Сборник докладов на 3 НТК «Перспективы использования новых технологий и научно-технических решений в изделиях ракетно-космической техники разработки ГКНПЦ им. М.В. Хруничева», Москва, 2003, С. 41-43.

Антонов Ю.В., Белов В.П., Голяков А.Д.
Научно-исследовательский институт точной механики,
г. Санкт-Петербург

АНАЛИТИЧЕСКОЕ И ЭКСПЕРИМЕНТАЛЬНОЕ ОЦЕНИВАНИЕ ТЕХНИЧЕСКИХ СИСТЕМ ПОВЫШЕННОЙ ОПАСНОСТИ

При разработке технических систем (ТС) повышенной опасности, к которым относятся изделия ракетно-космической техники, а также при решении задач, связанных продлением сроков эксплуатации таких систем, возникают проблемы обоснования и оценивания показателей безопасности.

В настоящем докладе приводится краткое изложение основных положений в области безопасности с позиций разработчиков ТС повышенной опасности, обосновываются показатели безопасности и предлагаются аналитические и экспериментальные методы их оценивания.

Под ***безопасностью*** ТС в докладе понимается свойство технической системы непрерывно сохранять безопасное состояние в течение некоторого времени или наработки. Безопасность является сложным свойством, которое включает ряд свойств, в том числе: электробезопасность, пожаробезопасность, взрывобезопасность, ядерная (радиационная) безопасность, химическая безопасность, экологическая безопасность и т.д.

Свойство безопасности формируется при проектировании ТС. На последующих этапах жизненного цикла ТС (при производстве, испытаниях, упаковке, транспортировке, хранении, монтаже, использовании по назначению, техническом обслуживании и утилизации) это свойство проявляется, а его показатели изменяются.

Показатели безопасности могут иметь качественный или количественный вид. При необходимости получения количественных оценок показателей безопасности ТС целесообразно использовать вероятностные характеристики опасного события, которые являются функциями времени, например вероятность того, что в течение некоторого времени ТС будет находиться в безопасном состоянии, т.е. вероятность отсутствия опасного события.

Безопасным является состояние, в котором ущерб не превышает приемлемого значения. Такой ущерб называется [1, 2] приемлемым ущербом. В том случае, когда ущерб превышает приемлемое значение, ТС находится в опасном состоянии.

Ущерб может иметь характер любого вида [2]: материальный, природный, политический и т.п. Приемлемое значение ущерба устанавливается в нормативно-технической документации на определённый период времени в зависимости от того состояния (экономического, социального, культурного и т.п.) общества, в котором оно в данный момент находится.

Под *опасным событием* понимается событие, в результате которого происходит переход ТС из безопасного состояния в опасное состояние. Такое событие иногда называется происшествием. Опасное событие наступает при наличии угрозы безопасности.

Угроза безопасности представляет собой событие, которое предшествует опасному событию (предвестник опасного события). При появлении угрозы опасное событие может произойти или не произойти. Угроза безопасности возникает при выходе определённых (критических) параметров за установленные границы, при наличии ошибок операторов, программного обеспечения и т.п. Перечень этих параметров и ошибок устанавливается для конкретной ТС, исходя из анализа этапа жизненного цикла, условий эксплуатации и квалификации обслуживающего персонала.

Для защиты ТС от угроз используются средства защиты (барьеры защиты), которые в зависимости от способа их реализации подразделяются на следующие типы: технические, информационные, программные и административные. Одним из признаков классификации средств защиты (СЗ) является возможность изменения или прекращения процесса решения целевых задач технической системы. В соответствии с этим признаком средства защиты классифицируются на активные и пассивные.

Активные средства применяются в ТС, которые обладают свойствами самоорганизации и саморегулирования [2] при возникновении угрозы. Такие СЗ предназначены для обнаружения (идентификации) угрозы, оповещения (при необходимости) обслуживающего персонала о появлении угрозы и проведения необходимых операций (действий) для перевода ТС в так

называемое защитное (как правило, неработоспособное) состояние, из которого переход в опасное состояние маловероятен.

С помощью пассивных СЗ обеспечивается снижение реализации соответствующего типа возможной угрозы без потери работоспособности ТС. Функционирование пассивного средства защиты связано только с вызвавшим его работу событием (угрозой) и не зависит от работы ТС. Типы барьеров, а также уровень защищённости, которые они обеспечивают, определяются из анализа уязвимых мест (областей) ТС или её составных частей, а также значения ущерба, связанного с осуществлением угрозы.

Традиционные методы оценивания указанных показателей (аналитико-структурный, метод ветвей и границ и т.п.) связаны с аналитическим или графическим описанием структуры ТС и в большинстве случаев оказываются неприемлемыми. Это обусловлено тем, что современные системы повышенной опасности обладают, как правило, исключительно сложной структурой, которая с течением времени способна к реконфигурации.

Для оценивания показателей безопасности таких систем на этапе их проектирования используются аналитико-статистический и аналитико-табличный методы. Эти методы не требуют составления структурно-логической схемы ТС. Они применяется при наличии любых видов резервирования, в том числе ненагруженного резервирования и резервирования с восстановлением.

На этапе комплексной отработки ТС в настоящее время внедряются расчетно-экспериментальные методы, которые основаны на оценивании показателей безопасности по исходным данным, определяемым экспериментальным путём. Комплексная экспериментальная отработка базируется на проведении ряда испытаний, в том числе: испытания функциональных алгоритмов; климатические, механические испытания; ускоренные (ужесточенные) испытания; испытания на воздействие электромагнитных помех; испытания на устойчивость при внесении отказов. Все виды испытаний разрабатываемых в НИИ ТМ систем проводятся при климатических и механических воздействующих факторах в испытательном центре. Этот центр сертифицирован Госстандартом РФ в части проведения испытаний электронной техники, электротехнических изделий, приборов и средств автоматизации.

Приведённые в докладе показатели безопасности имеют понятный физический смысл и позволяют решать с помощью рассмотренных методов практические задачи по обоснованию и обеспечению заданных требований по безопасности ТС, а также по продлению сроков их эксплуатации. Реализация этих методов проведена в НИИ ТМ при подтверждении заданных требований к разработанным системам безопасности движения поездов метрополитена [3].

Литература

1. Алпеев А.С. Основные понятия безопасности // Надёжность и контроль качества, № 7, 1994. - С.29 - 40.

2. Статистические методы анализа безопасности сложных технических систем / Л.Н. Александровская, И.З. Аронов, А.И. Елизарова и др.; Под ред. В.П. Соколова - М.: Логос, 2001. – 232 с.

3. Поездная аппаратура комплексной системы обеспечения безопасности движения и автоматизированного управления движением поездов. Доказательство безопасности. – С-Пб.: ОАО «НИИ ТМ», 1998. – 155 с.