

## ОЦЕНКА ЖИВУЧЕСТИ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

чл.-корр. РАН Н.А.Махутов, к.т.н. Д.О. Резников.  
Институт машиноведения РАН

В статье представлены основные подходы к проведению количественной оценки живучести сложных технических систем, в том числе, основанные на оценке соотношений прямых и косвенных рисков, соотношении вероятности катастрофических отказов для поврежденной и неповрежденной системы и энергетических критерий эскалации катастрофических сценариев. Представлен пример оценки живучести технической системы. Обоснована необходимость повышения живучести для обеспечения безопасности сложных технических систем при запроектных воздействиях.

**Ключевые слова:** живучесть, уязвимость, риск, безопасность.

### 1. Введение

Под живучестью сложной технической системы принято понимать способность системы выполнять предписанные ей функции после повреждения (или разрушения) ее отдельных элементов<sup>1</sup>.

Традиционные методы проектирования сложных технических систем (далее СТС) предполагают расчет реакции элементов систем на проектные воздействия, которые определяются, исходя из нормальных условий эксплуатации. Кроме того, проводятся также расчеты надежности СТС, т.е. вероятности их безотказной работы и выполнения возложенных на них функций при проектных воздействиях [1]. Однако в процессе эксплуатации СТС могут быть подвергнуты экстремальным (запроектным) воздействиям, в результате которых ряд их элементов будут получать повреждения. В этих условиях эксплуатационные качества сложных технических систем будут определяться их способностью выполнять предписанные им функции, после того как отдельные элементы этих систем выйдут из строя.

Таким образом, понятие живучести системы является центральным при рассмотрении ее поведения после запроектных воздействий. Системы, обладающие большой живучестью, разрушаются постепенно, сохраняя при этом ограниченную работоспособность. Это позволяет оператору системы принять защитные меры (провести ремонт, замену поврежденных элементов, перейти в безопасный режим эксплуатации, выполнить аварийный останов системы и т.д.), тем самым, сводя последствия аварии главным образом к первичным ущербам от повреждения элементов системы. Системы с малой живучестью разрушаются резко и катастрофически, что сопровождается значительными вторичными и каскадными разрушениями, которые являются несоизмеримыми (непропорциональными) инициирующим воздействиям.

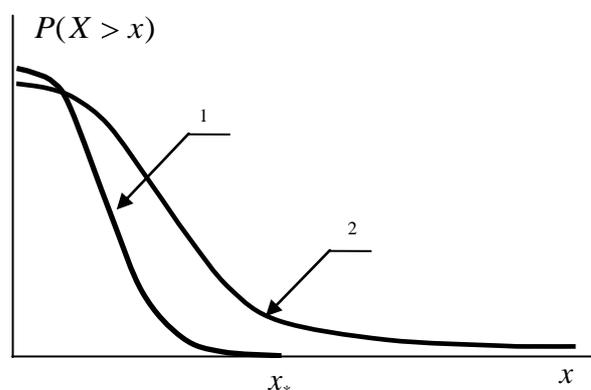


Рис.1 Распределения ущербов в системах с высокой и низкой живучестью

<sup>1</sup> Здесь под повреждением системы понимается отказ отдельных элементов, возникновение трещин, коррозии и т.д.

Важным различием между системами с низкой и высокой живучестью является вид кривых распределения ущерба. На рис. 1 (кривая 1) представлено распределение ущербов для системы с высокой живучестью. Это распределение является компактным и определяется прямыми ущербами от локальных повреждений системы. Кривая 2 – соответствует системе с низкой живучестью. Здесь приходится иметь дело с распределением «с тяжелым хвостом», которое обуславливается значительными вторичными ущербами от эскалации аварии системы и косвенными ущербами от невыполнения системой предписанных ей функций [2].

При проектировании СТС необходимо учитывать возможность экстремальных/запроектных воздействий и принимать конструктивные решения, направленные на повышение их живучести, чтобы избежать катастрофических разрушений системы.

## 2. Роль обеспечения живучести в системе мер по снижению риска

Повышение живучести сложных технических систем является важным направлением усилий по снижению риска. Оно направлено на снижение риска  $R^e$  сценариев катастрофических разрушений системы, приходящихся на хвостовые области распределения ущербов.

Необходимость оценки живучести СТС объясняется тем, что как бы тщательно ни проводились расчеты при проектировании системы, в силу ее сложности, всегда будут непредусмотренные заранее воздействия, обусловленные запроектными/экстремальными нагрузками на элементы системы, ошибками операторов, сложными взаимодействиями элементов системы, которые будут приводить к локальным повреждениям системы. Но при этом важно, насколько вероятно, что указанные локальные повреждения вызовут катастрофическое разрушение системы в целом.

Следует иметь в виду, что даже в системах с высокой избыточностью вследствие наличия положительных обратных связей возможны катастрофические сценарии, при которых могут одновременно выводиться из строя основные и резервные связи (пути передачи нагрузки, каналы управления, линии передачи энергии и т.д.).

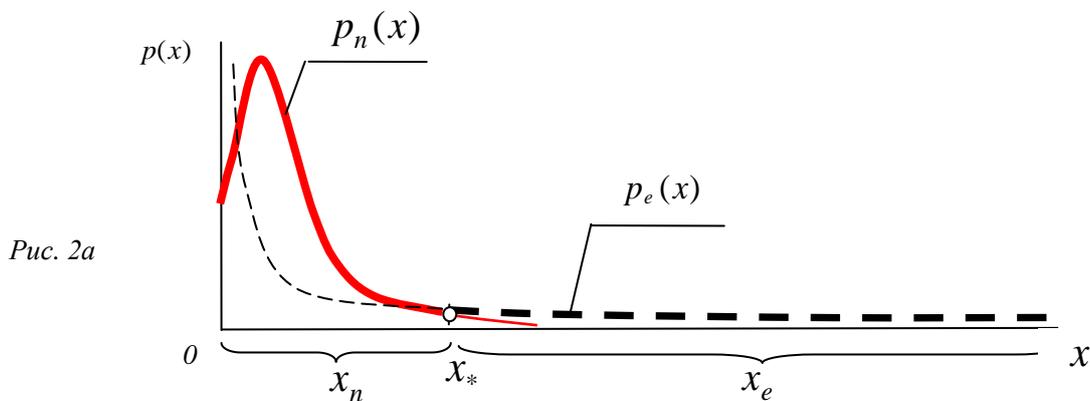


Рис. 2а

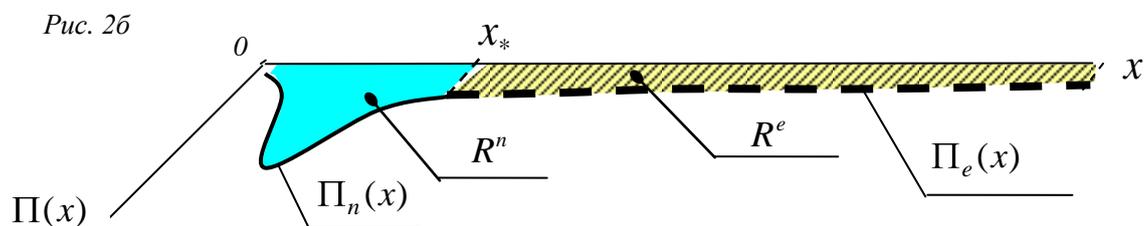


Рис. 2б

Рис. 2а – Распределение ущербов: область  $0 < x < x_*$  - центральная часть распределения ущербов;  $x > x_*$  - хвостовая область распределения ущербов.

Рис. 2б. – Вид функций  $\Pi_n(x)$  и  $\Pi_e(x)$  для систем с малой живучестью

Величина риска аварии определяется выражением  $R = \int_0^{x_*} p_n(x)xdx + \int_{x_*}^{\infty} p_e(x)xdx$ . Где  $p_n(x)$  и  $p_e(x)$  - функции плотности распределения ущерба соответственно центральной и хвостовой части распределения. Обозначив подынтегральные функции в интегралах риска  $\Pi_n(x) \hat{=} p_n(x) \cdot x$  и  $\Pi_e(x) \hat{=} p_e(x) \cdot x$ , можно записать  $R = \int_0^{x_*} \Pi_n(x)dx + \int_{x_*}^{\infty} \Pi_e(x)dx$

Статистика аварий СТС свидетельствует [2, 3], что для сценариев  $S_{n_j}$ , находящихся в центральной части распределений, характерны нормальные законы распределения ущербов вида:

$p_n(x) \sim e^{-\frac{(x-m)^2}{2\sigma^2}}$  для  $x < x_*$ . А для катастрофических/запроектных/каскадных сценариев  $S_{e_j}$  - отмечаются степенные законы  $p_e(x) \sim x^{-(1+\alpha)}$  для  $x > x_*$ , где  $x_*$  - пороговое значение ущерба, определяемое спецификой рассматриваемой задачи,  $\alpha$  - показатель степени, для большинства СТС лежащий в диапазоне [0; 1].

Пусть  $\alpha = 0.5$ , тогда  $\Pi_e(x) = p_e(x) \cdot x \sim x^{-0.5}$ . То есть для таких систем отмечается слабое убывание подынтегральной функции  $\Pi_e(x)$  при  $x > x_*$  (рис. 2б). Поэтому, несмотря на то, что экстремальные/запроектные сценарии реализуются значительно реже, чем нормальные/проектные, интегральный риск экстремальных сценариев ущербов  $R^e$  будет значительно превышать интегральный риск нормальных сценариев  $R^n$ :

$$R^e \gg R^n$$

$$\text{где } R^n = \int_0^{x_*} \Pi_n(x) dx \quad \text{и} \quad R^e = \int_{x_*}^{x_{\infty}} \Pi_e(x) dx$$

Центральная часть распределения ущербов формируется за счет сценариев, определяющихся локальной уязвимостью системы (т.е. прямыми/первичными ущербами, возникающими при повреждении отдельных элементов системы). При этих сценариях катастрофического разрушения системы не наступает и запаса живучести системы хватает на то, чтобы она сохранила ограниченную работоспособность после нанесения ей локальных повреждений.

Хвостовая часть распределения, напротив, формируется сценариями, для которых помимо первичных характерны значительные вторичные/каскадные и косвенные ущербы, возникающие при отказах системы в целом. Эти сценарии возникают вследствие экстремальных/запроектных воздействий на систему и характеризуются тем, что запаса живучести СТС оказывается недостаточно, чтобы сопротивляться катастрофическому разрушению после нанесения системе локальных повреждений.

В связи с тем, что риски экстремальных ущербов при авариях в СТС обусловлены недостатком их живучести, то учитывая (1) можно сделать вывод, что обеспечение безопасности СТС невозможно без повышения их живучести.

### 3. Количественная оценка живучести

Изменения, происходящие в технической системе, призванной обеспечить получение определенного результата (или реализацию заданного технологического процесса), могут быть представлены в виде траектории в пространстве состояния системы  $\Omega$ , определяющей переход от начального состояния системы  $HC$  в ее конечное состояние  $KC_0$  (рис.3а). В случаях, когда удастся обеспечить подобный переход, говорят, что в системе реализован заданный сценарий (или «сценарий успеха»)  $S_0$ . Конечное состояние  $KC_0$  определяет набор значений  $x_0^1, x_0^2, \dots, x_0^m$ , которые должны принимать переменные состояния системы  $x^1, x^2, \dots, x^m$ , чтобы система соответствовала предъявляемым к ней требованиям [4]. К этим требованиям могут, например, относиться: структурная целостность системы, неповрежденность ее элементов, выполнение системой заданных функций, обеспечение заданной производительности и качества (продукции или услуг) и т.д. Перечисленные

переменные состояния системы определяют размерность и конфигурацию пространства состояний системы.

В ситуациях, когда система подвергается экстремальным воздействиям, ей наносится локальное повреждение  $D_i$ , в результате чего она может отклониться от заданного сценария  $S_0$  (рис.3б) и перейти к реализации некоторого нового сценария  $S_*$ , заканчивающегося конечным состоянием  $KC_*$ , отличным от заданного конечного состояния  $KC_0$ :

$$KC_*(x_*^1, x_*^2, \dots, x_*^m) \neq KC_0(x_0^1, x_0^2, \dots, x_0^m)$$

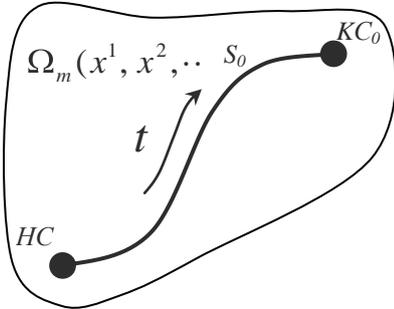


Рис.3а Сценарий успеха  $S_0$

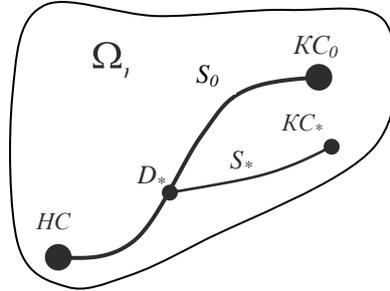


Рис. 3б. Сценарий отказа  $S_*$

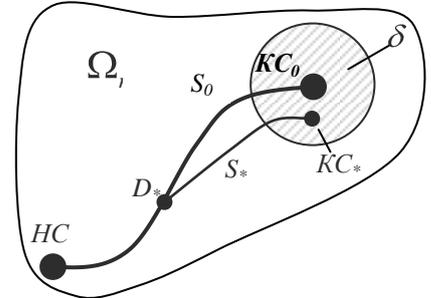


Рис. 3в. Область допустимых состояний  $\delta$

В этом случае можно сказать, что в системе произошел отказ, связанный с ее неспособностью обеспечить требуемое конечное состояние  $KC_0$ . То есть система не продемонстрировала достаточной живучести, чтобы противостоять экстремальному воздействию.

В настоящее время отсутствует единый подход к проведению количественной оценки живучести технических систем. Ниже будет представлен ряд возможных способов решения поставленной задачи.

Экстремальные (запроектные) воздействия, которые наносят системе локальные повреждения, могут иметь различную природу. При этом анализ живучести не должен зависеть от инициирующих событий. Поэтому разрабатываемые подходы к оценке живучести технических систем (1) не должны зависеть от вида экстремального воздействия (угрозы) и (2) должны быть применимы к широкому классу технических систем.

Вследствие высокого уровня неопределенности, связанной с типом и интенсивностью возможных экстремальных воздействий и вызываемых ими повреждений, а также способностью системы «сопротивляться» повреждениям, мера живучести должна быть вероятностной, то есть определяться вероятностью сохранения системой заданных функциональных свойств  $\varphi$ :  $G = f(P[\varphi])^2$ . В связи с тем, что свойства, характеризующие живучесть системы, начинают проявляться только после того, как она получила локальные повреждения, то мера живучести должна определяться условной вероятностью сохранения работоспособности, при условии, что система получила локальное повреждение  $D$ :  $G = f(P[\varphi | D])$ .

Очевидно, что на практике невозможно бывает обеспечить абсолютно точное достижение системой заданного конечного состояния  $KC_0$ . Рано или поздно в процессе эксплуатации реальная система будет подвергаться запроектным воздействиям, приводящим к повреждению ее элементов, что будет выражаться в отклонении ее траектории от заданного сценария успеха  $S_0$ . Поэтому при оценке живучести речь должна идти о вероятности сохранения конечного состояния системы внутри заданной допустимой области  $\delta$  пространства состояний  $\Omega_m$ , которое далее будет называться областью допустимых/безопасных состояний. В частности, на рис. 3в представлено повреждение  $D_*$ , которое приводит к конечному состоянию  $KC_*$ , лежащему в пределах заданной области  $\delta$ . При этом можно считать, что система проявляет достаточную живучесть.

<sup>2</sup> Здесь и далее под отказом будет пониматься получение системой определенной степени повреждения или невыполнение системой (полностью или частично) заданных функций.

Далее под отказом системы будет пониматься выход конечного состояния системы из заранее заданной области  $\delta$  пространства состояний системы  $\Omega_m$ , вне которой система либо перестает существовать, либо не обеспечивает выполнение заданных функций или качества продукции (услуг и т.д.).

Тогда может быть сформулировано следующее определение понятия «живучесть»:

*Под живучестью системы понимается условная вероятность невыхода конечного состояния системы  $KC_*$  за границы заданной области допустимых (безопасных) состояний  $\delta$  пространства  $\Omega_m$ , в случае, локального повреждения системы:*

$$G = P[\|KC_* - KC_0\| < \delta \mid D] \quad (1)$$

В работе [4] было также введено понятие структурной уязвимости системы  $V_S$ , под которой понималась условная вероятность отказа т.е. выхода конечного состояния системы из заданной безопасной области  $\delta$  в случае ее локального повреждения  $D$ .

$$V_S = P[\|KC_* - KC_0\| > \delta \mid D] \quad (2)$$

Поскольку события, связанные с «выходом» и «невыходом» конечного состояния из области  $\delta$  образуют полную группу событий, то справедливо:

$$G = 1 - V_S \quad (3)$$

Вопрос о выборе метрики в пространстве состояний системы также был подробно рассмотрен в работах [4,5].

Можно предложить ряд уточнений для выражения (1). Учитывая множественность возможных локальных повреждений  $D_j$ , и поврежденных конечных состояний  $KC_i^{D_j}$  живучесть системы определяется минимальной условной вероятностью невыхода системы из области допустимых состояний при различных повреждениях:

$$G = \min_{i,j} P[\|KC_i^{D_j} - KC_0\| < \delta \mid D_j] \quad (4)$$

Тогда живучесть СТС будет оцениваться как вероятность того, что после нанесения системе локального повреждения  $D_j$ , она сохранит свою функциональность, т.е. не придет в состояние отказа, или, иначе говоря, она придет в конечное состояние, находящееся в допустимой области  $\delta$ .

В более общей постановке следует учитывать, что в результате экстремального воздействия системе может быть одновременно нанесено более одного, например,  $l$  локальных повреждений:  $\underbrace{D_m, D_n, \dots, D_k}_l$ . Тогда живучесть системы может быть оценена с помощью выражения:

$$G = \min_{\substack{m,n,\dots,k,j \\ l}} P[\|KC_j^{D_m, D_n, \dots, D_k} - KC_0\| < \delta \mid (D_m, D_n, \dots, D_k)] \quad (5)$$

Далее для краткости событие, связанное с нахождением конечного состояния системы внутри области допустимых состояний  $\delta$ , будет обозначено с помощью символа  $\bar{F}$ , а событие «выход из области  $\delta$ » (т.е. отказ системы) будет обозначен символом  $F$ .

Тогда выражения (1) и (2) примут вид:

$$G = P[\bar{F} \mid D] \quad (6)$$

$$V_S = P[F \mid D] \quad (7)$$

*Оценка живучести системы в случае множественных сценариев отказов*

Следует отметить, что в сложной технической системе могут быть реализованы различные сценарии отказов, развивающиеся после различных экстремальных воздействий, и, приводящие к различным конечным состояниям системы. В этом случае живучесть системы наиболее полно характеризуется структурой дерева сценариев отказов. Точнее говоря той частью сценарного графа, которая расположена после локальных повреждений (рис. 4).

Иначе говоря, живучесть системы характеризуется совокупностью сценариев случайных событий (отказов в системе) и причинно-следственных связей между этими событиями. Живучесть



$$G_L = \min_i \frac{L_{F|D_i}}{L_{F|\bar{D}}} \quad (10)$$

3) Индекс живучести может вводиться на основе соотношения показателей надежности неповрежденной и поврежденной системы. Для этого последовательно рассматривается функция предельных состояний для неповрежденной и поврежденной системы. Пусть функция предельных состояний определяется соотношением несущей способности  $R$  и нагрузки  $L$ :  $g_{\bar{D}}(\mathbf{x}) = r - l$ , где  $\mathbf{x}$  - вектор случайных переменных системы, описывающих предельное состояние (параметры, характеризующие несущую способность и нагрузки). Здесь  $r$  и  $l$  - реализации случайных величин  $R$  и  $L$  соответственно.

Рассмотрим величину запаса несущей способности  $M_{\bar{D}} = g_{\bar{D}}(\mathbf{X}) = R_{\bar{D}} - L$ , равную превышению несущей способности над нагрузкой. Поскольку  $r$  и  $l$  являются случайными величинами, то  $M$  также является случайной величиной, имеющей математическое ожидание  $\mu_M$  и дисперсию  $\sigma_M$ . Их можно вычислить по математическим ожиданиям  $\mu_R, \mu_L$  и дисперсиям  $\sigma_R, \sigma_L$  величин  $R$  и  $L$ :

$$\mu_M = \mu_R - \mu_L$$

$$\sigma_M = \sqrt{\sigma_R^2 + \sigma_L^2 - 2\rho_{RL}\sigma_R\sigma_L}$$

где  $\rho_{RL}$  - коэффициент корреляции.

Далее подсчитывается показатель надежности неповрежденной системы  $\beta_{\bar{D}} = \mu_M / \sigma_M$ ,

Аналогичным образом может быть получен условный показатель надежности  $\beta_D$  для системы, получившей локальное повреждение  $D$ . Для этого строится функция предельных состояний поврежденной системы  $g_D(\mathbf{X}) = R_D - L$  и определяется запас несущей способности  $M_D$  для поврежденной системы (здесь  $R_D$  - несущая способность поврежденной системы после перераспределения нагрузок в результате локального повреждения  $D$ ). Затем подсчитываются математическое ожидание  $\mu_{M_D}$  и среднее квадратичное отклонение  $\sigma_{M_D}$  запаса. После чего может быть подсчитан показатель надежности  $\beta_D$  для поврежденной системы  $\beta_D = \mu_{M_D} / \sigma_{M_D}$ .

Тогда индекс живучести по показателю надежности определяется соотношением:

$$G_\beta = \frac{\beta_D}{\beta_{\bar{D}}} \quad (11)$$

Величина  $G_\beta$  варьируется в пределах от 0 до 1, причем, для живучих систем  $G_\beta \rightarrow 1$ .

4) Индекс живучести, основанный на соотношении рисков прямых и косвенных ущербов, который будет рассмотрен в п.4.

5) Энергетический индекс живучести системы, который будет рассмотрен в п.5.

6) Индекс живучести сетевых систем (см. п.6)

#### 4. Индекс живучести, основанный на соотношении рисков прямых и косвенных ущербов

Наиболее полно многовариантность сценариев отказа и поврежденных состояний системы может быть учтена с помощью индекса живучести, базирующегося на риске. При этом должны быть разграничены:

(а) первичные/прямые ущербы  $U_{пр}$  и риски  $R_{пр}$ , которые непосредственно связаны с локальными повреждениями элементов системы в результате экстремальных иницирующих воздействий;

(б) вторичные/каскадные/косвенные/ ущербы  $U_{кос}$  и риски  $R_{кос}$ , которые возникают в результате эскалации аварии и обусловлены отказом системы в целом.

Тогда индекс живучести может быть сформирован в виде [8, 9]:

$$G_R = \frac{\sum_{i=1}^m R_{np_i}}{\sum_{i=1}^m R_{np_i} + \sum_{j=1}^n R_{koc_j}} \quad (12)$$

где  $m$  - количество сценариев, в которых имеют место прямые ущербы и риски, обусловленные локальными повреждениями системы (т.е. общее количество сценариев),  $n$  - количество сценариев, в которых имеют место косвенные ущербы и риски, связанные с отказами системы в целом.

Эта величина также варьируется в интервале от 0 до 1. Система является живучей, в тех случаях, когда косвенные риски не вносят существенный вклад в общесистемный риск  $R_S = R_{np} + R_{koc}$ . Иначе говоря, для живучих систем ( $G_R \rightarrow 1$ ) - прямые риски значительно превышают косвенные ( $R_{np} \gg R_{koc}$ ). Напротив, у системы с низкой живучестью ( $G_R \rightarrow 0$ ) прямые ущербы и риски малы по сравнению с косвенными ( $R_{np} \ll R_{koc}$ ).

Таким образом, представленный индекс характеризует живучесть технических систем как их способность снижать риск непропорционального/катастрофического разрушения (отказа системы) в случае ее локального повреждения.

### Примеры оценки живучести технических систем

На рис. 5 представлено простейшее сценарное дерево, исходящее из начального состояния  $HC$ . Далее система подвергается экстремальному воздействию ( $H$ ), после которого она может, либо остаться неповрежденной (ветвь  $\bar{D}$ ) и придти к заданному конечному состоянию  $KC_0$  с нулевыми ущербами и рисками, либо получить локальное повреждение (ветвь  $D$ ). Во втором случае возможны два варианта:

- (1) система может сохранить работоспособность (ветвь  $\bar{F}$ ), оставаясь в допустимой области. Этому конечному состоянию  $KC_D^{\bar{F}}$  будут соответствовать лишь прямые ущербы и риски, связанные с локальным повреждением элемента системы;
- (2) система придет в состояние отказа  $KC_D^F$ . При этом будут иметь место как прямые ущербы и риски, обусловленные локальным повреждением системы, так и косвенные, связанные с невыполнением системой заданных функций.

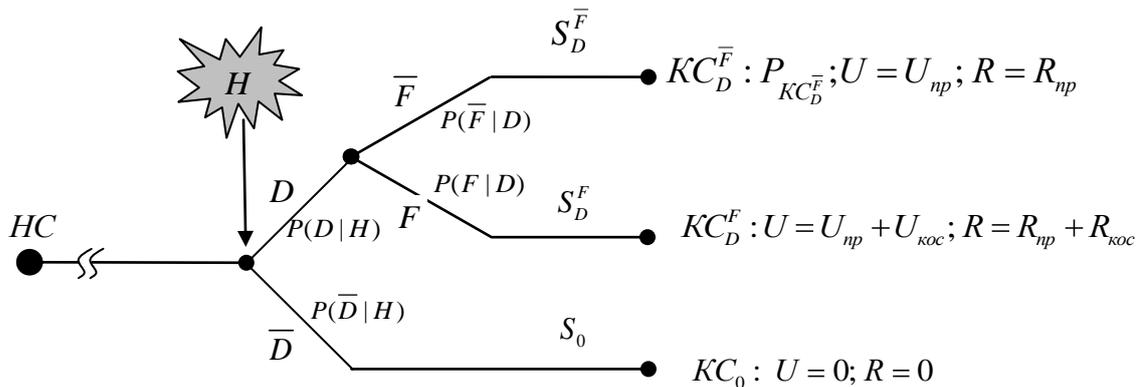


Рис. 5. Сценарное дерево для проведения количественной оценки живучести системы

Под угрозой  $H$  здесь понимается опасное событие (экстремальные нагрузки, ошибка оператора или деградация свойств материала), способное привести к повреждению локальному повреждению  $D$  системы. В результате повреждения элемента системы может произойти отказ  $F$  самой системы. Отказ системы - неспособность системы выполнять заданные функции. Возникающие в процессе эскалации аварии ущербы разделяют на прямые  $U_{np}$  и косвенные  $U_{koc}$ . Прямой ущерб связан с непосредственным повреждением элементов системы. Косвенный ущерб определяется ущербами для системы, возникающими в процессе эскалации аварии, и издержками, вытекающими из невыполнения системой возложенных на нее функций.

Основываясь на дереве событий, представленном на рис.5, можно подсчитать риск, связанный с реализацией сценариев  $S_D^{\bar{F}}$  и  $S_D^F$ . (очевидно, что при сценарии  $S_0$  риск равен нулю) [8]. Это может быть сделано путем умножения вероятности реализации сценария на значение ожидаемого ущерба и последующего интегрирования по всем случайным переменным, фигурирующим в модели (дереве событий). Риск, связанный с реализацией двух опасных сценариев может быть подсчитан как:

$$R_{np} = \int_x \int_y U_{np} f_{D|H}(y|x) f_H(x) dy dx$$

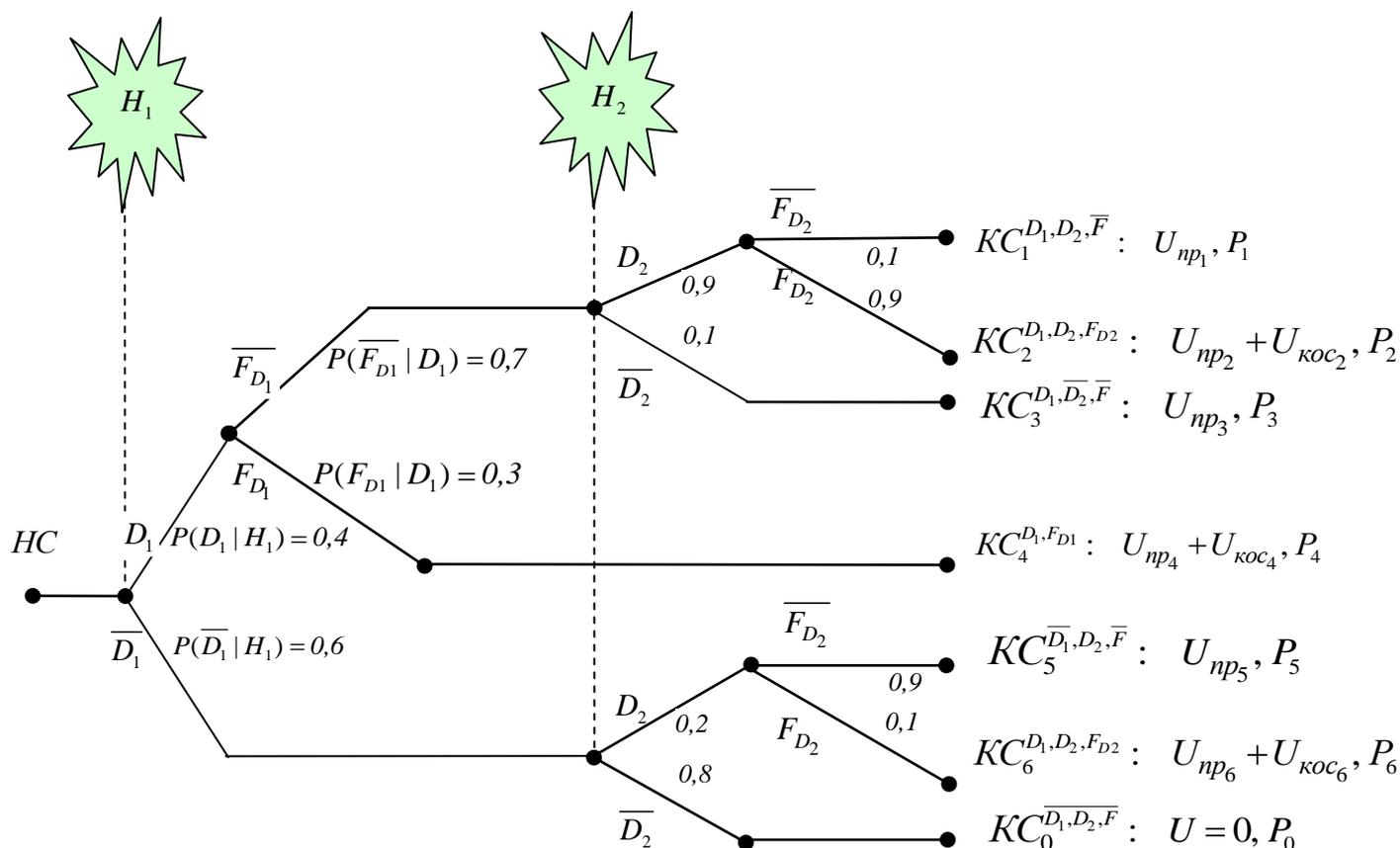
$$R_{косв} = \int_x \int_y U_{косв} P(F|D=y) f_{D|H}(y|x) f_H(x) dy dx \quad (13)$$

где случайные величины  $X$  и  $Y$  - соответственно уровень (интенсивность) угрозы и повреждения.  $f_Z(z)$ - функция плотности распределения вероятности случайной величины  $Z$ . Эти интегралы могут быть подсчитаны путем численного интегрирования или использования метода Монте-Карло [9]. Запись выражений (12) и (13) основывается на использовании интегральной формы теоремы полной вероятности. Подсчет вероятностей повреждений и отказов может производиться на основе методик, разработанных в рамках теории системной надежности.

Тогда живучесть системы, характеризующейся сценарным деревом, представленном на рис. 5, может быть рассчитана как:

$$G_R = \frac{\int_x \int_y U_{np} f_{D|H}(y|x) f_H(x) dy dx}{\int_x \int_y U_{np} f_{D|H}(y|x) f_H(x) dy dx + \int_x \int_y U_{косв} P(F|D=y) f_{D|H}(y|x) f_H(x) dy dx}$$

Рассмотрим численный пример. На рис.6 представлено сценарное дерево, описывающее систему, подвергающуюся экстремальным воздействиям  $H_1$  и  $H_2$ , в результате которых в системе могут возникнуть локальные повреждения  $D_1$  и  $D_2$ . Вероятность нанесения локального повреждения  $D_1$ .  $P(D_1|H_1) = 0,4$ . В случае локального повреждения с вероятностью  $P(F_{D1}|D_1) = 0,3$  может наступить отказ системы в целом; а с вероятностью система останется  $P(\bar{F}_{D1}|D_1) = 0,7$  система останется в работоспособном состоянии. Далее на систему оказывается экстремальное воздействие  $H_2$ .



$$U_{np(D_1)} = 1000 \text{ у.е.}; \quad U_{np(D_2)} = 2000 \text{ у.е.}; \quad U_{Koc(F)} = 10000 \text{ у.е.}$$

Рис.6. Сценарное дерево для технической системы, подвергающейся экстремальным воздействиям  $H_1$  и  $H_2$ .  $D_1$  и  $D_2$  - локальные повреждения, вызываемые воздействиями  $H_1$  и  $H_2$ ;  $F_{D_1}$  и  $F_{D_2}$  - отказы системы в результате повреждений  $D_1$  и  $D_2$ ;  $KC_i^{***}$  - конечные состояния системы с соответствующими им вероятностями реализации  $P_i$ , а также прямыми и косвенными ущербами  $U_{np_i}$  и  $U_{Koc_i}$ .

Результаты расчетов сведены в таблицу 1.:

Таблица 1

Оценка живучести системы					
Конечное состояние (сценарий) $KC_i$	Вероятность реализации $P_i$	Ущерб прямой $U_{np_i}$ , у.е.	Ущерб косвенный $U_{Koc_i}$ , у.е.	Риск прямой $R_{np_i}$	Риск косвенный $R_{Koc_i}$
$KC_1^{D_1, D_2, \bar{F}}$	0,0252	3000	0	75,6	0
$KC_2^{D_1, D_2, F_{D_2}}$	0,2268	3000	10000	680,4	2268
$KC_3^{D_1, \bar{D}_2, \bar{F}}$	0,028	1000	0	28	0
$KC_4^{D_1, F_{D_1}}$	0,12	1000	10000	120	1200
$KC_5^{\bar{D}_1, D_2, \bar{F}}$	0,108	2000	0	216	0
$KC_6^{D_1, D_2, F_{D_2}}$	0,012	2000	10000	24	120
$KC_0^{\bar{D}_1, \bar{D}_2, \bar{F}}$	0,48	0	0	0	0
Итого				<b>1144</b>	<b>3588</b>
				<b><math>G_R = 0,241</math></b>	

Тогда согласно выражению (11) индекс живучести системы равен  $G_R = 0,241$ .

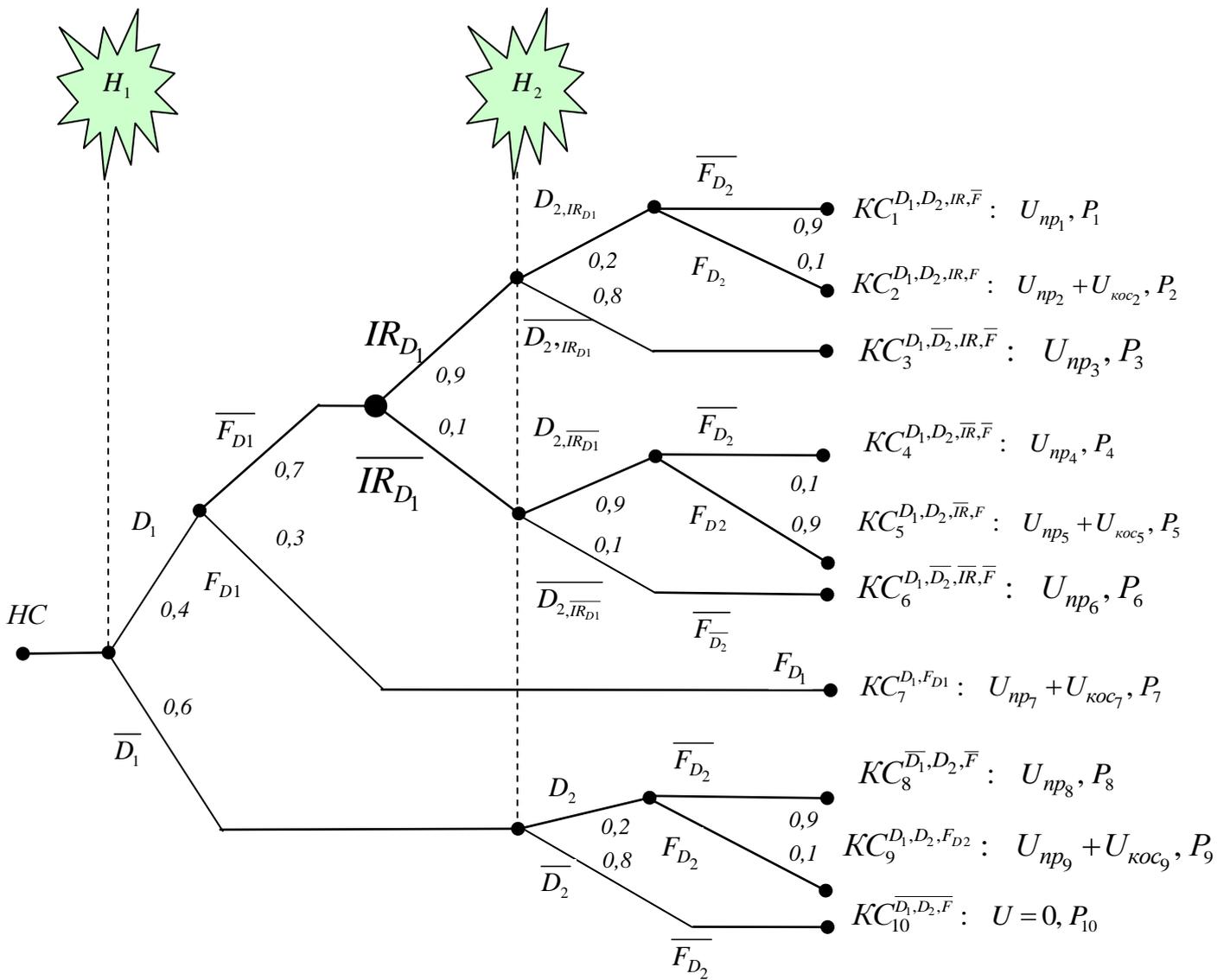
Важно, что живучесть СТС нельзя оценивать независимо от действующих в СТС систем мониторинга и управления, квалификации операторов, адекватности технических регламентов и т.д., поскольку все эти факторы влияют на способность ограничить последствия локальных повреждений и предотвратить катастрофическое разрушение системы, в случае если системе были нанесены локальные повреждения.

На рис.7 представлено сценарное дерево для той же системы, но оборудованной системой мониторинга локальных повреждений (узел  $IR_{D_1}$ ), которая позволяет с вероятностью 0,9 идентифицировать локальное повреждение  $D_1$  и осуществить ремонт до того момента как система будет подвергнута экстремальному воздействию  $H_2$ .

Таблица 2

Оценка живучести системы, оборудованной системой мониторинга

Конечное состояние (сценарий) $KC_i$	Вероятность реализации $P_i$	Ущерб прямой $U_{пр_i}$ , у.е.	Ущерб косвенный $U_{кос_i}$ , у.е.	Риск прямой $R_{пр_i}$	Риск косвенный $R_{кос_i}$
$KC_1^{D_1, D_2, IR, \bar{F}}$	0,04536	3000	0	136,08	0
$KC_2^{D_1, D_2, IR, F}$	0,00504	3000	10000	15,12	50,4
$KC_3^{D_1, \bar{D}_2, IR, \bar{F}}$	0,2016	1000	0	201,6	0
$KC_4^{D_1, D_2, \bar{IR}, \bar{F}}$	0,00252	3000	0	7,56	0
$KC_5^{D_1, D_2, \bar{IR}, F}$	0,02268	3000	10000	68,04	226,8
$KC_6^{D_1, \bar{D}_2, \bar{IR}, \bar{F}}$	0,0028	1000	0	2,8	0
$KC_7^{D_1, F_{D_1}}$	0,12	1000	10000	120	1200
$KC_8^{\bar{D}_1, D_2, \bar{F}}$	0,108	2000	0	216	0
$KC_9^{D_1, D_2, F_{D_2}}$	0,012	2000	10000	24	120
$KC_{10}^{\bar{D}_1, D_2, F}$	0,48	0	0	0	0
				<b>791,2</b>	<b>1597,2</b>
<b><math>G_R = 0,331</math></b>					



$$U_{np(D_1)} = 1000 \text{ y.e.}; \quad U_{np(D_2)} = 2000 \text{ y.e.}; \quad U_{Koc(F)} = 10000 \text{ y.e.}$$

Рис.9 Сценарное дерево для технической системы, оборудованной системой мониторинга состояний элементов

Представленные в таблице 2 расчеты свидетельствуют, что введение системы мониторинга позволяет повысить живучесть системы до  $G_R = 0,331$ .

### Оценка прямых и косвенных рисков для сложных технических систем

Как было отмечено в п. 2. прямые риски обусловлены локальными повреждениями  $D_i$  ( $i = 1, 2, \dots, n$ ), вызванными экстремальными воздействиями  $H_j$  ( $j = 1, 2, \dots, m$ ) на элементы систему.

$$R_{np} = \sum_{i=1}^n \sum_{j=1}^m P[D_i | H_j] \cdot P[H_j] \cdot U_{np_i}(D_i), \quad (14)$$

где  $U_{np_i}(D_i)$  - прямой ущерб, связанный с локальным повреждением  $D_i$ ,

Косвенные риски связаны с отказом ( $F$ ) системы в целом.

К отказу системы приводит цепочка событий, включающая: (а) экстремальное воздействие (внутреннее или внешнее)  $H$ ; (б) локальное повреждение  $D$  системы (повреждение одного из элементов) и (в) эскалацию аварийного процесса, которая представляет собой последовательность

промежуточных событий, приводящих к инициации вторичных и каскадных отказов других элементов системы, и завершается отказом системы в целом [10]. Этот отказ может выражаться, например, в обвальном разрушении несущей конструкции системы, ее неспособности выполнять заданные функции по передаче энергии (вещества и информации), или предписанные ей технологические процессы и т.д.

При этом вероятность отказа системы может быть определена с помощью цепочки условных вероятностей реализации последовательных событий:

$$P[F] = P[H] \cdot P[D | H] \cdot P[F | D, H] \quad (15)$$

В такой постановке вероятность отказа системы определяется тремя факторами: (а) вероятностью экстремального воздействия  $P[H]$ ; (б) условной вероятностью локального повреждения (повреждения элемента системы) в случае экстремального воздействия  $P[D | H]$  и (в) вероятностью отказа системы в целом в результате локального повреждения  $P[F | D, H]$ . Величина  $P[D | H]$  определяется прочностью и надежностью элементов системы (запасами, заложенными при проектировании элементов системы). А величина  $P[F | D, H]$  определяется структурными свойствами системы, уровнем резервирования в ней (наличием альтернативных маршрутов передачи нагрузки, избыточных связей и т.д.).

Таким образом, если абстрагироваться от заранее неизвестных и трудно прогнозируемых экстремальных воздействий, то могут быть выделены два направления действий по снижению вероятности отказа системы: повышение надежности ее элементов и повышение стойкости к локальным повреждениям (т.е. повышение живучести системы).

В ряде случаев выражение (15) может быть упрощено: Если рассматривать экстремальные воздействия, то часто можно считать, что  $P[D | H] \approx 1$ . Тогда выражение (15) принимает вид:

$P[F] = P[H] \cdot P[F | D, H]$ . Поэтому искусство проектировщика заключается в том, чтобы минимизировать величину  $P[F | D, H]$ .

Следует также отметить, что в рассматриваемой постановке, отказ системы возникает в результате локального повреждения  $D$ , которое, в свою очередь, может наступить только после экстремального воздействия  $H$ . Поэтому далее будем считать, что  $P[F | D, H] = P[F | D]$ . Тогда выражение (15) приобретает более простой вид:

$$P[F] = P[H] \cdot P[D | H] \cdot P[F | D] \quad (16)$$

Если учитывать множественность возможных экстремальных воздействий  $H_1, H_2, \dots, H_n$  и множественность возможных локальных повреждений  $D_1, D_2, \dots, D_m$ , то вероятность отказа системы может быть записана как

$$P[F] = \sum_{i=1}^n \sum_{j=1}^m P[D_j | H_i] \cdot P[F | D_j] \cdot P[H_i] \quad (17)$$

Для удобства вычислений это выражение может быть записано в векторно-матричной форме:

$$P[F] = \underbrace{P[F | D_1]; P[F | D_2]; \dots; P[F | D_m]}_{\{V_s\}} \times \underbrace{\begin{bmatrix} P[D_1 | H_1] & P[D_1 | H_2] & \dots & P[D_1 | H_n] \\ P[D_2 | H_1] & P[D_2 | H_2] & \dots & P[D_2 | H_n] \\ \dots & \dots & \dots & \dots \\ P[D_m | H_1] & P[D_m | H_2] & \dots & P[D_m | H_n] \end{bmatrix}}_{[V_e]} \times \underbrace{\begin{Bmatrix} P(H_1) \\ P(H_2) \\ \dots \\ P(H_n) \end{Bmatrix}}_{\{H\}} \quad (18)$$

Или в краткой форме

$$P[F] = \{V_s\} \cdot [V_e] \cdot \{H\}$$

Где  $V_s$  - вектор структурной уязвимости, компонентами которого являются условные вероятности отказа системы в случае различных локальных повреждений;

$[V_e]$  - матрица уязвимости элементов или связей системы (матрица локальной уязвимости системы), компонентами которой являются условные вероятности определенных локальных повреждений при различных экстремальных воздействиях.

$\{H\}$  - вектор угроз, компонентами которого являются вероятности осуществления различных экстремальных воздействий на систему.

Тогда косвенные риски могут быть оценены как:

$$R_{\text{кос}} = P_F \cdot U_F = V_s \cdot [V_e] \cdot \{H\} \cdot U_F \quad (19)$$

Где  $U_F = U_F^S + U_F^H + U_F^T + U_F^C$  - косвенный ущерб, связанный с отказом технической системы, включающий ущербы  $U_F^S$  для самой системы, возникающие в процессе эскалации аварии, а также издержками для природной, техногенной и социальной среды в районе размещения СТС, вытекающими из невыполнения системой возложенных на нее функций. Косвенные ущербы имеют несколько измерений: жертвы, пострадавшие; неудобства, претерпеваемые потребителями; финансовые издержки, репутационные потери и т.д. Для проведения сопоставления ущербов вводится скалярная мера ущерба, получившая название полезность (англ. utility) или, точнее, - отрицательная полезность (англ. disutility). Несмотря на то, что объединение в единый показатель таких разных величин как число жертв и финансовые потери, является не вполне корректным, к нему приходится прибегать для сопоставления ущербов при реализации различных сценариев и вариантах построения системы.

## 5. Энергетический подход к оценке живучести технических систем

Функционирование СТС связано с переработкой, хранением и транспортировкой энергии, вещества и информации ( $E, W, I$ ). Энергетический подход может быть использован для описания процесса эскалации аварии в технической системе. При этом живучесть СТС должна оцениваться с точки зрения энергетических характеристик системы: живучая система должна быть способна адекватным образом поглощать подведенную к ней энергию и энергию выделяемую при разрушении отдельных элементов системы. Целесообразность использования энергетического подхода обуславливается тем, что в процессе эскалации аварии имеют место определенные виды обмена энергией или работой между системой и окружающей средой. При реализации сценария отказа элементы системы выделяют и поглощают энергию. Энергетические параметры системы могут отражать распространение повреждений в системе, обобщая такие параметры как деформация и напряжения, пропускная способность, несущая способность и т.д.

Катастрофические сценарии отказов возникают в системе, если она не способна поглощать энергию (перераспределять потоки  $E, W, I$ ), выделяющуюся при повреждении ее отдельных элементов. Если система, находящаяся под высокой нагрузкой, находится в состоянии близком к критическому, она не способна поглощать выделяющуюся энергию и склонна к каскадному разрушению.

С точки зрения энергетического подхода могут быть выделены две группы мер, направленных на обеспечение живучести СТС: (а) повышение способности системы поглощать энергию, выделяемую при повреждении ее элементов и (б) снижение количества энергии, выделяемой в процессе эскалации аварии (при разрушении элементов). Первая группа мер включает введение специальных экранов (систем жесткой защиты) для критических элементов СТС, а также введение специальных демпферов, и создания условий для перехода от механизма хрупкого к пластическому разрушению и т.д. Ко второй группе мер может быть отнесено снижение запасов энергий в элементах системы, совершенствование технологических процессов и т.д.

Сценарий отказа СТС представляет собой непрерывный или дискретный процесс, который включает возникновение повреждений и распространение разрушений по элементам системы. В случае повреждения нового элемента система должна быть способна поглотить высвобождаемую при этом энергию. (Тогда процесс распространения повреждений будет затухать) [11, 12].

Если в системе произошел отказ элемента  $k$ , то необходимым (но недостаточным) условием продолжения реализации сценария отказа на следующий элемент системы является то, чтобы

величина энергии, высвобождаемой при разрушении этого элемента  $E_k^{высв}$ , превосходила величину энергии (работы разрушения)  $E_{k+1}^{разруш}$ , необходимую для разрушения элемента  $k+1$ , следующего в сценарии отказа за элементом  $k$ . Тогда можно записать необходимое условие для реализации всей цепочки разрушений элементов по сценарию отказа системы:

$$\sum_{k=0}^i E_k^{высв} \geq \sum_{k=0}^i E_{k+1}^{разруш}, \quad \forall i, i \leq n-1 \quad (20)$$

Здесь  $E_k^{высв}$  - энергия, высвобождаемая при разрушении  $k$ -ого элемента;  $E_{k+1}^{разруш}$  - энергия, необходимая для разрушения следующего по сценарию эскалации аварии ( $k+1$ ) элемента,  $n$  - число элементов системы, участвующих в сценарии отказа.

Тогда критерием живучести системы является условие:

$$\sum_{k=0}^i E_k^{высв} < \sum_{k=0}^i E_{k+1}^{разруш}, \quad \exists i, i \leq n-1 \quad (21)$$

Поэтому энергетический индекс живучести может быть записан:

$$G_E = \frac{\sum_{k=0}^n E_{k+1}^{разруш}}{\sum_{k=0}^n E_k^{высв}}, \quad (22)$$

Если  $0 \leq G_E < 1$ , то система достаточно живучая в том смысле что внутренних источников недостаточно, и для эскалации аварии и реализации сценариев отказа необходим подвод энергии извне. Если эта величина меньше 1, то ее можно рассматривать как индекс живучести текущей системы.

В качестве примера применения энергетического подхода к оценке живучести, рассмотрим техническую систему (рис.11), подвергающуюся экстремальному воздействию  $H$ , приводящему к локальному повреждению элемента  $k$ . Процедура поиска сценариев отказа системы, которые могут быть реализованы, исходя из энергетических соображений, проиллюстрирована на рис.12 [13]. Узел  $k$  представляет этап 0, сценария, на котором осуществляется локальное повреждение элемента  $k$ . Возможные варианты продолжения сценария отказа изображены ветвями, исходящими из корневого узла. Варианты рассматриваются путем последовательного перебора и проверки выполнения условия (20), необходимого для реализации сценария отказа системы. Пунктиром показаны ветви, которые не удовлетворяют этому условию и являются затухающими. Непрерывными линиями, показаны возможные сценарии эскалации аварии. Пусть на первом шаге эскалации аварии может быть разрушен элемент  $i$ . На втором шаге эскалации аварии может быть выведен из строя элемент  $j$  и т.д., а элемент  $l$  исходя из энергетического критерия выведен из строя быть не может. Также осуществляя на каждом шаге процедуру перебора, можно исходя из энергетических соображений, идентифицировать сценарий отказа системы  $S_*$ , который требует минимальной работы разрушения. Этот сценарий может считаться наиболее вероятным сценарием отказа исходя из энергетических соображений.

Энергетическая оценка живучести системы является весьма консервативной, поскольку она не учитывает потерь энергии и исходит из того, что вся высвобождаемая при разрушении элементов энергия переходит в работу разрушения элементов, располагающихся далее по сценарию эскалации аварии. Однако, в ряде случаев, когда для элементов системы удастся оценить величины энергий  $E_k^{высв}$  и  $E_{k+1}^{разруш}$ , представленный подход позволяет получать оценки живучести систем, не прибегая к построению сложных моделей (моделированию сценариев эскалации аварий).

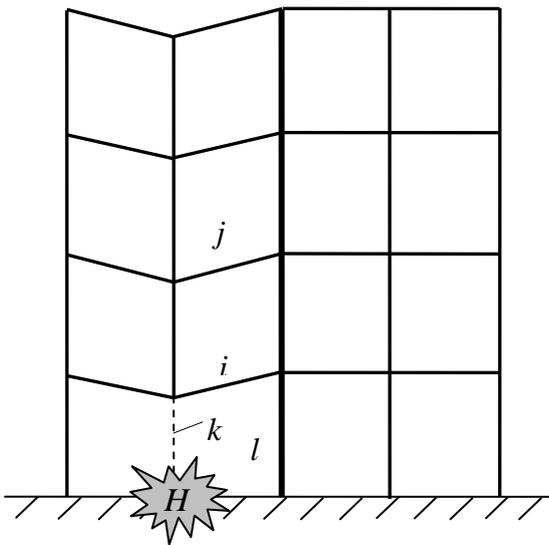


Рис. 11. Система, подвергающаяся экстремальному воздействию  $H$

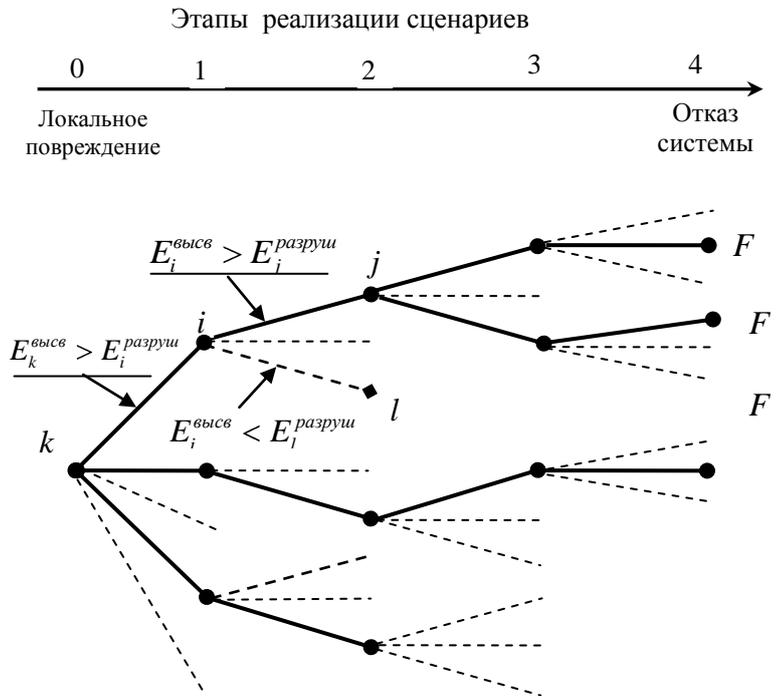


Рис. 12. Дерево возможных вариантов сценариев отказа

### 6. Живучесть сетевых систем

В многоэлементных системах, функционирование которых определяется соотношением «нагрузки» и «несущей способности» (таких как опорные конструкции, транспортные или коммуникационные сети т.д.) живучесть определяется способностью системы пропускать, поглощать и перерабатывать потоки энергии, вещества и информации  $(E, W, I)$ , которые перераспределяются в системе после того как в результате некоторого экстремального воздействия повреждаются ее отдельные элементы.

В таких системах могут реализовываться каскадные сценарии отказов. Элемент  $j$  системы выходит из строя, когда действующие на него эксплуатационные нагрузки (потоки  $E_j, W_j, I_j$ ) превосходят уровень пропускной (несущей) способности элемента. Помимо этого, элементы системы могут также выходить из строя из-за внешних экстремальных воздействий, ошибок операторов, износа и т.д. Отказ элемента выражается в том, что он перестает пропускать предписанные ему потоки энергии, вещества, информации  $E_j, W_j, I_j$ . В любом случае в результате этого отказа потоки  $E_j, W_j, I_j$  должны перераспределиться между другими компонентами системы. Отказ элемента вносит возмущение в систему и инициирует некоторый переходный процесс, заключающийся в перераспределении потоков  $E_j, W_j, I_j$ . Кроме того, отказ элемента может инициировать дополнительные потоки  $E'_j, W'_j, I'_j$  (например, при взрыве элемента), которые также должны перераспределяться среди других элементов системы. Подобное перераспределение может осуществляться среди соседних элементов, принадлежащих малой области сети, вокруг поврежденного элемента, но может выйти за эту область и охватывать значительную часть сети или всю сеть. Это означает, что отказ элемента сети приводит к увеличению нагрузки (потоков  $E_k, W_k, I_k$ ) на остальные элементы сети. Поэтому в результате отказа одного элемента сети вероятность отказа остальных элементов возрастает. Отказ элемента инициирует дополнительные взаимодействия между компонентами сети. Причем, интенсивность этих взаимодействий определяется уровнем нагрузки в сети. Если элементы сети сильно нагружены, то они имеют малые запасы, и, следовательно, могут выдержать меньшее увеличение нагрузки до того, как сами окажутся

разрушенными. С ростом загруженности сети сильно увеличиваются нелинейности и динамическая связанность между элементами.

Сценарий крупномасштабной аварии в сети включает локальное повреждение (инициирующий отказ одного из элементов), за которым следует последовательность каскадных отказов, каждый из которых приводит к дополнительному нагружению и ослаблению системы, т.е. делает более вероятными последующие отказы остающихся элементов.

Критерием живучести сетевых систем является их способность перераспределять потоки энергий, вещества и информации  $E, W, I$  и продолжать выполнение предписанных ей функций после того, как отдельные элементы системы выходят из строя.

Под живучестью сетевой системы понимается ее способность выполнять свои функции, в случае удаления определенного количества узлов или связей. Примером является так называемый  $N-1$  критерий проектирования инфраструктур, под которым понимается способность системы сохранять работоспособность, в случае выхода из строя одно из элементов.

Поскольку для широкого класса сетевых систем критерием работоспособности является выполнение условия:  $R > L$  (где  $R$  - несущая способность системы,  $L$  - эксплуатационная нагрузка на систему), то живучесть может оцениваться исходя из того, будет ли выполняться это условие после удаления одного из элементов системы и перераспределения проходивших через него потоков на оставшиеся элементы.

Тогда для сетевых систем может быть предложен следующий индекс живучести:

$$G_{net} = \min_i P(R > L | D_i) \quad (23)$$

где  $D_i$  - локальное повреждение системы, выражающееся в удалении  $i$ -го элемента.

Для получения более точных оценок живучести сетевых систем необходимо совершенствовать модели эскалации аварий. В большинстве проводящихся в настоящее время оценок живучести сетевых систем, используются простые модели повреждения сети, основанные на представлении сети в виде графа. В такой постановке рассматриваются только топологические эффекты, т.е. изучается воздействие повреждения на структуру сети. При этом узлы (элементы) и ребра (связи) сетевого графа находятся в одном из двух возможных состояний: работающем или неработающем. В случае повреждения: узлы и ребра удаляются из графа. При этом не учитывается временной фактор процесса распространения повреждений и перераспределение потоков. В такой модели распространения аварии живучесть системы может характеризоваться зависимостью степени выполнения системой заданных функциональных обязанностей (уровня функциональности системы) от количества удаленных узлов или ребер.

Поскольку реальные элементы и связи имеют ограниченную пропускную способность при построении более совершенных моделей, необходимо учитывать потоки энергий, вещества и информации, проходящие по сети. В случае повреждения элемента или связи, поток, проходивший через него, перенаправляется по альтернативным маршрутам. Это может вызвать перегрузку других элементов и связей, приводящую к их повреждению. Таким образом, любое локальное повреждение системы может привести к дальнейшей перегрузке других элементов сети и их последующим отказам. Подобные каскадные процессы могут стать причиной масштабных катастроф в сетевых системах.

## 7. Выводы

1. Живучесть сложных технических систем характеризует ее способность сопротивляться катастрофическому разрушению и выполнять предписанные ей функции, в случае если в результате экстремальных (запроектных) воздействий система получит локальные повреждения. В связи с этим для проведения количественной оценки живучести принято брать соотношение между какими либо параметрами, характеризующими состояние неповрежденной системы и состояние системы при наличии локального повреждения. В частности может рассматриваться отношение нагрузок разрушения системы с повреждением и неповрежденной системы  $G_L = L_{F|D_i} / L_{F|\bar{D}}$  или отношение вероятностей отказа системы при наличии повреждения и вероятности отказа неповрежденной системы  $G_p = P(F | \bar{D}) / P(F | D)$ .

2. Наиболее полно живучесть СТС описывается с помощью сценарного графа, который определяет вероятностные связи между событиями, наступающими после нанесения системе

локальных повреждений. Поэтому с точки зрения универсальности следует отметить индекс живучести, основанный на соотношении прямых и косвенных рисков для рассматриваемой системы

$$G_R = \sum_{i=1}^m R_{np_i} / \left( \sum_{i=1}^m R_{np_i} + \sum_{j=1}^n R_{koc_j} \right).$$

Этот индекс позволяет оценить склонность системы к катастрофическим отказам, соответствующим хвостовым частям распределений ущербов.

3. Необходимым условием реализации сценария катастрофического разрушения СТС является то, чтобы величина энергии  $E_k^{высв}$ , высвобождаемой при разрушении элементов на  $k$ -ом этапе сценария, превосходила величину энергии (работы разрушения)  $E_{k+1}^{разруш}$ , необходимую для разрушения элементов на последующем  $k+1$  этапе (для любого этапа  $k$  рассматриваемого сценария, кроме заключительного).

4. Могут быть выделены вероятностный и детерминированный подходы к оценке живучести технических систем. К детерминированным подходам, в частности, относятся силовой и энергетический методы оценки живучести. Вероятностный подход реализуется путем построения индексов, характеризующих надежность поврежденной и неповрежденной системы, и индекса надежности, базирующегося на соотношении прямых и косвенных рисков.

5. Повышение живучести сложных технических систем является важным направлением усилий по снижению рисков. Живучесть СТС может обеспечиваться путем реализации совокупности технических и организационных мер. К техническим мерам относятся совершенствование топологии СТС, построения систем мониторинга состояния и защиты СТС, введение систем резервирования процедур автоматических переключений и реконфигураций. К организационным мерам могут быть отнесены совершенствование системы управления, повышение квалификации операторов и персонала и подготовка плана ликвидации последствий отказов СТС.

## Литература

1. В.В.Стружанов. Живучесть и устойчивость механических систем. Вестник Самарского технического университета. Серия Физико-математические науки. 2004, №30, стр. 5-21.
2. Воробьев Ю.Л., Малинецкий Г.Г., Махутов Н.А. Управление риском: Риск. Устойчивое развитие. Синергетика. М.:Наука.2000,431с.
3. Махутов Н.А., Резников Д.О., Петров В.П. Оценка риска аварий на КВО с учетом возможности реализации экстремальных ущербов//Проблемы безопасности и чрезвычайных ситуаций.- М.: ВИНТИ, 2008, №5.
4. Махутов Н.А., Резников Д.О. Оценка уязвимости технических систем и ее место в процедуре анализа риска. Проблемы анализа риска, том 5, 2008, № 3 с. 76-89
5. Махутов Н.А., Петров В.П., Резников Д.О. и др. Прочность, ресурс, живучесть и безопасность машин. Либроком. 2008, 565 с.
6. Lind, N. C. (1996). "Vulnerability of damage-accumulating systems." Reliability Engineering & System Safety, 53(2), 217-219.
7. M. Maes, K. Fritzsos, S. Glowienka, Risk-based indicators of structural system robustness. JCSS and IABSE Workshop on Robustness of Structures.
8. Baker, M. Schubert, M. Faber On the assessment of robustness. Structural Safety 30 (2008)253 -267
9. M.Schubert, , and M.Faber (2007). "Robustness of Infrastructures Subject to Rare Events.". 10th International Conference on Applications of Statistics and Probability in Civil Engineering, Tokyo, Japan
10. U. Starossek, M. Haberland. Measures of Structural Robustness – Requirements and Applications. Proceedings of ASCE SEI 2008 Structural Congress – Crossing Borders. Vancouver. Canada.
11. M. Haberland. Progressiver Kollaps und Robustheit (Progressive collapse and robustness). Hamburg University of Technology, Structural Analysis and Steel Structures Institute. Diploma thesis. 2007– (in German)
12. D. Dusenberry, R. Hamburger. Practical Means for Energy-Based Analyses of Disproportionate Collapse Potential. JOURNAL OF PERFORMANCE OF CONSTRUCTED FACILITIES. ASCE / NOVEMBER 2006
13. J. Smith. Structural Robustness Analysis and the Fast Fracture Analogy. JCSS and IABSE Workshop on Robustness of Structures.

## Assessment of Complex Technical Systems Robustness

Nikolay A. Makhutov, Vitaly P. Petrov, Dmitry O. Reznikov

The paper presents the basic approaches to quantitative assessment of complex technical system robustness. These include: approaches based on the relationship between direct and indirect risks, relationship between failure

probability of damaged and intact systems, and energy based robustness assessment approach. The example of robustness assessment for technical system is given. The importance of robustness increase in the efforts to ensure safety of complex technical systems is substantiated.

**Kew words: robustness, vulnerability, risk, safety.**

### **References**

1. V. Strujnikov. Robustness and Resilience of Mechanical Systems. Bulletin of Samara State University. Physical and Mathematical Sciences Series. 2004, №30, pp. 5-21, (in Russian).
2. Yu. Vorobiev, G. Malinetsky, N. Makhutov. Risk Management. Risk. Sustainable Development. Synergistics. Moscow, Nauka publishers. 2000, 431p. (in Russian)
3. N. Makhutov, D. Reznikov. Assessment of Accident Risks at Critical Facilities Taking into Account the Possibility of Extreme Losses. Problems of Safety in Emergencies. Moscow, VINITI publishers, 2008, vol. 5, 55-72 (in Russian)
4. N. Makhutov, D. Reznikov. Technical System Vulnerability Assessment and its Role in the Framework Risk Analysis. Issues of Risk Analysis, 2008. vol. 5, 76-89 (in Russian)
5. N. Makhutov, V. Petrov, R. Akhmetkhanov, D. Reznikov at al. Strength, Lifetime, Robustness and Safety of Machines, Librocom publishers, 2008, 565 (in Russia).
6. N. C. Lind, (1996). "Vulnerability of damage-accumulating systems." Reliability Engineering & System Safety, 53(2), 217-219.
7. M. Maes, K. Fritzsos, S. Glowienka, Risk-based indicators of structural system robustness. JCSS and IABSE Workshop on Robustness of Structures.
8. J. Baker, M. Schubert, M. Faber On the assessment of robustness. Structural Safety 30 (2008) 253 -267
9. M. Schubert, , and M. Faber (2007). "Robustness of Infrastructures Subject to Rare Events.". 10th International Conference on Applications of Statistics and Probability in Civil Engineering, Tokyo, Japan
10. U. Starossek, M. Haberland. Measures of Structural Robustness – Requirements and Applications. Proceedings of ASCE SEI 2008 Structural Congress – Crossing Borders. Vancouver. Canada.
11. M. Haberland. Progressiver Kollaps und Robustheit (Progressive collapse and robustness). Hamburg University of Technology, Structural Analysis and Steel Structures Institute. Diploma thesis. 2007– (in German)
12. D. Dusenberry, R. Hamburger. Practical Means for Energy-Based Analyses of Disproportionate Collapse Potential. JOURNAL OF PERFORMANCE OF CONSTRUCTED FACILITIES. ASCE / NOVEMBER 2006
13. J. Smith. Structural Robustness Analysis and the Fast Fracture Analogy. JCSS and IABSE Workshop on Robustness of Structures.