отклонения от ТЗ. В качестве ключевых слов применяются: “меньше”, “больше”, “нет” (“отсутствие”) и т.п.

Исследования каждого отклонения установленных параметров от заданных значений проводятся как в прямом направлении (т.е. к каким последствиям

эти отклонения могут привести), так и в обратном направлении (т.е. каковы могут быть причины возникновения этих отклонений). При обнаружении “опасных” отклонений принимаются соответствующие мероприятия, например, проводится модификация конструкции критичного элемента системы.

При использовании группы количественных методов решается задача оценивания безопасности технических систем. Методы количественного оценивания показателей надежности и безопасности ИУС в зависимости от способа получения исходных данных подразделяются на три группы:

расчетные;

экспериментальные;

расчетно-экспериментальные.

Расчетные методы основаны на вычислении показателей безопасности систем по справочным данным и официальным сведениям:

о надежности её элементов с учетом функциональной структуры и видов разрушения при возникновении опасных отказов;

о свойствах материалов, элементов и нагрузке на них;

о механизме “опасных” отказов элементов, составных частей и комплектующих изделий;

об ошибках персонала, обслуживающего аналогичные системы при возникновении штатных и нештатных ситуаций в процессе их эксплуатации;

об условиях эксплуатации технических систем при транспортировке, хранении и использовании по назначению и т.п.;

о критичных элементах структуры системы, отказ которых является угрозой безопасности, и допустимых значениях интервалов времени, необходимых для организации защиты от этой угрозы;

о возможных воздействиях на систему возмущающих факторов окружающей среды, их значениях, продолжительности и интенсивностях появления;

о характеристиках преднамеренных угроз безопасности (при необходимости противодействия этим угрозам).

В основе экспериментальных методов лежит использование статистических данных, получаемых при нормальных или ускоренных испытаниях на безопасность системы, или результатов её опытной или подконтрольной эксплуатации.

Основой расчетно-экспериментальных методов является расчёт показателей безопасности с помощью математической модели системы по исходным данным, определяемым экспериментальными методами.

К группе расчётных методов оценивания безопасности относятся:

- логико-графические методы;
- логико-вероятностные методы;
- аналитико-табличный метод;
- аналитико-статистический метод и др.

Основой логико-графических методов является графическое представление причинно-следственных связей логической последовательности событий, которые описывают развитие процесса, приводящего систему к опасному состоянию. К группе этих методов относятся хорошо известные методы деревьев отказов и деревьев событий [3].

Сущность логико-вероятностных методов [4] заключается в использовании функций алгебры логики для аналитической записи условий безопасности и в разработке строгих способов перехода от функций алгебры логики к вероятностным функциям, объективно выражающим свойства безопасности исследуемой системы.

Аналитико-табличный метод [2] основан на двухуровневой схеме расчёта. На нижнем уровне определяются безопасные состояния функциональных блоков (по входу), соответствующие им состояния каналов связи, обеспечивающие правильное функционирование блоков, а также вероятности данных состояний. На верхнем уровне по вероятности состояний функциональных блоков и каналов связи рассчитываются показатели безопасности системы с учетом конкретизации количества и вида каналов связи и присоединенных к ним блоков.

В основе аналитико-статистического метода [2] лежит построенная для решения задачи оценивания безопасности математическая модель системы. В результате обработки данных, полученных при статистических испытаниях с использованием этой модели, находятся искомые показатели безопасности.

Выбор расчётного метода производится на основе анализа структуры системы, степени трудоёмкости процесса оценивания, опыта и квалификации исполнителей, наличия ресурсов и необходимой информации для выполнения расчёта и других факторов. Высокий уровень достоверности искомых оценок достигается путём совместного использования двух-трёх расчётных методов.

Литература

1. Горячев А.В. Достоинства и недостатки Федерального закона “О техническом регулировании” / Стандарты и качество, №7, 2003.
2. Антонов Ю.В., Белов В.П., Голяков А.Д. и др. Надёжность и безопасность информационно-управляющих систем (методы оценивания и контроля). – СПб.: ОАО “НИИ ТМ”, 2004. – 326 с.
3. Хенли Э.Дж., Кумамото Х. Надёжность технических систем и оценка риска: Пер. с англ. В.С. Сыромятникова, Г.С. Дёминой. Под общ. Ред. В.С. Сыромятникова. – М.: Машиностроение, 1984. – 528 с.
4. Рябинин И.А. Надёжность и безопасность структурно-сложных систем. - С-Пб.: Политехника, 2000. - 248 с.