



# Оценка безопасности сложных систем на основе моделей управления рисками с учетом требований ИКАО

## В.М. Рухлинский

*д.т.н., председатель комиссии по связям с ИКАО, международными и межгосударственными организациями Межгосударственного авиационного комитета (МАК), действительный член АПК*

## Л.Е. Малышева

*начальник отдела Межгосударственного авиационного комитета (МАК), аспирант Московского государственного технического университета гражданской авиации (МГТУ ГА),*

## В.Л. Балановский

*вице-президент проблемного отделения «Электромагнитная безопасность» Академии проблем качества РФ, действительный член АПК*

## В.М. Калмыков

*Заместитель генерального директора ООО «НИЦЭМБС», действительный член АПК*

Существует множество разнообразных и отличающихся как по структуре, по назначению, так и по особенностям эксплуатации сложных технических систем, представляющих собой комплексы транспортных технических систем (аэропортов, железнодорожных узлов и сетей, комплексы морских и речных перевозок и др.), системы атомных, гидро-, тепловых и иных электростанций, системы технических средств защиты военных, а также гражданских объектов и многие другие. Каждая из перечисленных сложных систем, обладает рядом качеств, позволяющих рассматривать системы мер повышения безопасности с позиции близкой к организации их информационной обеспеченности. На современном этапе технологического информационного развития предполагается, прежде всего, для каждой сложной технической системы выделение в качестве элементов таких подсистем, которые уже допускали бы по-

строение связанных информационных систем, включающих наборы баз (и системы передачи и обмена таковыми) данных, системы анализа, прогнозирования, выявления вероятных (или потенциальных значимых) рисков ситуаций как для задач принятия решений людьми, так и в режиме работы автоматизированных систем. Для повышения уровня безопасности на таких объектах необходимо проведение специальных мер мониторинга параметров и характеристик, создание информационных баз и накопление данных, построение автоматизированных систем для прогнозирования, предотвращения и количественного оценивания рисков на основе соответствующего анализа этой информации. При этом одной из наиболее уязвимых и сложных систем является авиационно-транспортная система (АТС), в которую входят: персонал, воздушные суда, авиакомпании, аэропорты, предприятия по организации воздушного движения, организации по техническому обслуживанию и ремонту воздушных судов, центры подготовки персонала, научно-исследовательские организации, учебные заведения (рис. 1).



**Рис. 1. Группа специалистов проводит осмотр самолета после вынужденной посадки**

Одним из показательных примеров организации такого типа системы мер повышения безопасности является создание служб безопасности на транспорте. При этом естественной становится задача установления автоматизированных режимов работы как для повышения их эффективности, так и в связи с возрастающими потоками информации.

Создание автоматизированных систем безопасности полетов относится к приоритетному направлению модернизации экономики, установленному

Комиссией при Президенте РФ, «Компьютерные технологии и программы» и к приоритетным направлениям развития науки и техники «Информационно-телекоммуникационные системы» и «Транспортные, авиационные и космические системы». Основной целью при этом является повышение безопасности воздушных перевозок в коммерческих авиакомпаниях за счет перехода к превентивной системе управления рисками на основе их количественной комплексной оценки при поступлении данных в режиме реального времени с использованием программных средств математического моделирования последствий и способов предотвращения чрезвычайных ситуаций.

Автоматизированная система также должна позволять решать следующие задачи. Во-первых, определение интегральных характеристик состояния компонентов фактора «Человек (экипаж)». Во-вторых, определение интегральных характеристик состояния компонентов фактора «Машина (воздушное судно)». В-третьих, определение интегральных характеристик состояния компонентов фактора «Среда (внешняя среда)». В-четвертых, определение характеристик при пересечении факторов из всех трех групп.

Одним из новых, но уже, по мнению специалистов, очень важным компонентом безопасности, в особенности в условиях террористической опасности, является электромагнитная безопасность. Необходимость решения проблемы электромагнитной безопасности аэропортов вызвано тем, что обычно аэропорты находятся в непосредственной близости от города, а самолеты совершают маневры перед посадкой и при взлете над жилыми домами. При возникновении аварийной ситуации в результате деструктивного электромагнитного воздействия в лучшем случае экипаж самолета, как минимум, вынужден производить сброс топлива на жилые постройки, а в худшем случае происходит отказ систем управления и жизнеобеспечения самолета и его аварийная посадка с высокой степенью вероятности разрушения.

Важное место в этой работе занимает разработка методов математического моделирования электромагнитной безопасности полетов на основе принципов управления безопасностью полетов (SMS), базирующихся на системе качества. Количественная оценка рисков для эксплуатационной безопасности проводится на основе анализа информации об эксплуатационной деятельности аэропорта и формирования перечня управленческих решений из базы данных с оценкой их эффективности на основе расчета предотвращенного ущерба. Система должна выполнять: расчет риска авиационных событий и общего стоимостного риска; выявление влияющих факторов опасности в аэропорту; выдачу рекомендаций руководителю,

принимающему решение, по оптимальному набору управленческих решений; расчет остаточного риска по типу авиационного события и общего остаточного риска.

На данном этапе используется вероятностно-статистическая модель риска. Ущерб – это случайная величина с некоторой плотностью распределения. Риск выражается характеристиками этого распределения, но непараметрическая оценка плотности затруднена. Поэтому на первом этапе используется упрощенный вариант расчета одной из характеристик – математического ожидания, т.е. среднего ожидаемого ущерба как произведения вероятности авиационного события (рассчитывается по исходным данным о деятельности аэропорта) и среднего ущерба (рассчитывается по данным страховых случаев с экспертным учетом опыта авиакомпании). Экспертным путем определяются многие параметры, необходимые для реализации системы, например, минимальная величина ущерба, как характеристика события, для его учета в долгосрочном прогнозировании. Подчеркнем, что результаты краткосрочного или долгосрочного прогнозирования нецелесообразно выражать в вероятностях. Работникам авиакомпании трудно с практической точки зрения отличить, например,  $10^{-5}$  от  $10^{-6}$ . Поэтому лучше использовать стоимостные оценки риска. В рассматриваемой на первом этапе модели риск – это произведение оценки вероятности на оценку среднего ущерба (математического ожидания ущерба).

На следующем этапе разработки системы предполагается более подробно анализировать риски. В частности, изучать функции распределения случайного ущерба, строить управление на основе квантилей, близких к 1, а также медианы как дополнительного варианта среднего значения по сравнению с математическим ожиданием. Кроме того, ввести показатели разброса случайного ущерба – среднее квадратическое отклонение и межквартильное расстояние, двухкритериальную задачу снижения ущерба (одновременное снижение двух показателей – среднего ущерба и разброса) тем или иным способом сводить к однокритериальной. Кроме вероятностно-статистической модели риска, на следующем этапе в соответствии с рекомендациями ИКАО предполагается ввести в рассмотрение модель на основе теории нечетких множеств и модель с использованием интервальных математики и статистики [3]. Тем самым будет существенно расширен математический инструментарий описания неопределенностей, которые необходимо учитывать при управлении безопасностью полетов. Экспертные оценки используются в тех случаях, когда обширные статистические данные отсутствуют или в настоящее время недоступны. По мере накопления



информации в новых базах данных и извлечения необходимой информации из имеющихся баз данных экспертные оценки будут заменяться на объективные данные.

ИПУ РАН предлагается нечеткая мера интегральной значимости риска (опасности) с признаками классификации для трех ситуаций на основе двумерного показателя риска в зависимости от ситуаций.

Ситуация 1: «Риск велик» («Ущерб большой, и вероятность события достаточно велика»).

Ситуация 2: «Риск велик» («Ущерб мал, вероятность события велика»).

Ситуация 3: «Риск нулевой» («Ущерб велик, но вероятность события нулевая – событие невозможно»).

Однако оценка безопасности сложных систем через понятие риска по ИКАО [5, 6] и оценки безопасности по европейскому плану (EASp), разработанному Европейским агентством (EASA) и группой США по безопасности коммерческой авиации (CAST), включает «Метод анализа областей изменений для будущих угроз» [7].

Подход в основе своей состоит в сочетании оценки рисков по стандартным (вероятностным при наличии достаточной статистики) моделям и моделям с использованием теории нечетких множеств (когда мы не имеем статистики).

Величина риска  $\tilde{R}$  как меры количества опасности оценивается через двумерное или трехмерное множество элементов в виде:

$$\tilde{R} = \{\mu_1, \tilde{H}_R | \Sigma_0\}, \tilde{R} = \{\mu_1, \mu_2, \tilde{H}_R | \Sigma_0\},$$

где  $\mu_1$  – мера риска 1-го рода (неопределенность или случайность появления негативного результата – степень риска);  $H_R$  – мера последствий или ущерба (цена или величина риска);  $\mu_2$  – мера риска 2-го рода в системе за счет системных ошибок;  $\Sigma_0$  – условия опыта или ситуация при эксплуатации системы (класс опытности или модель системы).

Введенное трехэлементное множество не является вектором и не может быть сведено к скалярной свертке для случая катастрофических событий при  $\mu_1 \approx 0$  (в нечетких терминах).

Показатель  $\mu_2$  структурной сложности событий R при системных ошибках сценария в системе (угроза состояния системы) в рассматриваемой системе:

$$\mu_2 = \begin{cases} 0 - \text{тривиальный риск при } \mu_1 \neq 0, \\ 1 - \text{сложный риск при } \mu_1 = 0, \\ 2 - \text{сложный риск в виде цепи событий при } \mu_1 = 0 \\ \text{и т.д.} \end{cases}$$

Уровень риска задаем множеством

$$\tilde{R} = (0, \mu_1, \frac{\tilde{H}_R}{\Sigma_0}) \Rightarrow \tilde{R} \rightarrow H_R \text{ (ущерб)}.$$

Значимость рисков в пространстве событий: интегральный показатель  $\hat{R}$  с критическим значением  $R^*$ , в форме:

$$\tilde{R} \leq \tilde{R}^*, \tilde{R} \rightarrow \tilde{R}^* \Rightarrow \tilde{R}^* = \{\tilde{R}^*_{*j}\},$$

$$\hat{R} = f_R(\frac{\tilde{R}^*}{\Sigma_0}) = f_R(\mu_{1*}, \mu_{2*}, \frac{\tilde{H}_{R^*}}{\Sigma_0}).$$

При этом нельзя забывать, что поскольку процесс управления эксплуатационной безопасностью, как и процесс управления безопасностью полетов, включает в себя этапы определения угроз (источников опасности), факторов риска и этапы оценки рисков с выработкой решений, направленных на снижение рисков до приемлемого уровня, то создание баз данных по факторам угроз, опасностей, рисков и приемлемых рисков (рис. 1) также является неотъемлемой частью всего процесса.

**Фаза 1. Идентификация угроз и рисков**



**Фаза 2. Управление безопасностью полетов путем управления рисками**

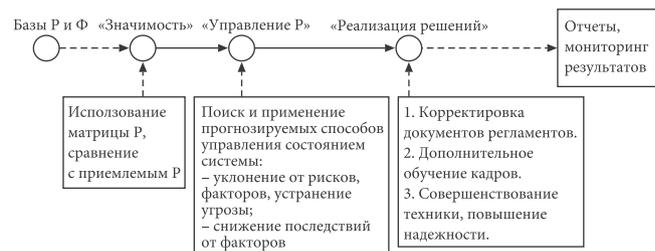


Рис. 1. Диаграмма анализа факторов риска [8, 1, 4]

Другая методология оценки будущих рисков основывается также на моделях нечетких множеств и содержится в плане европейской группы (EASp) [7]. Данная методология предусматривает процесс из восьми этапов:

- 1 этап: Определение области системы и оценки.
- 2 этап: Описание/моделирование системы и операций.
- 3 этап: Выявление угроз.
- 4 этап: Объединение опасностей в терминах риска.
- 5 этап: Оценка рисков.

6 этап: Определение потенциальных управляющих воздействий (барьеры) и оценка остаточных рисков, сравнение с приемлемым.

7 этап: Мониторинг безопасности.

8 этап: Исследование и совершенствование поиска, новые технологии.

Обобщая все вышесказанное, необходимо отметить следующее.

Для простых линейных систем риски могут быть точно предсказаны, если известны причинно-следственные связи, и все переменные могут быть измерены с достаточной точностью. Именно поэтому усталостный ресурс определенных агрегатов ВС может быть точно предсказан, если проведено достаточное количество испытаний, и имеются данные по результатам эксплуатации.

Для сложных систем сложно сделать точные предсказания. Никто не может предсказать, где и в каком контексте произойдет следующее авиационное или чрезвычайное происшествие. Но все-таки можно оценить риски или среднюю частоту и серьезность авиационных происшествий, скажем, следующие за год-два. Используя представленный подход, можно повысить уверенность, заглядывая немного дальше в будущее.

Настоящая сложность оценки будущих рисков – это не сама по себе сложность, а повышенная скорость изменений в сложных системах. Чем быстрее меняется рискованная среда, тем больше рисков остается за рамками существующих методов или их просто становится невозможно посчитать. Теперь уже меняются не только отдельные параметры, но все системы меняются с нарастающей скоростью. По этой причине вероятность/возможность потенциальных опасностей выше.

Таким образом, нельзя сказать, что будущие риски совсем нельзя оценить, но все-таки они не могут быть оценены определенно и окончательно. Мы сможем распознать нежелательные тенденции, как только они возникнут, и затем принять стратегии по минимизации их влияния, только если на ранних этапах мы подвергнем глубокому анализу все эти изменения.

В соответствии с требованиями ИКАО, каждая авиакомпания разрабатывает и совершенствует систему управления безопасностью полетов. Разработанная ГрК «Волга-Днепр» совместно с УлГУ и консультантами автоматизированная система прогнозирования и предотвращения авиационных происшествий (2011–2012 гг.) отличается гораздо более глубокой проработкой вопросов оценки, анализа и управления рисками, краткосрочного и долгосрочного прогнозирования на основе специально разработанных 14 деревьев событий с учетом многочисленных

факторов опасности в группах факторов «Человек», «Машина», «Среда». Единственным существующим в настоящее время аналогом является система CATS, разработанная по заказу правительства Нидерландов, однако эта система заметно проще, не использует объективные данные об эксплуатационной деятельности авиакомпании и ожидаемых условиях выполнения полета и позволяет решать существенно меньший объем задач по управлению безопасностью полетов. Поэтому можно констатировать, что предлагаемые в настоящей работе методы прогнозирования и предотвращения авиационных происшествий являются новой инновационной разработкой, позволяющей успешно решать ключевую в авиационной отрасли проблему контроллинга (т.е. подготовки правил принятия решений и выдачи рекомендаций руководителям по принятию управленческих решений) при управлении эксплуатационной безопасностью.

## Литература

1. Рухлинский В.М., Наумова Е.В. О количественной оценке уровня безопасности полетов в современных условиях. // Научный вестник МГТУ ГА, № 173, 2011, С. 19-24.
2. Рухлинский В.М., Малышева Л.Е. Разработка управляющих решений с целью снижения рисков возникновения авиационных происшествий до приемлемого уровня в автоматизированных системах управления безопасностью полетов. // Известия Самарского научного центра Российской академии наук, Т. 14, № 4(2), 2012, С. 359-363.
3. Шаров В.Д., Макаров В.П., Орлов А.И., Волков М.А., Санников И.А., Рухлинский В.М. Контроллинг при управлении безопасностью полетов. – Материалы II Международного Конгресса по контроллингу: выпуск № 2 / Под ред. С.Г. Фалько. – М.: НП «Объединение контроллеров», 2012. – С. 222-232.
4. Гипич Г.Н., Евдокимов В.Г., Куклев Е.А., Шапкин В.С. Риски и безопасность авиационных систем: монография. // М.: ФГУП ГосНИИ ГА, 2013. – 232 с.
5. Приложение 19 ИКАО, Издание 1, 2013 г.
6. Руководство по управлению безопасностью полетов, Doc 9859 ИКАО, Издание 3, 2013 г.
7. European Aviation Safety Plan (EASp) Action EME 1.1 «Method to Assess Future Risks», Final Deliverable, November 2012.
8. Rukhliniskiy V., Kuklev E., Malysheva L. Risks and safety of complex aviation systems. // Assembly – 37th Session, ICAO, Canada, Montreal, A37-WP/113, 28 September to 08 October, 2010. 4p.