Прогнозирование уровня безопасности авиационных систем на основе моделей рисков возникновения критических функциональных отказов

Сравнение моделей оценивания рисков в гражданской авиации и железнодорожном транспорте выявляет серьезные разночтения в интерпретации базовых понятий. Развитие системы интермодальных перевозок требует от специалистов по транспортной безопасности выработки согласованных позиций по ряду вопросов, в первую очередь — единой методики исчисления рисков. Предлагаемая авторами новая доктрина «надежность — риски — безопасность», созданная на базе теории редких событий и процедур нечетких множеств, позволяет внедрить экспертные методы оценки безопасности и проактивное управление рисками.

Е. А. Куклев,
доктор техн. наук, профессор Санкт-Петербургского государственного университета гражданской авиации

В. Г. Евдокимов,
канд. техн. наук, генеральный директор ОАО «Авиатехприемка» (Москва)

За последние 10 лет в транспортной сфере России сформировался достаточно четкий подход к оцениванию безопасности в той или иной деятельности. В его основе лежит методология исчисления рисков как характеристик опасности, потерь, ущербов и негативных последствий при возникновении особых состояний в виде функциональных отказов в сложных системах **[1]**. В гражданской авиации (ГА) РФ этот подход закреплен благодаря глобализации авиационной деятельности: национальные стандарты были скорректированы с учетом международных требований, например по ИКАО (ICAO — International Civil Aviation Organization — Международная организация гражданской авиации), FAA (Federal Aviation Administration — Федеральное управление гражданской авиации США) **[2]**. В то же время доминирующей отраслью в России является железнодорожный транспорт со своими традициями. Поэтому неизбежны нестыковки ключевых позиций и определений в сфере управления безопасностью и исчисления рисков из-за разных подходов к трактовке моделей опасности, сформировавшихся в железнодорожной отрасли и в ГА. Развитие системы интермодальных перевозок делает целесообразным поиск компромиссных решений в вопросах безопасности. Необходимо также установить взаимосвязь положений классической теории надежности (ТН), в частности методов вероятностного анализа безопасности (ВАБ), и подходов ИКАО, разрабатываемых в новом приложении Annex-19 **[3]**. Должна быть учтена и поправка № 101 ИКАО. Концепция управления безопасностью воздушных судов с учетом этой поправки уже предложена в одной из последних публикаций **[4]**.

Терминологические аспекты

Рассмотрим основные положения в рамках принятого нами подхода **[5–7]**. В ГА понятие риска выводится из положений документа Annex-19 **[3]** и **[2; 8; 9]**. В соответствии с трактовкой этой категории в глоссарии Оксфордского университета **[5]**, «риск — это возможность возникновения серьезных (негативных) последствий в предполагаемых ситуациях при условиях определения угроз заданного типа; угроза — это источник опасности». Это означает, что, по сути, рассматривается (оценивается и вычисляется) прогнозируемое количество некоторой опасности в заданном состоянии системы.

Базовым в стандарте РЖД является другое определение риска: «Риск — это потенциально существующая вероятность потери ресурсов или недополучения доходов» **[6; 7]**. Дальнейший контекст указанного определения содержит трудные для понимания сочетания, например: «вероятность реализации риска в виде…» (получается, что риск — «вероятность реализации вероятности» (?)). Можно заключить, что здесь риск — уже событие, а не его вероятность.

В тексте принятого в ОАО «РЖД» стандарта имеются и противоречия. В частности, встречаются следующие формулировки: «ущерб от наступления риска» (фраза непонятна, если принять, что риск — вероятность, а не событие); «воздействие на риск» (если риск — это вероятность или даже сочетание вероятности и ущерба, неясно, каким способом можно на него воздействовать). Формулировка «потенциально существующая вероятность» вынуждает заметить: потенциально существовать может только некоторая возможность. Понятие «вероятность» связывается с явлением типа «событие»; при этом вероятность как четкая величина может и должна детерминированно вычисляться по известным функциям распределения вероятностей (ф.р.в.) и плотностей распределения вероятностей (п.р.в.). В противном случае можно оперировать лишь с оценками вероятности, но это уже

совсем другой аппарат и инструменты, о которых в стандарте ОАО «РЖД» **[6]** не упоминается.

Таким образом, по ИКАО и по **[3; 5]**, риск — всегда вред, потеря или опасность, но не шанс. Шанс — это удача или выигрыш. Поэтому некорректно утверждать, что спекулятивный риск может быть положительным, поскольку в спекулятивных играх велик риск потерять, например, капиталы, хотя имеется и шанс получить выгоду, если играть безошибочно.

В стандарте ОАО «РЖД» **[6]** принято, что «безопасность — состояние, в котором отсутствует недопустимый риск». Это устаревший (в сравнении с ISO-8402) документ: на основе такого стандарта невозможно измерить и оценить уровень безопасности, так как математически не определено, что такое отсутствие, т. е. какова величина этого отсутствия. Как при этом оценивать уровень безопасности? По ИКАО рекомендовано измерять то, что есть — например, уровень риска, если обнаружены признаки рискового предполагаемого события R, но не его отсутствие.

В РЖД проведена уникальная по масштабам работа в области менеджмента надежности **[7]**, но четкая идея управления рисками в документах не просматривается. Так, в **[7]** записано, что корпоративная система управления рисками в ОАО «РЖД» определена как «комплекс взаимосвязанных утвержденных процедур, реализуемых на основе регламентированного взаимодействия…». Это отличается от классического определения систем управления **[10]**.

Управление, например по **[там же]**, — это целенаправленные воздействия (во времени, в пространстве) на избранный объект или систему с учетом измерения расхождения (невязки) целевой функции и измеряемой величины. Согласно **[2; 3]**, в ГА принимается, что измеряемой (проактивно, предиктивно) величиной является риск $\hat{R}$(интегральная характеристика опасности). Эта величина сравнивается с приемлемым уровнем риска $\hat{R}_*$, и определяется невязка (дефект риска) $\Delta\hat{R} = \hat{R}_* - \hat{R}$, что позволяет обеспечить управление состоянием системы с учетом значимости риска. Управляющее (корректирующее) воздействие на системы в зависимости от невязки позволяет смягчить риски, или принять их, или устранить возможность (не вероятность) возникновения в системе прогнозируемого рискового события R до того, когда это событие может произойти.

В страховом деле сумма возмещения убытков определяется заранее с учетом предполагаемых меры μ_R случайности события R и ущерба H_R. Возмещение выплачивается страхователю, если рисковое событие (страховой случай) происходит.

Примером игнорирования подобного способа управления рисками можно считать ситуацию с затоплением Крымска. Один из специалистов по ТН, выступавший по телевидению, заявил, что подобное опасное событие прогнозировалось как чрезвычайно редкое и почти невозможное. Поэтому на этапе проектирования защитных сооружений затраты на предотвращение последствий подобных событий были признаны неоправданными. Это и могло привести к крупным системным ошибкам. После наводнения страховое возмещение (очень большое) было выплачено: фактически это была плата за ошибки метода ВАБ **[1]**.

Подобные ситуации в мировой ГА практически исключены, поскольку здесь созданы и совершенствуются специальные системы управления безопасностью полетов, получившие название SMS (Safety Management System), в РФ по аналогии — СУБП (системы управления безопасностью полетов). Известны SMS, построенные на принципах управления рисками **[2; 3]**, в корпорациях Boeing, Airbus и др. Главным для них является прогноз возникновения аварий и катастроф, заложенных в систему ввиду объективного существования условий для возникновения чрезвычайно редких событий, вероятность которых близка к нулю, но которые способны причинить большой ущерб.

В ИКАО (а также в NASA и в FAA) принята концепция риска по **[2; 3; 9]** в виде:

Risk Concept: Likelihood & Severity of Harm. (1)

С учетом этого были предложены подходы **[2; 3; 5]** к оцениванию рисков по (1) на основе **[5]** и к управлению безопасностью полетов или безопасностью деятельности провайдеров услуг, включая производство и промышленное изготовление самолетов, вертолетов, двигателей, пропеллеров **[3; 9]**:

• прореактивное, реактивное воздействие, т. е. немедленная реакция на происшествие;

• проактивное, предиктивное, т. е. прогнозируемое воздействие — упреждающее управление состоянием системы по факторам риска.

В этой триаде управляющих воздействий (реактивное, проактивное, предиктивное) главным становится принятие упреждающих мер для изменения состояния системы до того, как прогнозируемое опасное событие произойдет. Изменение состояния является следствием развития сценария из предшествующих событий с начальным инициирующим событием в структурно-сложной системе **[8]**. Подобные сценарии классифицируются как функциональные отказы систем **[6]** и могут быть всегда найдены в ТН по методу дерева событий **[1; 4]** на основе стандартов и программ FMES, FTA, MMEL **[4]** и других, что нашло применение в методе ВАБ и для ГА, и для РЖД. Для этого требуется точное задание ф.р.в. (функция распределения вероятности) и п.р.в. (плотности распределения вероятностей), что при малой статистике практически невозможно. Поэтому поиск доверительных границ параметров недостаточно эффективен в задачах по проблеме редких событий. Доверительные байесовские оценки **[1]** не позволяют определять точные уровни рисков, если риск — это вероятность, как трактует его ОАО «РЖД» **[6; 7]**.

При попытках произвести оценку безопасности логистических интермодальных систем перевозок, например, в модуле «железнодорожный транспорт — авиация», придется корректировать формулировки действующих отраслевых документов и рекомендаций и приводить к единообразию подходы в ГА и железнодорожной отрасли. В рамках описываемой ниже новой доктрины «надежность — риски — безопасность» (НБР) предлагается применить процедуры нечетких множеств для оценки значимости рисков в соответствующих модулях SMS (СУБП) с учетом результатов **[9]**.

SMS (СУБП — СМБ АД) для проактивного и предиктивного управления безопасностью в транспортных системах

Назначение рассматриваемых SMS заключается в идентификации и устранении потенциальных угроз в процессах управления воздушными судами, финансами и инвестициями для достижения таких целевых результатов, как

обеспечение безопасности полетов по регламентированным показателям, получение реальной финансово-экономической выгоды, например в деятельности авиакомпании при традиционных или интермодальных перевозках.

Подобные SMS разработаны в корпорации Boeing **[8]**, в FAA **[2; 9]**, в ОАО «Аэрофлот».

Основные положения новой доктрины следующие.

В дополнение к традиционным SMS предложено принять, что в высоконадежных системах рисковые события R редкие (по вероятности ниже 10^{-6} в ф.р.в.), все они имеют почти нулевую вероятность, так как другие значения точно определить невозможно. Это позволяет обоснованно отказаться от использования трактовок риска как вероятности, которых придерживается ОАО «РЖД». События этого сорта обнаруживаются только на хвостах ПРВ и не могут быть описаны достоверно. Нет практического смысла в перемножении недостоверных величин со значениями 10^{-7}, 10^{-8}, ..., 10^{-12}, которыми оперируют исследователи в методе ВАБ.

Переход к новой доктрине НРБ позволяет узаконить применение экспертных методов оценки безопасности и проактивное (предиктивное) управление рисками возникновения негативных последствий в авиационной деятельности (возможно, и в других отраслях). Сущность этого подхода заключается в том, что некоторый здравый смысл, заложенный в понятие риска **[5]**, удастся математически ввести в теорию безопасности систем.

Соглашения, предлагаемые здесь, могут стать основой для решения рассмотренных вопросов из **[6; 7]**. Одно из конструктивных предложений состоит в первоначальном описании прогнозируемого рискового события R как случайного и измеримого при некоторых условиях Σ_0 определения системы в U — в вероятностном пространстве в обычном смысле [12]:

$$R = A_*(\omega \mid \Sigma_0, U), \qquad (2)$$

$$U = (\Omega, E, P \mid \Sigma_0), \qquad (3)$$

где E — сигма-алгебра;

P — вероятностная мера (по А. Н. Колмогорову **[12]**) элементарных случайных событий $\omega \in \Omega$ из пространства исходов Ω;

A_* — некоторое критическое событие типа класса $A_* \in A = f(E \mid \Omega)$.

Критичность $(*)$ событий $A \sim A_*$, составленных из $\omega \in \Omega$ в A (E), определяется по последствиям при функциональных отказах, но только без вероятностной меры $P_A \sim P_{A_*}$ или $P_A \sim P$ из (3). Вероятности P_{A_*} не существуют (или они не имеют смысла при событиях с почти нулевой вероятностью при недостоверных статистиках). Подобные события A_* находятся по методу дерева событий известными в ТН способами **[1; 4]**.

Выделенное множество подобных событий $\{A_{*i}\}$ строго четкое, хотя этим событиям нельзя приписать измеримость по P из (3) вследствие их «редкости». Но их функциональная четкость известна, так как они определены на булевой решетке (на «0» и «1» — в гиперкубе истинности по **[11]**). Из этого вытекает, что подмножество введенных событий $A_* = \{A_{*i}\}$ может трактоваться как универсальное множество атрибутов, для которых можно задать предикаты в виде любых предполагаемых (в предиктивном методе) свойств, в том числе ввести нечеткость их значимости по случайности появления или по другим признакам.

Предлагается разделить A из U в (3) на две части $A = A_0 \cup \Delta A$, $\Delta A = A_*$, ввести по **[11]** нечеткие подмножества $A_* \to \underset{\sim}{A}$ и нечеткую алгебру $\underset{\sim}{E}_R$:

$$U \to \underset{\sim}{A}(\omega, \underset{\sim}{M}_R \mid \Sigma_0, \underset{\sim}{E}_R), \qquad (4)$$

где A — область (подмножество) четких (по функциям) событий из U;

$A_* = \{A_{*i}\} \sim E \subset U$ — множество критических событий (четких функциональных отказов);

$\underset{\sim}{M}_R$ — множество мер нечеткости (вследствие случайности) и значимости критических функциональных отказов, взятых из универсального множества A_* с учетом нечетких оценок меры количества опасности (риска) типа: «риск мал», «риск велик», «риск значимый», «риск приемлемый».

Нечеткая мера μ_1 случайности появления рискового события R будет: «редко», «очень редко», «часто», «нечасто», «иногда», что позволяет применять известные матрицы оценки рисков по FAA, МЧС и т. д. и избавиться от некорректного понятия «прогнозируемая (угадываемая) вероятность события», что было отмечено в **[8]**. В качестве иллюстрации данной схемы ниже приводятся соотношения из **[там же]** для математического представления идеи (1) ИКАО:

$$\tilde{R} = (\mu_1, H_R \mid \Sigma_0),$$

$$\hat{R} = \hat{f}(\tilde{R} \mid \Sigma_0) = \hat{f}(\mu_1, H_R \mid \Sigma_0), \qquad (5)$$

где $\hat{R}$ — интегральная оценка уровня риска (количества опасности, как предложено выше) в виде функции от двухэлементного множества в $\tilde{R}$;

H_R — ущерб.

При этом понятие скаляра — среднего риска, некорректного при редких событиях, исключается из рассмотрения, что затруднительно сделать в ВАБ. Но (5) — универсальное соотношение, где μ_1 может быть и вероятностью по ВАБ, если доступна достоверная статистика.

Некоторые различия в подходах к оценке безопасности интермодальных перевозок (в модуле «ГА — РЖД») могут быть наиболее корректно устранены на основе методов нечетких множеств.

Представленные нами результаты сравнения моделей исчисления рисков в транспортных системах следует рассматривать как предварительную иллюстрацию возможной схемы решения актуальных вопросов, поскольку в статье были использованы только доступные и в ограниченном объеме источники информации о стандартах ОАО «РЖД». Т

Литература

1. Аронов З. И., Александровская Г. Г. и др. Безопасность и надежность технических систем. М.: Логос, 2008.
2. Руководство по обеспечению безопасности полетов (РУБП). Doc. 9859, AN/460. ИКАО (Монреаль). М.: Минтранс РФ, 2009.
3. Annex 19 — Safety Management. AN-WP/8715. ICAO. 0.12.12.
4. Ливанов В. Н., Новожилов Г. В., Неймарк М. С. Система управления безопасностью полета ОАО «ИЛ» (СУБП «ИЛ»). М.: Авиасоюз, 2013.
5. The Little Oxford Thesaurus. OUn. USA. 1994. ISBN 0-19-869221-8.
6. Порядок идентификации опасностей и рисков. Стандарт ОАО «РЖД». М.: СТО РЖД 1.02.033-2010.
7. Порядок определения допустимого уровня риска. Стандарт ОАО «РЖД». М.: СТО РЖД 1.02.035-2010.
8. Смуров М. Ю., Куклев Е. А., Евдокимов В. Г., Гипич Г. Н. Безопасность полетов воздушных судов гражданской авиации с учетом рисков возникновения негативных событий // Транспорт Российской Федерации. 2012. № 1 (38). С. 48–52.
9. Safety Management Manual. FAA. Washington. 2012.
10. Большая советская энциклопедия. 3-е изд. Т. 27. М., 1977. С. 129.
11. Рыбин В. В. Основы теории нечетких множеств и нечеткой логики. М.: МАИ, 2007.
12. Прохоров Ю. В., Розанов Ю. А. Теория вероятностей. М.: Наука, 1987.