ПРОБЛЕМЫ МАШИНОСТРОЕНИЯ И НАДЕЖНОСТИ МАШИН

№ 6, 2011

ТЕХНОГЕННАЯ БЕЗОПАСНОСТЬ МАШИН И КОНСТРУКЦИЙ

УДК 614.84

© 2011 г. Махутов Н.А., Резников Д.О.

СОПОСТАВИТЕЛЬНАЯ ОЦЕНКА НОРМАТИВНОГО И ОСНОВАННОГО НА УПРАВЛЕНИИ РИСКОМ ПОДХОДОВ К ОЦЕНКЕ ЗАЩИЩЕННОСТИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ[1]

Рассмотрено нормативное обеспечение защищенности сложных технических систем, основанное на назначении запасов по основным механизмам достижения предельных состояний. Представлен расчетный подход к обеспечению защищенности, основанный на управлении риском, и, предполагающий последовательное снижение угроз, которым подвергается техническая система, уязвимости по отношению к действующим угрозам и ущербов при авариях в сложных технических системах.

Защищенность сложных технических систем (СТС), определяется их способностью противостоять возникновению и развитию неблагоприятных ситуаций в штатных и нештатных условиях. Оценку защищенности сложных технических систем и выработку защитных мероприятий приходится осуществлять в условиях высокого уровня неопределенности относительно интенсивности эксплуатационных нагрузок и внешних воздействий на систему, а также несущей способности ответственных элементов СТС на различных этапах цикла эксплуатации. Источниками неопределенностей являются: естественная вариативность параметров системы и внешней среды, ограниченность знаний о связях между элементами СТС, между событиями и процессами, протекающими в сложных технических системах; неточность имеющихся статистических данных и существующих оценок; несовершенство используемого контрольно-измерительного оборудования и математических моделей.

Защищенность СТС можно обеспечивать на основе использования: нормативных подходов к обеспечению защищенности, которые базируются на снижении возможности достижения системой различных предельных состояний за счет реализации технических и организационных мер, обеспечивающих соответствующие запасы по основным механизмам достижения предельных состояний; подходов, основывающихся на управлении риском аварий и катастроф в СТС, и предполагающих выработку комплекса технических и организационных мероприятий, направленных на снижение уровня угроз, которым подвергаются СТС, снижение уязвимости СТС по отношению к угрозам и минимизацию ущербов в случае аварий в СТС.

[1] Работа выполнена при финансовой поддержке РФФИ (Грант № 10-08-00989).

Применение нормативных подходов бывает оправдано в тех случаях, когда имеется значительный опыт строительства и эксплуатации систем данного класса, позволяющий опираться на проверенные на практике нормативные значения параметров системы. В тех случаях, когда строятся уникальные технические системы, или когда эти системы будут эксплуатироваться в регионах, имеющих принципиально иные природно-климатические, экономические и социальные условия, обеспечение защищенности должно базироваться на оценке рисков и выработке мероприятий по их снижению.

Нормативное обеспечение защищенности. Нормативные подходы к обеспечению защищенности СТС предполагают проектирование и эксплуатацию системы таким образом, чтобы обеспечить выполнение условия по обеспечению защищенности по основным механизмам достижения предельных состояний $i = 1, 2, ..., k$ на протяжении всего срока эксплуатации $T_э$

$$\Sigma_i^C(t) - \Sigma_i^э(t) > 0, \quad \forall t \in [0; T_э], \quad \forall i = 1, 2, \ldots, k, \tag{1}$$

где $\Sigma_i^C(t)$ – предельные характеристики прочности, надежности, ресурса и живучести ответственных элементов СТС (далее – характеристики несущей способности): $\Sigma_i^э(t)$ – соответствующие им факторы эксплуатационного нагружения (далее – нагрузки) [1].

В выражении (1) фигурируют неопределенные величины нагрузки и несущей способности.

При реализации нормативного подхода неопределенные величины $\Sigma_i^C(t)$ и $\Sigma_i^э(t)$ в выражении (1), заменяются на детерминированные: расчетную (номинальную) несущую способность и расчетную нагрузку. В качестве расчетных величин можно выбирать некоторые детерминированные характеристики случайных величин нагрузки и несущей способности, например, их математические ожидания $E\{\Sigma_i^C\}$ и $E\{\Sigma_i^э\}$. При этом для учета неопределенности вводятся парциальные запасы по несущей способности $n_i^C(t) > 1$ и нагрузке $n_i^э(t) > 1$. При назначении парциальных запасов учитывается разброс величин нагрузки и несущей способности, уровень неопределенности, присутствующий в задаче и критичность рассматриваемых элементов системы. При этом условие обеспечения защищенности (1), можно записать с помощью детерминированных величин

$$\frac{E\{\Sigma_i^C(t)\}}{n_i^C(t)} - n_i^э(t)E\{\Sigma_i^э(t)\} > 0, \quad \forall t \in [0; T_э], \quad \forall i = 1, 2, \ldots, k.$$

Введем понятия предельно допустимой несущей способности $[\sigma_i^C(t)] = E\{\Sigma_i^C(t)\}/n_i^C(t)$ и предельно допустимой нагрузки $[\sigma_i^э(t)] = n_i^э(t)E\{\Sigma_i^э(t)\}$, а также понятие предельно-допустимого (нормативного) запаса $[n_i(t)] = n_i^э(t)n_i^C(t)$. Тогда условие обеспечения защищенности по i-му предельному состоянию можно записать в виде

$$E\{\Sigma_i^C(t)\} - [n_i(t)]E\{\Sigma_i^э(t)\} > 0, \quad \forall t \in [0; T_э], \quad \forall i = 1, 2, \ldots, k.$$

Введя понятия расчетного дифференциального запаса, равного отношению расчетных значений несущей способности и нагрузки при i-м механизме достижения пре-

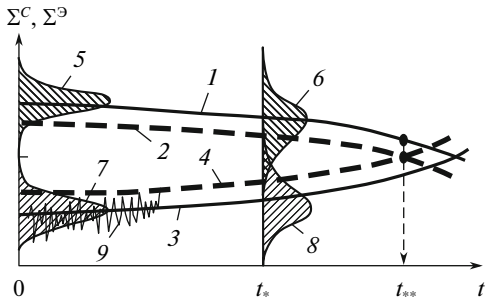

Рис. 1

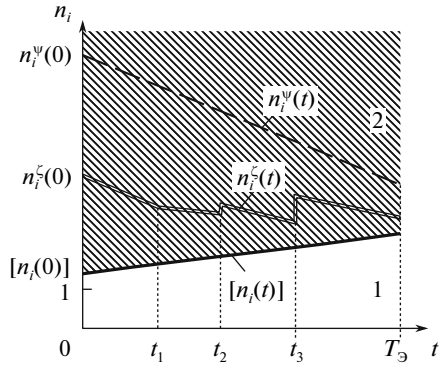

Рис. 2

Рис. 1. Определение точек поверхностей предельных состояний: *1* – математическое ожидание несущей способности $E\{\Sigma_i^C(t)\}$; *2* – предельно допустимая несущая способность $[\sigma_i^C(t)]$; *3* – математическое ожидание нагрузки $E\{\Sigma_i^Э(t)\}$; *4* – предельно допустимая нагрузка $[\sigma_i^Э(t)]$; *5* и *6* – плотности распределения несущей способности при $t = 0$ и $t = t_*$; *7* и *8* – плотности распределения нагрузки при $t = 0$ и $t = t_*$; *9* – реализация случайного процесса нагружения $\Sigma_i^Э(t)$

Рис. 2. Обеспечение защищенности СТС при традиционном нормативном подходе: *1* – область незащищенных состояний, *2* – область защищенных состояний

дельных состояний $n_i(t) = E\{\Sigma_i^C(t)\}/E\{\Sigma_i^Э(t)\}$, можно записать условие обеспечения защищенности системы, выраженное через запасы

$$n_i(t) > [n_i(t)], \quad \forall t \in [0;\ T_Э], \quad \forall i = 1, 2, \ldots, k.$$

Величину расчетного дифференциального запаса n_i в момент времени t можно представить как сумму трех величин $n_i(t) = n_i(0) - \Delta_i(t) + \delta_i^{\zeta}(t)$, где $n_i(0)$ – величина начального запаса, задаваемого при проектировании путем выбора соответствующих технических решений, геометрических и физических параметров системы; $\Delta_i(t)$ – величина, отражающая снижение несущей способности вследствие действия деградационных процессов в технической системе (усталость, коррозия, износ); $\delta_i^{\zeta}(t)$ – величина, характеризующая увеличение несущей способности (и/или снижение уровня эксплуатационных нагрузок) вследствие реализации определенной программы эксплуатации системы $\zeta(a_m, a_o, a_r, a_Z)$, предусматривающей осуществление набора защитных мероприятий (мониторинг a_m, техническое обслуживание a_0, ремонт a_r, создание систем защиты a_Z).

В инженерной практике дифференциальные запасы n_i выбираются на этапе проектирования, при этом задается вектор начальных запасов по прочности, живучести, надежности, ресурсу и др. Очевидно, что комплекс начальных запасов $n_1(0), n_2(0), \ldots, n_k(0)$, обеспеченных на этапе строительства системы, не полностью определяет состояние защищенности системы на различных этапах ее функционирования. Ввиду действия деградационных процессов (усталость, коррозия, износ), а также экстремальных внешних воздействий, ошибок операторов и т.д., несущая способность элементов СТС имеет естественную тенденцию к снижению (рис. 1). Поэтому дифференциальные запасы $n_i(t)$ являются убывающими функциями, которые со временем могут опу-

ститься ниже допустимых уровней $[n_i(t)]$. В связи с этим, в процессе эксплуатации системы предусматривается проведение комплекса специальных защитных мероприятий, включающих: мониторинг технического состояния, техническое обслуживание, ремонтные работы, введение систем защиты, которые в совокупности составляют избранную (на этапе проектирования) программу эксплуатации системы $\zeta(a_m, a_o, a_r, a_z)$, призванную поддерживать требуемое состояние защищенности на протяжении всего жизненного цикла системы. Следует отметить, что начальные запасы $n_i(0)$ по основным механизмам достижения предельных состояний СТС должны назначаться с учетом ожидаемой интенсивности деградационных процессов и во взаимоувязке с принимаемой программой эксплуатации СТС.

Таким образом, защищенность системы может характеризоваться: совокупностью начальных дифференциальных запасов $n_1(0)$, $n_2(0)$, ..., $n_k(0)$, семейством, так называемых, функций деградации $\Delta_1(t)$, $\Delta_2(t)$, ..., $\Delta_k(t)$, отражающих снижение несущей способности вследствие действия деградационных процессов; комплексным параметром "программа эксплуатации системы" $\zeta(a_m, a_o, a_r, a_Z)$, определяющим систему защитных мероприятий, реализуемых в процессе эксплуатации СТС. В такой постановке защищенность системы характеризуется функционалом

$$Z_{\text{Н}}(t) = F_{n,\zeta}\{n_1(0), n_2(0), \ldots, n_k(0), \Delta_1(t), \Delta_2(t), \ldots, \Delta_k(t), \zeta(a_m, a_o, a_r, a_z)\}. \qquad (2)$$

Учитывая функционал (2), можно выделить две стратегии обеспечения защищенности (рис. 2).

Стратегия 1, предусматривающая задание малых начальных запасов $n_i^{\zeta}(0)$ при значительном объеме защитных мероприятий (программа эксплуатации ζ, предусматривающая проведение в моменты времени t_1, t_2 и t_3 – техническое обслуживание, текущий и капитальный ремонт, соответственно).

Стратегия 2, предусматривающая задание значительных начальных запасов $n_i^{\psi}(0)$ по основным механизмам достижения предельных состояний при минимальном объеме защитных мероприятий (программа эксплуатации ψ).

Первая стратегия применяется для тех элементов СТС, которые легко контролировать в процессе эксплуатации и, которые могут быть отремонтированы или заменены без остановки системы. Вторую стратегию целесообразно использовать для систем (или их элементов), доступ к которым в процессе эксплуатации затруднен и, которые не могут быть отремонтированы без значительных материальных или временных издержек.

Нормативный критерий обеспечения защищенности при программе эксплуатации ζ можно записать в виде

$$n_i^{\zeta}(t) > [n_i(t)], \quad \forall t \in [0;\, T_{\text{Э}}], \quad \forall i = 1, 2, \ldots, k.$$

Тогда можно ввести нормативный показатель защищенности

$$Z_{\text{Н}} = \begin{cases} 1, & \text{если} \quad n_i^{\zeta}(t) > [n_i(t)], \quad \forall t \in [0;\, T_{\text{Э}}], \quad \forall i = 1, 2, \ldots, k, \\ 0, & \text{если} \quad \exists (t_* \in [0;\, T_{\text{Э}}] \wedge j \in \{1, 2, \ldots, k\}) \left| n_j^{\zeta}(t_*) < [n_j(t_*)]. \right. \end{cases}$$

Обеспечение защищенности СТС, основанное на управлении интегральным риском. Обеспечение защищенности путем управления риском является новым подходом, базирующимся на результатах фундаментальных и прикладных исследований последних трех десятилетий по проблемам безопасности природно-техногенно-социальной сферы, выполненных специалистами в области физики, химии и механики катастроф. В рамках этих исследований были разработаны научные основы изучения механизмов

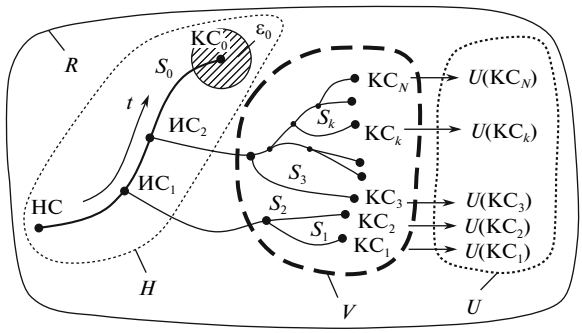

Рис. 3. Структура анализа риска и защищенности СТС: R – анализ риска, H – анализ угроз, V – анализ уязвимости, U – калькуляция ущербов

достижения предельных состояний, источников возникновения и сценариев развития аварийных ситуаций в СТС [4].

В качестве интегрального показателя защищенности вводится риск-индекс защищенности СТС, представляющий собой отношение установленного законодательно максимально допустимого значения интегрального риска для рассматриваемой системы $[R]$ к текущему значению интегрального риска R: $Z_R = [R]/R$.

Использование критерия риска для оценки состояния защищенности рассматриваемой системы является новой постановкой проблемы, при которой обеспечение защищенности СТС достигается путем реализации комплекса мероприятий, направленных на снижение интегрального риска R.

Основанный на управлении риском подход к обеспечению защищенности СТС предусматривает применение системного анализа, позволяющего учесть весь спектр угроз природного, техногенного и террористического характера, инженерные, экономические, социальные факторы, общечеловеческие ценности и имеющего в виду не только ближайшие, но и отдаленные последствия решений, принимаемых в условиях ограниченности всех видов ресурсов. Это возможно только на путях создания математических моделей СТС и математического исследования динамики их состояния, поиска таких вариантов (сценариев) их развития, которые соответствуют в любой момент времени целям и критериям обеспечения заданного уровня их защищенности $Z(t)$.

Общий контекст анализа риска и защищенности для сложных технических систем предполагает последовательный анализ угроз, которым подвергается система, анализ уязвимостей системы по отношению к выявленным угрозам и анализ ущербов от аварий, реализующихся в тех случаях, когда система оказалась уязвимой к действующим на нее угрозам (рис. 3).

Под угрозами для СТС понимаются эксплуатационные нагрузки, отказы элементов, внешние экстремальные (проектные и запроектные) воздействия, ошибки операторов, несанкционированные воздействия [5]. В зависимости от уровня неопределенности относительно угроз для СТС и возможных механизмов достижения предельных состояний элементов СТС, угрозы, действующие на СТС, рассматриваются: как случайные величины, характеризующиеся вероятностью реализации опасного события определенной интенсивности; вероятностные распределения (кривые угроз), определяющие плотность распределения вероятности реализации опасных событий по интенсивности; случайные процессы, позволяющие описывать историю эксплуатационного нагружения и экстремальных воздействий на систему.

Уязвимость системы характеризуется совокупностью сценариев случайных событий (отказов в системе) и причинно-следственных связей между этими событиями, т.е. структурой сценарного графа системы [6]. При этом параметрами уязвимости системы будут являться условные вероятности реализации различных конечных состояний

системы, возникающих в случае эскалации аварии, развивающейся в системе после инициирующего события различного типа и интенсивности. Анализ уязвимостей предполагает исследование последовательностей событий и причинно-следственных связей между событиями, происходящими вслед за инициирующим событием вплоть до достижения системой конечных состояний. Иными словами, анализ уязвимости системы заключается в проведении качественного и количественного исследования структуры сценариев эскалации аварии. Таким образом, анализ уязвимости предполагает детальное изучение дерева сценариев рассматриваемой системы.

Траектория в пространстве состояний, описывающая эволюцию системы от исходного состояния НС до требуемого конечного состояния $КС_0$, будет называться сценарием успеха S_0 (рис. 3). В моменты времени t_1, t_2, ..., t_k в системе могут произойти инициирующие события ($ИС_i$), которые способны отклонить траекторию сценария S_0, запуская последовательность событий соответствующих сценариям отказов S_1, S_2, ..., S_N, которые будут приводить к достижению системой соответствующих конечных состояний $КС_1$, $КС_2$, ..., $КС_N$. Тогда уязвимость системы можно описать с помощью матрицы, компоненты которой $V_{i,j}$ будут представлять собой условные вероятности достижения системой конечного состояния $КС_i$ при условии, что произошло инициирующее событие $ИС_j$: $V_{i,j} = P[КС_i|ИС_j]$.

Реализация определенного сценария аварии S_i приводит к достижению системой соответствующего поврежденного конечного состояния $КС_i$, сопряженного с ущербом $U(КС_i)$ [9]. Таким образом, ущерб от аварии на СТС – это результат изменения состояния системы, выражающийся в нарушении ее целостности или ухудшении других свойств; фактические или возможные экономические и социальные потери, возникающие в результате каких-то событий, явлений, действий; полная или частичная потеря здоровья либо смерть человека, утрата имущества или других материальных, культурных, исторических или природных ценностей [8].

Проведя последовательно оценку угроз, уязвимости и ущербов для СТС, можно оценить индекс риска для рассматриваемой системы $R = \mathbf{H} \cdot \mathbf{V} \cdot \mathbf{U}^T$, где $\mathbf{H} = \{P(ИС_1); P(ИС_2); ...; P(ИС_m)\}$ – вектор угроз, компонентами которого являются вероятности реализации инициирующих событий $ИС_1$, $ИС_2$, ..., $ИС_m$; $\mathbf{V} = [P(КС_i|ИС_j]$ – матрица уязвимости, элементы которой представляют собой вероятности реализации возможных поврежденных состояний $КС_i$ при условии оказания на систему различных экстремальных воздействий $ИС_j$; $\mathbf{U} = \{U(КС_1), U(КС_2), ..., U(КС_N)\}^T$ – вектор ущербов, компонентами которого являются величины полных ущербов, соответствующих конечным состояниям $КС_1$, $КС_2$, ..., $КС_N$.

Сопоставление нормативного подхода к оценке защищенности и подхода, основанного на управлении риском. Нормативный подход предполагает оценку избранного проектного решения, определяемого совокупностью (а) начальных запасов $\{n_i(0)\}$ по прочности, жесткости, ресурсу, надежности, живучести и (б) выбранной программой эксплуатации системы ζ, с последующим сопоставлением этих запасов в различные моменты времени в течение периода эксплуатации системы $[0; T_Э]$ с допустимыми значениями запасов $[n_i]$, при которых защищенность системы по отношению к различным механизмам достижения предельных состояний считается обеспеченной.

При этом вводится нормативный индекс защищенности $Z_Н$, который полагается равным единице при соблюдении условия обеспечения защищенности, и равным нулю в случае несоблюдения этого условия

$$Z_Н = \begin{cases} 1, & \text{если} \quad n_i^{\zeta}(t) > [n_i], \quad \forall t \in [0; T_Э], \quad \forall i = 1, 2, \ldots, k, \\ 0, & \text{если} \quad \exists (t_* \in [0; T_Э] \wedge i \in \{1, 2, \ldots, k\}) \big| n_i^{\zeta}(t_*) < [n_i]. \end{cases}$$

Если условие обеспечения защищенности не выполняется, то выбирают новые параметры системы или новую программу эксплуатации, после чего вновь оцениваются запасы по различным механизмам достижения предельных состояний и выясняют, соблюдается ли условие обеспечения защищенности для модифицированной системы. Эта процедура повторяется до тех пор, пока условие не будет выполнено.

Основанный на управлении риском подход к обеспечению защищенности предполагает оценку интегрального риска R, связанного с эксплуатацией СТС и сопоставление полученного значения с предельно допустимым значением риска $[R]$. При этом вводится расчетный индекс защищенности, равный отношению предельно допустимого риска СТС к расчетному значению интегрального риска $Z_R = [R]/R$.

Полученное значение сравнивают с допустимым расчетным индексом защищенности $[Z_R]$. При этом система считается защищенной, если выполняется условие $Z_R > [Z_R]$. В случае невыполнения этого условия параметры системы меняются, выполняется новый расчет риска и проводится оценка защищенности для модифицированной системы.

Представленный нормативный и расчетный подход формируют традиционное направление действий по обеспечению защищенности СТС.

Новое направление обеспечения защищенности СТС предполагает решение обратной задачи. При этом изначально задается уровень защищенности $Z(t)$. Этот уровень определяет все основные группы требований: по ресурсу $R_N(t)$, надежности $P_{PR}(t)$, живучести $L_d(t)$, прочности $R_\sigma(t)$, жесткости $R_\delta(t)$, устойчивости $R_\lambda(t)$ (в случае нормативного подхода) или по интегральному риску R (в случае расчетного подхода). Далее подбираются параметры системы и программа эксплуатации, отвечающие заданным требованиям.

СПИСОК ЛИТЕРАТУРЫ

1. *Махутов Н.А.* Прочность и безопасность. Фундаментальные и прикладные исследования. Новосибирск: Наука, 2008. 523 с.
2. *Доронин С.В., Лепихин А.М., Москвичев В.В. и др.* Моделирование прочности и разрушения несущих конструкций технических систем. Новосибирск: Наука, 2005. 247 с.
3. *Elishakoff I.* Safety Factors and Reliability: Friends or Foes? Kluwer Academic Publishers. Dordrecht, 2004. 294 p.
4. *Махутов Н.А., Петров В.П., Ахметханов Р.С. и др.* Безопасность России. Анализ риска и проблемы безопасности. Ч. 2. Безопасность гражданского и оборонного комплексов и управление рисков. М.: МГФ “Знание”, 2006. 434 с.
5. *Махутов Н.А., Петров В.П., Резников Д.О. и др.* Идентификация определяющих параметров угроз, уязвимости и защищенности критически важных объектов по отношению к превалирующим угрозам природного, техногенного и террористического характера // Проблемы безопасности и чрезвычайных ситуаций. М.: ВИНИТИ, 2008. № 2. С. 34–41.
6. *Махутов Н.А., Резников Д.О.* Оценка уязвимости технических систем и ее место в процедуре анализа риска // Проблемы анализа риска. 2008. Т. 5. № 3. С. 76–89.
8. *Шойгу С.К., Владимиров В.А., Воробьев Ю.Л. и др.* Безопасность России. Защита населения и территорий от чрезвычайных ситуаций природного и техногенного характера. М.: МГФ “Знание”, 1999. 594 с.

Москва Поступила в редакцию 18.V.2011