

### ПРОГНОЗИРОВАНИЕ ОПАСНОСТИ ПОЛЕТОВ КОСМИЧЕСКИХ ЧЕЛНОКОВ ТИПА «ЧЕЛЕНДЖЕР» И «КОЛУМБИЯ» НА ОСНОВЕ УПРАВЛЕНИЯ РИСКАМИ

д.т.н. Е.А. Куклев  
(АГА, Санкт-Петербург)

*На примере известных катастроф с космическими челноками (Space-Shuttle) "Челенджер" (1987 г.), "Колумбия" (2003 г.) дается ретроспективное развитие научной идеи о возможности применения новых моделей рисков для прогнозирования заранее возникновения опасных сценариев развития событий в космических полетах. Риски катастроф оцениваются как измеримые случайные величины и события в рамках теории алгебры логики и цепей случайных событий.*

В технической сфере оценки рисков основаны на представлениях из теории надежности, что не всегда применимо при изучении редких и маловероятных событий, к которым могут быть отнесены катастрофы с космическими аппаратами, подводными лодками и самолетами. Известна [1] так называемая проблема – «старта на авось» (launch on hunch), выявленная при анализе особенностей возникновения некоторых катастроф. Отсутствие достоверной статистики при прогнозировании возможностей возникновения маловероятных катастроф приводит к большой неопределенности результатов. Использование при этом по [1] метода доверительных интервалов, накрывающих статистику, приводит к новой неопределенности, связанной с выбором границ интервалов и критериев достоверности.

Отмеченное обстоятельство, являющееся главным в теории безопасности на транспорте [3], достаточно основательно исследовалось в NASA [1] при разработке космической программы «Space-Shuttle». В этой программе вероятностная концепция риска, вытекающая из теории надежности, приводила, как выяснилось впоследствии, к ошибочным решениям ввиду недостоверности вычисления вероятности катастрофы по ряду конструктивных параметров Шатла. После гибели "Челенджера" [1] концепция «launch on hunch» была подвергнута сомнению. Но как было выяснено в [11], в случае «Колумбии» концепция упомянутого подхода, рассматривавшегося ранее в NASA, все же, до известной степени, имела место. Вместе с тем, при разработке теорий оценки безопасности полета в гражданской авиации находит применение концепция цепей событий J. Reason's и исчисления индикаторов рисков (уровней рисков) на основе экспертных методов по примеру программы CFIT [6], без вероятностных показателей.

Цепи Дж. Ризона определяют последовательности причинно-следственных факторов, завершающихся катастрофой. Впервые подобный подход был применен для оценки возможностей возникновения аварий на атомных электростанциях. При этом достаточно широко используются показатели опасности в форме индикаторов уровней риска и экспертные коэффициенты риска, имеющие знаковые значения измерений уровня опасности с порядками от 1 до 1000 баллов.

Целью данной статьи является разработка некоторых моделей управляемых рисков в задачах анализа возможностей возникновения катастроф с космическими комплексами типа «Space-Shuttle» «Челенджер» [1] и «Колумбия» [11].

#### Постановка задачи

Некоторые явления, объясняющие природу опасности и катастроф в транспортных комплексах и в сложных человеко-машинных системах, могут быть изложены с новых позиций. Дело в том, что эффективность и безопасность человеко-машинной системы трудно количественно оценить в рамках теории надежности и теории вероятностей. Так, теорему о полной вероятности событий практически невозможно применить для исследования процессов в

человеко-машинной системе из-за вычислительных трудностей и многомерности пространства исходов. Но именно в таких системах при рискованных редких ситуациях маловероятная ошибка человека-оператора может привести к большим ущербам.

Предлагается принять [1 - 4], что риск  $R$  – это случайное событие: опасное нежелательное и с последствиями в виде ущерба  $H_R$ .

Некоторое событие  $A=R$  считается рискованным, если имеющимися техническими средствами нельзя обеспечить необходимую безопасность [5].

В связи с этим вводится многомерная оценка  $R$  риска  $R$  в следующем виде [4]:

$$R=(\mu_1, \mu_2, H_R | \Sigma_0), \quad (1)$$

где  $\mu_1$  – известная мера случайности появления рискованного события, например, с оценкой этой меры через вероятность или эквивалентный показатель в виде относительной частоты появления события;  $\mu_2$  – оценка опасности ситуаций, возникающей в системе в зависимости от сложности ее структуры [6, 7];  $\Sigma_0$  – комплекс условий, определяющих функционирование системы и ее структуру.

Рискованное событие  $A$  является классом  $A=R=UR_j$ , составленным из тех несовместных частных рисков  $R_j$  или, что то же самое, из альтернативных способов попадания системы в катастрофическое состояние заданного типа. Поэтому в первом приближении ущерб считается постоянной величиной  $H_R=const$  для всего выделенного класса  $R$ . Например,  $H_R$  – это материальные и моральные потери, возникшие в связи с затоплением подводной лодки или гибели космического аппарата из-за разных причин. Мера  $\mu_1$  по определению – это вероятность класса:

$\mu_1=P\{R_j\} \equiv \mu_p, j=1, 2, \dots, n_R$ . Мера  $\mu_p$  можно определять по формуле полной вероятности события  $A=R$ , а частные  $\mu_{1i}$  – соответственно через условные вероятности, если это в каких-то случаях удастся сделать.

Сформулированные положения вытекают из концепции «дерева отказов», определяющего пути попадания системы в одно и то же состояние – катастрофу [3] с фиксированным ущербом.

Комплекс условий  $\Sigma_0$  определяет степень деформации структуры системы на момент начала развертывания рискованных сценариев и может также содержать признаки (коды) внешней среды, вызывающей лавину отказов и т.п. Например, этот комплекс есть дизъюнкция экспертных признаков опасности в виде  $\Sigma_0=(e_0 \vee e_1 \vee e_2)$ , где  $e_0=1$  – «норма»;  $e_1=1$  – «опасно»;  $e_2=1$  – «крайне опасно» (катастрофическое состояние, например при затоплении отсеков подводной лодки),  $\vee$  – дизъюнкция.

Предложенный вид оценки (1) отражает достаточно устоявшиеся способы 2-х-мерного оценивания рисков  $R \sim (\mu_1, H_R)$  через вероятность события  $\mu_1=\mu_p$  и ущерб [2, 8, 9]. Но поскольку в случае вероятности катастрофы «почти нуль» подобная оценка практически ничего не дает, то следствием этого является возникновение проблемы «старта на авось», т.к.  $\mu_1 \approx 0$ . Поэтому естественным является выдвинутое выше предложение (1) о том, чтобы почерпнуть информацию о предполагаемой опасности из других источников, т.е. по  $\mu_2$ .

Следует отметить, что введенное трехэлементное множество (1) не является вектором и не может быть сведено к скалярной свертке из [2]. Это может быть объяснено тем, что, во-первых, здесь усреднение ущерба по вероятности не имеет смысла, т.к. катастрофические события имеют единичный характер, тем более что  $\mu_1 \approx 0$ . Далее, мера риска 2-го рода не зависит от вероятности событий и является объективной характеристикой опасности, заложенной в структуру системы.

Задача заключается в том, чтобы найти способы вычисления меры риска или меры опасности 2-го рода в виде  $\mu_2$  с учетом структуры системы и комплекса условий  $\Sigma_0$ .

### Схема решения задачи

Рассматриваются системы  $S$ , в которых случайное рискованное событие  $R$  осуществляется как цепочка событий  $L_R$ :

$$L_R=\{qi_0, \dots, qi_R\} \Rightarrow R, \quad (2)$$

где  $\Rightarrow$  - знак взаимосвязи,  $qi_0$  – начало цепочки,  $qi_R$  - последнее событие в цепи  $L_R$ , что в совокупности дает сценарий развития процесса в заданной системе (в транспортной, банковской, в космической и т.д.). Результатом каждой рискованной цепочки будет ущерб  $H_R$ , который может быть выражен в стоимостном эквиваленте объекта или в виде материальных и других видов потерь. Анализ структуры цепочки (2) дает способы описания риска как случайного события, но в виде управляемого риска, поскольку на свойства цепочки  $L_R$  можно воздействовать определенным образом [9].

В классе событий  $R$  соответственно может быть выделено множество частных рискованных цепочек  $L_{R_j}=R_j, \{L_{R_j}\}=R(\{L_{R_j}\})$ , что позволяет оценивать вероятностную меру риска  $\mu_l=\mu_p$  более детально: через последовательности причинно-следственных связей. К сожалению, частные меры  $\mu_{l_j}$  и суммарная мера  $\mu_l$  так малы, а статистика отсутствует, что становится целесообразным все же отыскивать меру риска 2-го рода  $\mu_2$  из (1). В сформулированной задаче необходимо связать предложенную здесь новую дополнительную меру риска 2-го рода  $\mu_2$  из (1) со свойствами цепи (2).

### Формула риска

Принимается рабочая гипотеза, что риск  $R$  – это измеримое случайное событие  $A_\xi$  с признаками случайности  $\xi \in \Omega_\Sigma$ .

$$R=A_\xi(D), A_\xi \in \Omega_\Sigma, A_\xi \equiv L_R, \quad (3)$$

где  $\Omega_\Sigma$  - пространство случайных исходов в опытах и их значений в зависимости от способа определения событий типа  $A_\xi$ ;  $D$  - условия определения рассматриваемых случайных чисел  $\xi$  в пространстве  $\Omega_\Sigma$ . Поскольку риск  $R$  должен измеряться определенным способом, то события  $A_\xi$  должны быть измеримы с учетом условий  $D$ .

Измеримость событий  $R \sim A_\xi$  по [8] понимается в следующем смысле:

- обеспечивается регистрация появления событий через индикаторные функции  $\chi_A$ ,

$$\chi_A = \{1 - \text{есть событие } A_\xi \in D, 0 - \text{нет события } A_\xi\};$$

$$\forall R=A_\xi \in \Omega_\Sigma \exists \mu_{AR} = \mu_R \sim D;$$

- существует некоторая неслучайная мера  $\mu_R$  возможности возникновения риска  $R$  в виде события  $A_\xi$ , определенного через некоторую цепочку событий  $L_R$ . Согласно (1) и в отличие от [1], здесь предлагается использовать, как было выше принято, независимые меры опасности или риска 2-х видов  $\mu_R \sim (\mu_1 \text{ и } \mu_2)$ :

$$\mu_l = \mu_p, \mu_2 = \mu_R \{L_{R_j} | \Sigma_0\}, \quad (4)$$

где  $\mu_l$  – мера 1-го рода, в обычном толковании [1],  $\mu_2$  – мера непосредственной опасности ситуации, вычисляемой в зависимости от структуры цепочек событий  $L_{R_j}$ , ведущих к риску.

Понятие измеримости вводится для того, чтобы сузить класс рискованных событий по степени неопределенности их появления и возникновения ущерба. Это позволяет ограничиться только теми рисками, которые могут быть отнесены к случайным с вероятностной мерой и не рассматривать игровые ситуации, возникающие в процессах принятия решений. Таким образом, сохраняется общность оценки (1) для 2-х мер риска, находимых в одном и том же вероятностном пространстве. В тех случаях, когда  $\mu_l = \mu_p \equiv 0$ , используется только оценка  $\mu_2$ , зависящая от структуры системы и от цепочек и не зависящая от вероятности событий.

Основное положение заключается в том, что при использовании цепей событий для описания катастрофического сценария по методу J. Reason [6] полная мера риска 2-го рода  $\mu_{R\Sigma}$  аддитивна вдоль цепи  $L_R$ . Метод цепей был реализован в системах CFIT [6] и FORAS [7] в виде формулы «суммы рисков и шансов».

Меру риска 2-го рода  $\mu_2$  можно определить в зависимости от свойств цепей  $L_R \sim \{L_{R_j}\}$  из (1) следующим образом. Можно принять, что цепь составляют логические элементы надежности  $x_i \in X$ , определяющие состояние физических элементов в виде:  $x_i=0$  – «норма» (неотказ),  $x_i=1$  – «отказ» ( $x_i$  - отрицание  $x_i$ ). Тогда сумма «отказов» и «неотказов» в цепях дает в первом приближении степень опасности цепи и путь к катастрофе. Известен критерий «кратчайшего

пути» по Рябину И.А. [10], который определяет минимальное сечение или набор элементов  $\{x_i|R\}$ , при котором катастрофа обязательно будет, где «\*» - знак критичности комбинации  $x_i$ , обозначающих возникновение катастрофы.

При этом оценка  $R$  риска  $R$  из (1) по мере 2-го рода находится по шкале CFIT [6] (по «Check – List» - Vandell, (FSF)) в виде суммы баллов:

$$\mu_{R2\Sigma} = \sum_i m_i(L_R) - \text{для заданных условий и ситуаций } \Sigma_0 \text{ (основное соотношение), для «суммы}$$

рисков и шансов» в виде:

$$\mu_{R2\Sigma} = \sum_{i_1} m_{i_1}(L_R) - \sum_{i_2} m_{i_2}(L_R) = \Delta_{12} - \text{ по шкале «Check – List»,} \quad (5)$$

где  $m_{i_1}$  – риски опасности, знак (-) - «минус»,

$m_{i_2}$  – шансы благоприятных результатов, знак (+) – «плюс».

Суммарная мера опасности вычисляется следующим образом:

- коэффициенты риска (уровни) выбираются путем экспертного оценивания степени опасности в каждом звене цепи;

- производится суммирование коэффициентов  $m_i$  (баллов) по (5);

- полученный результат сравнивается с нормой  $\Delta_{12*}$ , причем в безопасной системе все «минусы» должны компенсироваться «плюсами», в противном случае система опасна по мере риска 2-го рода.

По Check-List CFIT принято: если  $\Delta_{12} \sim - (100 \div 300)$  – «нормально» или «достаточно не опасно» - риск невелик; при  $\Delta_{12} \sim - (350 \text{ и более})$  - риск велик и необходимо управление рисками. Это значит, что если в цепи событий имеются элементы или звенья с определенным уровнем опасности или риска, то общий риск опасности, а точнее мера риска 2-го рода  $\mu_{R2\Sigma}$ , найденная по шкале в CFIT или по другой шкале, предназначается для принятия решений по оценке степени соответствия системы требованиям по безопасности в ситуациях «старта на авось» при вероятности катастрофы «почти нуль». Главный результат при этом состоит в том, что удастся выявить опасные пути - цепи к катастрофе и найти безопасные ситуации предотвращения катастроф.

Все множество цепей  $\{L_{Rj}\}$  в (2), ведущих к катастрофе, может быть найдено на основе правил алгебры логики событий с помощью цифровых кодов элементов (состояний  $qi$ ), входящих в каждую цепь  $L_{Rj}$ . Обе, введенные выше в (1), меры  $\mu_1$  и  $\mu_2$  – неслучайные и определяют свойства измеримых случайных событий. Эти меры определяются теоретически и непротиворечиво в смысле аксиоматики случайных процессов при определенных условиях  $\Sigma_0 \sim \Sigma_P, \Sigma_R$  в вероятностных пространствах  $D$  (или  $D \sim D_R$  - в условном пространстве для класса рисков событий). Сформулированный тезис отражает направление разработок, развиваемых в гражданской авиации в мировом авиационном сообществе в области оценивания безопасности полетов. Этот подход предлагается применить здесь для выявления тех схемных ошибок в реализации космического проекта, которые могут привести к катастрофе как возможные причины.

### Практическое значение мер риска второго рода

Принятые в данной статье нестандартные меры риска типа меры 2-го рода  $\mu_2$  позволяют непосредственно измерить количественно опасность ситуации или транспортной системы при ее эксплуатации. Для этого теоретически не требуется знать значения вероятности рискованного события. Практически это означает, что в тех случаях, когда вероятность рискованного события почти нулевая или неизвестная, недостоверная или не может быть вычислена на основе статистики или свойств системы, то мера риска 2-го рода будет объективно (и достоверно) обозначать реальную измеримую опасность. Для этого, как было показано выше, достаточно описать структуру процесса с помощью дерева событий или дерева отказов. Возможные способы воздействия на риск включают следующие варианты управления рисками:

а) **компенсация риска** (максимальное устранение опасности за счет вложения средств - это разорительно, но, тем не менее, безопасность полетов в какой-то степени гарантируется;

вырожденный случай компенсации риска – это отказ от деятельности, т.е. предлагается ничего не делать, например, не летать, но это неконструктивно);

б) **текущее управление и мониторинг** (оценивание рисков заранее по CFIT, контроль рисков в каждом полете по FORAS; изменение структуры цепочек событий типа J. Reason);

в) **поглощение риска путем страхования** полного материального ущерба (при этом убытка может не быть, но, по-видимому, это будет аморально, если произойдет катастрофа с человеко-машинной системой).

### **Возможные схемы принятия решений с учетом рисков по реализации космических проектов**

Задачу о выборе стратегии предпочтения при анализе вариантов решений в некоторых операциях в транспортных комплексах можно решать с учетом оценки опасности ситуаций на основе способов оценки рисков в рамках принятых определений. Главным является обоснование выбора действий и принятия решений в ситуациях типа «старт на авось». С введением двух мер риска  $\mu_l$ ,  $\mu_p$  эту задачу можно сформулировать иначе, чем в [1]: поиск оптимальных вариантов построения систем предлагается делать с использованием 2-х мер рисков 1-го и 2-го рода, а не одной в виде  $\mu_l = \mu_p$ , как в [1], поскольку  $\mu_l \neq 0$ .

**Стратегия 1 – «старт на авось»**, если вероятность катастрофы или опасность риска очень мала. Эта стратегия, например, может состоять в том, что на основании малости вероятностной меры  $\mu_l = \mu_p \neq 0$  можно пренебречь ожидаемым ущербом  $H_{RI}$  и не тратиться на компенсацию опасности конструкций или ситуации, т.е. принять решение «launch on hunch» [1] и сделать выбор о «не важности» вреда или ущерба, хотя в данном случае ущерб будет максимальным:

$$H_{RI}(\mu_p) = H_{RI}^* \rightarrow \max, \text{ при условии } \mu_p = 0. \quad (6)$$

Очевидно, что величина среднего ущерба, предлагаемого в [2] не будет иметь никакого смысла. Решение (6) чревато большими ущербами, если риск как событие все же осуществится.

Можно полагать, что именно это и произошло в случае катастрофы с челноком «Челенджер», а именно: приходится признать, что потерпел аварию высоконадежный объект. Представленные выше высказывания по обсуждаемой теме выражают только личное мнение авторов и не имеют отношения к оценкам фактических причин гибели космических челноков. Использованные здесь некоторые недостоверные сведения представлены всего лишь для иллюстрации основной идеи статьи о необходимости и возможности решения проблемы «старта на авось» в рамках оценки (1), что позволяет обойти трудности вычисления малых значений вероятности для редких событий с большими ошибками.

В рассматриваемом случае катастрофы с челноком «Челенджер» было установлено [1], что прогорели прокладки горловин, соединяющих стартовые двигатели с корпусом корабля. Однако предварительные расчеты надежности системы показывали, что принятого в конструктивной схеме вариантов дублирования элементов, было вполне достаточно. Точность расчетов считалась высокой. Однако катастрофа произошла. Это событие послужило причиной появления серии работ и научных споров о том, как избежать ситуации «старта на авось», возникающей всегда, когда обнаруживается неопределенность исходных данных в случаях редких, маловероятных событий. В работах НТК РАН «Надежность» проблемам риска на примере катастрофы «Space-Shuttle» были посвящены специальные исследования по устранению последствий, вытекающих из проблем типа «старта на авось».

На примере «Челенджер» видно, что вместо предотвращения возможной предполагаемой опасности, что требовало больших финансовых затрат, было принято решение не менять конструктивную схему, и это оказалось ошибочным. Таким образом, неправильная оценка безопасности только по мере первого рода  $\mu_l \rightarrow 0$  привела к катастрофе космического корабля «Челенджер» [1]. Принятие решений по стратегии 1 привело к ситуации «launch on hunch» [1], которой, по-видимому, можно было бы избежать, если бы были использованы стратегии принятия решений на основе двух мер рисков по [7].

**Стратегия 2** может состоять в том, что для гарантии безопасности **заранее компенсируются** неудовлетворительные или сомнительные по  $\mu_2$  особенности системы **S** путем выделения ресурсов на модернизацию системы с учетом значения меры  $\mu_2$  (второго рода), т.е. производится изменение вектора конструктивных параметров системы  $K \sim (K_1, K_2)$ . Это уже будет дороже, но и опасность  $\mu_2$  существенно уменьшится, что необходимо для транспортных систем и, особенно, для космических проектов.

На основе цепочек событий и мер риска 2-го рода в стратегии 2 может быть осуществлено некоторое управление рисками: надо менять структуру цепочки  $L_{Rj}$  по мере 2-го рода  $\mu_2$ , обеспечить возвраты процесса смены состояний в начало цепочки, и естественно, если это возможно, обеспечивать характер процессов таким образом, чтобы мера риска 2-го рода  $\mu_2 \ll \mu_2^*$  была малой. За счет влияния на свойства звеньев цепи можно добиться также уменьшения вероятности рискованных событий и по вероятностной мере  $\mu_I \sim \mu_P$ , так как  $\mu_P = \mu_P(\mu_2)$ . В случае «Колумбии» [11], независимо от истинных причин катастрофы, необходимо было бы отказаться от концепции «старта на авось» и просчитать все возможные цепочки событий и соответствующие исходы с предполагаемым ущербом, хотя бы с учетом устаревания конструкции или явной неисправности отдельных устройств в виде повреждения теплозащиты крыла [11] и т.п.

### Заключение

Отождествление «понятия риск» с определением «вероятности некоторого события», особенно в случаях изучения «управляемых рисков» и маловероятных редких событий, неконструктивно. Целесообразно для оценивания значений или уровней рисков использовать две разнородных по смыслу меры риска 1-го рода и 2-го рода, отражающих двойственность свойств риска как события с некоторой мерой (1-го рода) случайности или возможности появления риска и как степень опасности состояния или процесса (мера 2-го рода).

Использование понятия измеримость случайных событий необходимо для того, чтобы исключить особый класс катастроф с «игровой неопределенностью» и остаться в классе событий, мера случайности которых подчиняется закону больших чисел.

На основе результатов данной работы появляется возможность изучать всего лишь один риск – рискованное событие, но с различными мерами, вместо многих рисков, предложенных во многих работах [1, 2]. К разным видам риска с различной природой можно отнести страховой риск, коммерческий, политический риски, экологические риски и т.п.

### ЛИТЕРАТУРА

1. *Володин В.В. (ред.)* Надежность в технике. Научно-технические, экономические и правовые аспекты надежности. - Институт машиноведения им. А.А. Благонравова, МНТК "Надежность машин" - РАН, М.: 1993, с. 119-123.
2. *Мушик Э., Мюллер П.* Методы принятия технических решений. Пер. с немецкого. - "Мир", М: 1990. (ENT SCHEIDUNGSPRAXIS, Ziele Verfahren Konsequenzen, Veb Verlap Technice, Berlin, 1990).
3. *Э. Дж. Хэнри, Х. Кумamoto.* Надежность технических систем и оценка риска. – Машиностроение, М.: 1984 (пер. с английского. Ред. В.С. Сыромятников).
4. *Куклев Е.А.* Прогнозирование появления авиационных происшествий на основе цепей случайных событий: Сборник Докладов Международного Симпозиума "МАКС-99" (ЦАГИ), август 1999.
5. British Standart Quality management and quality assurance – Vocabulary. BS EN ISO-8402, 1992.
6. *G. Vandell.* Check-List-CFIT-FSF. Rev. 2.2R/500/Г, - ICAO. Montreal: 1994 - Программа CFIT, ИКАО, циркуляр (методика оценки рисков): 1996.
7. *J. McCarthy, U.S. Naval Research Labaratory, D. Schwartz, AT & T.* Modeling Risk with the Flight Operations Risk Assessment System (FORAS). - Conference of ICAO in Rio de Janeiro, Brasil, Nov. 1999.
8. *Ховановн Н.В.* Математические модели риска и неопределенности. СПГУ-С.Пб.:1998.

9. *Макаров И.Н. (ред.), Малинецкий Г.Г., Кульба В.В. и др. Управление риском. (Риск. Устойчивое развитие. Синергетика).* – РАН - "Наука", М.: 2000.
10. *Рябинин И.А. Надежность, живучесть и безопасность корабельных электроэнергетических систем.* – ВМА им. Н.Г. Кузнецова, СПб.: 1997.
11. *Невский А. (ФГУП ЦНИИМАШ РАКА). Метеоритная версия гибели шатла "Колумбия".* – "Воздушный флот", № 7 (81) 02. 2003.