Методы менеджмента качества, №10, 2003, С.46 – 49

В.П. Белов, А.Д. Голяков, С.Я. Старков

О понятиях «надёжность» и «безопасность» технических систем с позиций разработчиков

Предисловие

При решении многих задач, возникающих перед заказчиками и разработчиками систем управления потенциально опасными объектами, к которым, в частности, относятся различного рода средства передвижения (от космических до подземных и подводных), встают проблемы обоснования показателей и критериев надёжности и безопасности, отражающих разные свойства создаваемых систем. Одним из способов решения этих актуальных проблем является, наряду с существующей нормативно-технической базой по надёжности изделий, разработка стандартов по безопасности технических систем. Центральное место при этом занимают вопросы терминологии, дискуссия по которым своевременно предложена редакцией журнала.

В настоящей статье, авторами которой являются сотрудники научно-исследовательского института точной механики, непосредственно участвующего в разработке систем безопасности, пожаро-взрывопредупреждения и тушения ракетно-космической техники, а также систем обеспечения безопасности управления движением поездов метрополитена, предлагается краткое изложение основных положений в области безопасности и терминологические аспекты взаимосвязи понятий «надёжность» и «безопасность» с позиций разработчиков потенциально опасных систем.

Все свойства, входящие в понятие «качество» изделия (технической системы), неразрывно связаны между собой. Но в то же время каждое из этих свойств имеет свою индивидуальность, отличительные черты, которые проявляются при использовании технической системы по целевому назначению. Это, в первую очередь, относится к свойствам надёжности и безопасности, которые, несмотря на некоторую близость, имеют принципиальные различия.

Благодаря успехам, достигнутым в теории надёжности, терминология в этой области не вызывает трудностей при разработке и контроле выполнения требований по надёжности технических систем (ТС) повышенной опасности. В то же время при решении аналогичных задач по безопасности возникают терминологические проблемы. Они обусловлены тем, что терминология, в частности, показатели и критерии безопасности, не носит понятный заказ-

чику и разработчику физический смысл и недостаточно чётко сформулирована. В результате свойство безопасности ТС в отдельных случаях включается в состав надёжности, а показатели надёжности (безотказности) применяются для оценивания уровня безопасности, что представляется, по нашему мнению, недостаточно корректным.

Действительно, для технических систем, представляющих опасность при изготовлении или эксплуатации, наиболее значимым из совокупности свойств, входящих в понятие «надёжность», является безотказность, под которой понимается свойство ТС сохранять работоспособное состояние в течение некоторого времени или наработки.

В качестве базового (ключевого) понятия в этом определении выступает работоспособное состояние. Находясь в этом состоянии, ТС выполняет свои функции, которые соответствуют её назначению, т.е. правильно и своевременно решает поставленные перед ней функциональные задачи. Перечень этих функций (целевых задач) определяется в нормативно-технической и (или) конструкторской документации и характеризуется определёнными параметрами. При выходе хотя бы одного из функциональных параметров за установленные границы нарушается работоспособность технической системы, т.е. происходит событие, называемое отказом. В результате этого ТС переходит в неработоспособное состояние.

Наряду с этими состояниями, выделяется так называемое предельное состояние, при котором дальнейшая эксплуатация ТС нецелесообразна или недопустима. Недопустимость эксплуатации связана, как правило, с тем, что работоспособная ТС может перейти из безопасного состояния в опасное. Эти состояния ТС являются предметом анализа не теории надёжности, а теории безопасности, которая в последнее время интенсивно развивается, но не имеет достаточно прочной терминологической базы [1]. Поэтому более детально остановимся на терминологических аспектах безопасности технических систем, которые в процессе эксплуатации способны причинить вред жизни или здоровью граждан, имуществу или окружающей среде.

В теории безопасности и ряде государственных и международных стандартов при формировании критерия вида состояния (опасное или безопасное) используется понятие «ущерб» [2 – 4, 6, 7], который характеризует потерю здоровья или жизни людей, убытки или непредвиденные расходы, урон или вред, который наносится сопрягаемым объектам или окружающей природной среде.*

---

* Под окружающей природной средой понимается окружение, в котором функционирует ТС, включая воздух, воду, землю, природные ресурсы, флору и фауну.

Безопасным является состояние, в котором ущерб не превышает приемлемого значения. Такой ущерб называется [2, 4] приемлемым ущербом. В том случае, когда ущерб превышает приемлемое значение, ТС находится в опасном состоянии.

Ущерб может иметь характер любого вида: материальный, моральный, природный, политический и т.п. [2, 7]. Приемлемое значение ущерба устанавливается в нормативно-технической документации, на определённый период времени в зависимости от состояния (экономического, социального, культурного и т.п.) общества. Таким образом, опасное и безопасное состояния различаются уровнем ущерба, который наносится технической системой населению, материальным объектам или окружающей природной среде, а не способностью ТС к выполнению заданных функциональных задач.

Очевидно, что неработоспособная ТС может находиться в безопасном (защитном от угрозы наступления опасного события) состоянии. С другой стороны, работоспособная (неисправная или исправная) ТС, решая соответствующие своему функциональному назначению задачи, может находиться в опасном состоянии, например, при превышении концентрации загрязняющих атмосферу веществ предельно допустимого значения. Следовательно, находящаяся в работоспособном состоянии ТС обладает свойством безотказности, а находящаяся в безопасном состоянии - свойством безопасности.

В связи с этим, под ***безопасностью*** ТС, на наш взгляд, понимается свойство технической системы непрерывно сохранять безопасное состояние в течение некоторого времени или наработки. Таким образом, свойством безопасности обладает такая техническая система, ущерб от которой в течение заданного времени не превышает приемлемого значения. Свойство безопасности формируется при проектировании технической системы и раскрывается на последующих этапах её жизненного цикла (при производстве, испытаниях, упаковке, транспортировке, хранении, монтаже, использовании по назначению, техническом обслуживании и утилизации).

Безопасность является сложным свойством, которое включает ряд свойств, в том числе: электробезопасность, пожаробезопасность, взрывобезопасность, ядерная (радиационная)
безопасность, химическая безопасность, экологическая безопасность, сейсмическая безопасность, бактериологическая безопасность и т.д.

Переход ТС из безопасного состояния в опасное состояние происходит в результате *опасного события*, которое иногда называется происшествием. Опасное событие наступает при превышении ущерба приемлемого значения. Обратный переход технической системы из опасного состояния в безопасное состояние осуществляется путём восстановления безопас-

ного состояния. Опасное событие имеет вероятностный характер. Оно происходит при реализации угрозы наступления опасного события (угрозы безопасному состоянию).

Угроза безопасному состоянию (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, отказов критичных элементов, ошибок в программном обеспечении и т.п. Перечень этих параметров, критичных элементов и ошибок устанавливается для конкретной ТС, исходя из анализа процесса функционирования, этапа жизненного цикла, условий эксплуатации и квалификации обслуживающего персонала.

В связи с необходимостью оценивания показателей безопасности и достаточно обширным диапазоном причин возникновения и последствий угроз проводится их классификация. Один из возможных вариантов такой классификации содержит четыре признака:

1. *Место появления угрозы*. В соответствии с этим признаком угрозы подразделяются на внутренние и внешние. К внутренним угрозам относятся отказы аппаратных средств и ошибки в программном обеспечении ТС. Внешние угрозы являются результатом воздействия на ТС со стороны людей, сопрягаемых объектов и окружающей природной среды;

2. *Источник появления угрозы*. Согласно этому признаку выделяются угрозы от:

- вредных факторов (шум, пыль, микроорганизмы, радиация, ультразвук и т.п.);

- электрических факторов (сопротивление изоляции токоведущих частей вблизи органов ручного управления автоматизированной системы, значение напряжения в цепях внешнего источника питания ТС и т.п.);

- термических факторов (сгорание части конструкции, отрыв термоизоляции от корпуса технической системы и т.п.);

- механических факторов (вибрация, удары и т.п.);

- других факторов, в том числе факторов старения (деградации) электрорадиоизделий, материалов и веществ;

3. *Последствия угроз*. Этот признак делит все угрозы безопасности на три группы. К первой группе относятся угрозы, последствия от которых связаны с возможностью гибели людей. В эту группу входят угрозы аварий и угрозы катастроф. Среди угроз аварий выделяются так называемые угрозы несчастных случаев, которые характеризуются различными травмами и потерей трудоспособности людей. Вторую и третью группы образуют соответственно угрозы нанесения вреда окружающей среде и угрозы экономических потерь;

4. *Мотивы угроз*. По этому признаку угрозы классифицируются на ненамеренные и преднамеренные. Ненамеренными угрозами являются стихийные бедствия, ошибки персо-

нала, обусловленные некомпетентностью или случайным нарушением инструкции по эксплуатации (например, в связи с небрежностью или невнимательностью), отклонения условий эксплуатации от условий, заданных в технической документации, и т.п. Преднамеренные угрозы могут быть обусловлены такими действиями посторонних лиц, в задачу которых входит нанесение вреда окружающей природной среде, здоровью людей или ущерба технической системе или сопрягаемым с ней объектам.

Для защиты ТС от угроз используются специальные средства. Средства защиты (барьеры защиты) в зависимости от способа их реализации подразделяются на технические, информационные [5], программные и административные. Другим признаком классификации средств защиты 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 технических системах, которые обладают свойствами самоорганизации и саморегулирования [4] при возникновении угрозы. Такие барьеры предназначены для обнаружения (идентификации) угрозы, оповещении (при необходимости) обслуживающего персонала о появлении угрозы и проведения необходимых операций (действий) для перевода технической системы в так называемое защитное (как правило, неработоспособное) состояние, из которого переход в опасное состояние маловероятен (практически исключён).

С помощью пассивных барьеров защиты обеспечивается снижение реализации соответствующего типа возможной угрозы без потери работоспособности ТС. Функционирование пассивного барьера связано только с вызвавшим его работу событием и не зависит от работы другой (активной) системы [4]. Типы барьеров, а также уровень защищённости, которые они обеспечивают, определяются из анализа уязвимых мест (областей) технической системы или её составных частей, а также значения ущерба, связанного с осуществлением угрозы.

При разработке средств защиты от возможной совокупности угроз целесообразно использовать в качестве показателей безопасности ТС вероятностные характеристики опасного события, например, вероятность того, что в течение некоторого времени t техническая система будет находиться в безопасном состоянии $P_Б(t)$, т.е. вероятность отсутствия опасного события. Эта вероятность определяется из выражения

$$P_Б(t) = \prod_{i=1}^{n} \left[1 - \left(1 - P_{З_i}(t)\right) P_{У_i}(t)\right], \qquad (1)$$

где $P_{З_i}(t)$ - вероятность защиты от i-ой угрозы в течение времени t (уровень защищённости);

$P_{У_i}(t)$ - вероятность появления i-ой угрозы в течение времени t;

n - количество угроз безопасному состоянию ТС.

Поскольку уровень защищённости ТС от угрозы зависит от эффективности и надёжности (безотказности) защиты, вероятность $P_{З_i}(t)$ рассчитывается по формуле

$$P_{З_i}(t) = P_{З_i}^{Э} P_{З_i}^{БР}(t), \qquad (2)$$

где $P_{З_i}^{Э}$ - вероятность защиты от i-ой угрозы при условии безотказной работы средства защиты (показатель эффективности защиты);

$P_{З_i}^{БР}(t)$ - вероятность безотказной работы средства защиты от i-ой угрозы.

При использовании восстанавливаемого защитного средства вместо вероятности безотказной работы в соотношении (2) применяется коэффициент готовности.

Наибольшая степень сближения свойств надёжности и безопасности происходит в том случае, когда в виде угрозы выступает отказ критичного элемента, который обусловлен только естественным расходом технического ресурса. Вероятность безопасного состояния ТС, в состав которой включено невосстанавливаемое средство защиты, обеспечивающее перевод ТС в защитное (неработоспособное) состояние при отказе критичного элемента, находится с учётом (1) из выражения

$$P_{Б}(t) = 1 - q_{оо}(t) = 1 - [1 - P_{З}(t)] q_{КР}(t), \qquad (3)$$

где $q_{оо}(t)$ - вероятность опасного отказа ТС;

$q_{КР}(t)$ - вероятность отказа критичного элемента ТС.

Требования по безопасности при этом задаются в виде минимально допустимого значения вероятности $q_{оо}^{\min}(t)$ опасного отказа в течение времени t. Тогда на основании (2) и (3) при известном значении $q_{КР}(t) \neq 0$, которое устанавливается в результате анализа структуры ТС на всех режимах её работы, рассчитывается требуемая вероятность защиты

$$\left[P_{З}(t)\right]_{тр} = 1 - \frac{q_{оо}^{\min}(t)}{q_{КР}(t)} = \left[P_{З}^{Э} P_{З}^{БР}(t)\right]_{тр}. \qquad (4)$$

При условии использования идеального средства защиты, у которого показатель эффективности $P_{З}^{Э} = 1$, требуемое значение вероятности безотказной работы защитного средства ТС, исходя из заданного значения показателя безопасности, находится с помощью соотношения

$$\left[P_{З}^{БР}(t)\right]_{тр} = 1 - \frac{q_{оо}^{\min}(t)}{q_{КР}(t)}, \qquad (5)$$

т.е. свойство безопасности ТС при идеальной (в смысле эффективности функционирования) защите определяется только свойствами надёжности критичных элементов и средства защиты. В действительности, стремление разработчика к высокому уровню эффективности защиты ведёт, как правило, к снижению вероятности безотказной работы разрабатываемого средства. Поэтому в процессе разработки ТС с требованиями по безопасности решается задача поиска оптимальной (по критерию максимума уровня защищённости) структуры средства защиты.

Выводы

Надёжность и безопасность технических систем являются, с одной стороны, самостоятельными свойствами, входящими в понятие «качество», а с другой стороны, достаточно близкими к друг другу. Наибольшая степень сближения этих свойств происходит в том случае, когда в виде угрозы безопасному состоянию ТС выступает отказ критичного элемента, который обусловлен только естественным расходом технического ресурса. Такой отказ при отсутствии соответствующих мер защиты может стать опасным.

Введённые в настоящей статье понятия (опасное и безопасное состояния, опасное событие, угроза безопасности) позволяют использовать для оценивания безопасности ТС такие показатели, которые имеют понятный физический смысл и пригодны для практического решения задач по обоснованию и обеспечению заданных требований по безопасности при разработке потенциально опасных технических систем и средств защиты от возможных угроз. В состав этих показателей могут быть включены: вероятности опасного состояния и его отсутствия, средняя и гамма-процентная наработка до опасного события, интенсивность опасных событий, вероятность защиты от угрозы определённого вида и т.п.

Список использованной литературы

1. Демидович Н.О. Гармонизация терминологии в области надёжности // Методы менеджмента качества, № 10, 2002, С. 43 - 47.

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

3. ГОСТ Р 51898 –2002. Аспекты безопасности. Правила включения в стандарты. – М.: Издательство стандартов, 2002. – 6 с.

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

5. ГОСТ Р 51333 – 99. Безопасность машин. Основные понятия, общие принципы конструирования. Термины, технологические решения и технические условия. - М.: Издательство стандартов, 2000. – 55 с.

6. ГОСТ Р 51344 - 99. Безопасность машин. Принципы оценки и определения риска. - М.: Издательство стандартов, 2000. – 15 с.

7. ГОСТ 27.310 –95. Надёжность в технике. Анализ последствий и критичность отказов. Основные положения. – М.: Издательство стандартов, 2000. – 15 с.

Аннотация

Рассмотрены терминологические аспекты взаимосвязи понятий «надёжность» и «безопасность» технических систем с позиций разработчиков систем управления и средств защиты потенциально опасных объектов. Предложены показатели безопасности, которые имеют понятный физический смысл и позволяют решать практические задачи по обоснованию и обеспечению заданных требований по безопасности технических систем, а также по продлению сроков их эксплуатации.

Библ. 7.

Abstract

Terminological aspects of a relationship between the terms “reliability” and “safety” are considered from a point of view of developers of safety facilities for potential danger objects. Physical content safety characteristics are offered and make it possible to solve practical problems associated with feasibility study and accordance with determined requirements of safety for technical systems and extension of their life.

Bibl. 7