

Управление рисками в системах обеспечения безопасности полетов воздушных судов в режимах RVSM

С помощью систем типа Safety Management System (SMS) возможно оперативное управление параметрами текущих ситуаций в режимах полета на суженных эшелонах (RVSM) и проактивное назначение показателей безопасности транспортного уровня (TLS) в задачах с редкими событиями.



Е. А. Куклев,
доктор технических наук, профессор, заведующий
кафедрой механики СПбГУ ГА, директор Центра
экспертиз научных проектов (ЦЭНС)



С. А. Исаев,
доктор физ.-мат. наук, профессор СПбГУ ГА



Я. М. Далингер,
канд. техн. наук, заведующий кафедрой прикладной
математики, проректор по информатизации
и региональному образованию СПбГУ ГА

В настоящее время поиск путей совершенствования систем обеспечения безопасности на воздушном транспорте определяет содержание соответствующих научных разработок по режимам полета воздушного судна (ВС) на суженных эшелонах (RVSM). В области развития технических и технологических подходов реализации RVSM необходимо создание средств компенсации последствий от поражающих воздействий внешней среды на объекты и системы инфраструктуры воздушного транспорта. Главным здесь является разработка принципов и методов оценивания уровня безопасности полетов ВС и решение проблемы safety при редких событиях [1].

В основе подхода к оцениванию степени совершенствования систем обеспечения безопасности лежат два основных принципа регулирования деятельности на транспорте:

- принцип мониторинга, предполагающий мониторинг состояния системы с использованием соответствующих расчетных и инструментальных процедур и технических средств;
- принцип управления безопасностью.

Здесь же следует упомянуть принципы профилактики происшествий путем прогнозирования рисков катастроф, инцидентов и конфликтов при RVSM [там же], применение которых возможно на основе процедур упреждения [2].

Эффективность управления ВС по RVSM, в том числе в авиакомпаниях [там же], оценивается с позиций рисков, которые при этом трактуются традиционно на основе понятия «вероятность» из теории надежности (ТН).

В Международной организации гражданской авиации (ИКАО — ICAO) применялись модели конфликтов в виде CRM (Collision Risk Model). Был выполнен грант ИКАО [2] (автор М. Фуджита, Токио),

выявлена проблема оценивания ошибок вычисления в CRM малых значений вероятностей событий с аргументами на «хвостах» функции плотности распределения вероятности (ф.п.р.в.), т. е. та же самая, что для полетов ВС.

Необходимо отметить, что в [1] для обеспечения безопасности полетов при RVSM предлагается создавать SMS (Safety Management System), но обращается внимание на то, что научной задачей является синтез функций распределения ошибок расчетов в форме TSE (Total System Errors Distribution) при использовании формул Райха [там же].

В связи с этим в данной статье ставится задача оценить чувствительность формулы Райха к ошибкам исходных данных и предлагается скорректировать концепцию CRM на основе терминов и определений ИКАО, а именно, чтобы риск понимался как количество прогнозируемой опасности в состояниях системы при возникновении угрозы, которая может вызвать появление опасного (рискового) события [3].

Схема оценки чувствительности формулы рисков по Райху

Для оценки риска для двух ВС при параллельных эшелонах за основу принимается формула из [1] (Reich-type formulate) в виде:

$$N_{ay} = N_x \cdot P_y(S_y) \cdot P_z(0) \left(1 + \frac{\lambda_x |y|}{\lambda_y |x|} + \frac{\lambda_y |z|}{\lambda_z |x|} \right), \quad (1)$$

где N_{ay} — риск конфликта как ожидаемое число фатальных инцидентов за 1 час полета в связи с нарушением разведения ВС;

$P_y(S_y)$ — вероятность бокового перекрытия траекторий полета;

$P_z(0)$ — вероятность вертикального перекрытия;

λ_i — геометрические общепринятые параметры ВС и соответствующие средние скорости в проекциях на оси избранной системы координат.

По рекомендации ИКАО с помощью этой формулы можно вычислить ожидаемое число катастроф на один час полета при RVSM.

В связи с (1) возникает вопрос, почему ИКАО отстает от своих рекомендаций [2] в сфере организации воздушного движения и называет риском скаляр — среднее число прогнозируемых конфликтов за 1 час полета. Обоснование этому дано ниже в формулах (2), (3).

Конфликты, принятые в качестве основной характеристики моделей опасности для двух самолетов на смежных эшелонах полетов, рассматриваются как угроза нормальному полету. Для оценки уровня угроз используется показатель допустимого уровня опасности при заданной категории угрозы в виде показателя TLS (Transport Layer Security — безопасность транспортного уровня), который нормируется ИКАО для разных регионов мира, в частности для режимов RVSM в Европе. При этом принято называть величину N_{ay} риском. Эта величина зависит от вероятностей $P_y(S_y)$, $P_z(0)$, которые достаточно малы (до 10^{-5}), и, очевидно, определяются с некоторыми ошибками, что составляет суть метода поиска решений из [1].

Влияние ошибок распределения указанных в (1) величин и неопределенность значений скоростей движений ВС (в проекциях) могут быть причиной ошибок прогнозируемых значений TLS, т. е. пропуска неожиданных конфликтов. Например, диспетчер и пилоты совершают ошибки вследствие проявления человеческого фактора; навигационное оборудование ВС дает информацию с ошибками и т. п. Указанные факторы в силу случайности имеют неизвестные распределения, что снижает точность вычислений и приводит к некорректности решения диспетчера.

ИКАО рекомендует использовать в задачах (1) только четкие законы ф.п.р.в.: гауссов закон и экспоненциальное распределение. В [1] для этих рекомендаций предлагаются CRM и заявляется право на авторство. Трудности, которые при этом возникают, можно обойти на основе предложений [4].

Анализ принципов построения моделей опасности в ТН и теории системной безопасности (ТСБ)

Этап интенсивного развития ТН в основном завершился, поскольку методы обеспечения высокой надежности систем по нормативным показателям качества с нормативным уровнем остаточного риска (по вероятности рискованного события) уже жестко регламентированы соответствующими стандартами. Многие проблемы ТН (теоретические и технические) практически решены. Существует математическая ТН сложных систем (Р. Барлоу, Ф. Прошан, Б. В. Гнеденко, М. А. Каштанов, Е. Ю. Барзилович, И. А. Рябинин, И. З. Аронов и др. [там же]), в рамках которой:

- разработаны процедуры и методики расчета нормативных показателей надежности [там же];
- созданы стандарты, справочники, регламенты, определены технические нормативы, организовано техническое обслуживание систем и объектов, действуют системы поддержания (функциональной) летной годности авиатехники в гражданской авиации, отлажена индустрия контроля, мониторинга состояния изделий и диагностики систем (по техническому состоянию);
- отработаны принципы создания высоконадежных систем и агрегатов и т. п.

Однако при этом возникла необходимость решения новой проблемной задачи настоящего времени, которая состоит в исследовании систем и обеспечении их безопасности с позиции теории рисков с учетом нормативного приемлемого уровня риска возникновения аварий и катастроф в гражданской авиации на основе последних рекомендаций ИКАО (ANNEX-19 и SARPS).

Фактически возникает проблема оценки такого явления, как возможность возникновения случайных событий, не с помощью вероятности, которую невозможно вычислить, а на другой основе (например, в проблеме редких событий) — Fuzzy Sets.

С физической точки зрения в ТН потребительское качество систем достигается за счет обеспечения необходимых свойств, из чего вытекают следующие понятия [2]:

- «надежность» (безотказность) — потребительские качества с позиций работоспособности изделия (качества, которые являются главными для потребителя);
- «безопасность» (гарантированная по уровню или по категории «защищенность») — состояние, в котором в процессе эксплуатации возможный вред или ущерб для пользователя при эксплуатации изделия вполне приемлемый;
- «состояние» — такое текущее изменение параметров процессов в системе при наличии угроз, когда негативное событие еще не произошло (не возникло), но из-за возникшей угрозы может произойти. В этом случае возможно возникновение негативных последствий для пользователя. Точно так же оценивается

«опасность», но через показатели состояния на этапе прогнозов, когда никакого реального процесса еще не возникло.

В прогнозах предполагается возникновение потенциальной угрозы и оценивается (прогнозно) возникновение прогнозируемых последствий.

В ТН все методы апостериорны и базируются на проведенных ранее экспериментах и результатах опытов. Именно поэтому вероятностная оценка P_A события A (благоприятного) является неслучайной и известной через аналитические четкие описания в виде функции распределения вероятностей (ф.р.в.) и ф.п.р.в. В этом случае применяется *вероятностный анализ безопасности* (ВАБ) [5] как разновидность и продолжение ТН в область определения значений малых вероятностей событий. Однако в ВАБ достоверно определять малые значения вероятностей принципиально трудно, так как (по положениям ТН) отсутствует необходимый апостериорный базис данных.

Здесь мы принимаем другую, отличную от принятой в ВАБ формулировку понятия риска — более универсальную и базирующуюся на физическом смысле рассматриваемой категории. За основу предлагается принимать трактовки из американских глоссариев, используемых в документах ИКАО, в частности в ANNEX-19.

Значимость рисков предложено оценивать на основе двухмерной модели оценки риска (формулы Е. А. Куклева — аналог концепции ИКАО, но в математическом виде [3; 4]) и принять соотношения:

$$\tilde{R} = (\mu_1, H_R | \Sigma_0), \quad (2)$$

$$\hat{R} = \hat{f}(\tilde{R} | \Sigma_0) = \hat{f}(\mu_1, H_R | \Sigma_0), \quad (3)$$

где μ_1 — мера риска 1-го рода, обозначающая неопределенность (или случайность) появления (возникновения) рискованного события R с негативным результатом H_R , например [6];

H_R — мера последствий или ущерба (цена риска — тяжесть вреда);

Σ_0 — условия опыта или ситуация при эксплуатации системы (класс опасности и модель опасности системы типа CRM, дерево событий, граф смены состояний, состояния катастрофических отказов системы по методу минимальных сечений отказов (по Ю. А. Рябинину, Н. А. Махутову));

\hat{R} — интегральный риск (при нечетких оценках по [3]), т. е. количество опасности в заданном состоянии [4].

Из (2), (3) вытекает, почему в ИКАО величина N_{av} (и т. п.) названа риском, хотя по стандартам (и в ранних публикациях ИКАО) риск определялся как «вероятность негативного события». Дело в том, что математически (1) дает, согласно (3), средний риск — скаляр как средний ущерб. Если принять новое определение ИКАО (ANNEX-19, DRAFT), в соответствии с которым риск есть возможность последствий и серьезного ущерба, то получится (3), но для заданной вероятности событий. В связи с этим и для системы организации воздушного движения предлагается применять универсальные понятия (2), (3).

Проблема управления рисками

К концепции риска [1; 2; 5] могут быть высказаны следующие замечания:

- даны различные определения риска («риск — среднее число катастроф», «риск — вероятность», «риск — двумерное понятие»), имеются несогласованные определения в матрице рисков понятий possibility and likelihood (Possibility or Likelihood are not the same. There are some contradictions, which are inadmissible);
- не разработана концепция редких событий и скрытых недостатков или катастроф с вероятностью «почти ноль».

Схема решения задачи

Последовательно рассматриваются структура SMS [2] и модели рисков [3; 4], которыми можно управлять.

Предлагаемые модели рисков (дополнительно к CRM из [1]) основаны на определениях понятия «риск», взятых из документов Госстандарта-Р и ИКАО.

В принятых моделях считается, что риск — это опасность или количество опасности (с нечеткой мерой) в состоянии, когда возможно (прогнозируется) дискретное рисковое событие R , которое может быть или не быть в опытах или при испытании систем.

Предложенные формулировки дают возможность использовать математическую модель рискового события (дискретного) с двумя свойствами:

- случайность (или частота) появления события при некоторых условиях, например, обозначенных в виде Σ_0 ;
- нежелательные последствия или потери (с ущербом для изучаемой системы).

Интегральная оценка \hat{R} , зависящая от двух свойств рискового события, может быть получена, если принять, что оценка \hat{R} риска — это множество из двух показателей; μ_1 — характеристика частоты и неопределенности появления нежелательного (рисковог) события, например, в виде $\mu_1 = \mu_p$ — вероятность; μ_1 — статистика; μ_1 — коэффициент риска по ИКАО [3] в виде частоты катастроф, нормированных ко времени работы (в часах налета ВС), к числу взлетов и посадок в виде нормы 10^{-6} (млн).

Введенные понятия адекватно отражают смысл таких высказываний, как, например, «полет на самолете связан с определенным риском для жизни», т. е. с опасностью; или «имеется риск серьезного заболевания ...» и т. д.

Применение понятия «риск» в смысле «количество опасности» более предпочтительно в задачах, связанных с оценкой убытков, ущербов и т. п., поскольку при этом дается ориентир для разработки вычислительных процедур. В задачах по RVSM это будет наиболее продуктивно, так как TLS* вычисляются по Райху с большой ошибкой, но TLS фактически нельзя получить практическим путем.

Предлагается показатель TLS, вытекающий из (1), считать допустимой нормой, т. е. приемлемым риском по [2]:

$$TLS \rightarrow TLS^*,$$

где * — критичность.

В таком случае это и будет приемлемое (допустимое), например по [там же], количество опасности в форме среднего числа катастроф за 1 час полета двух ВС на заданных эшелонах.

Из формулы (1) видно, что это простая модель типа CRM, но в предположении, что «два шара» (к примеру, два ВС) движутся навстречу друг другу (или иначе) и могут столкнуться. Никакого управления в этой формуле не предусмотрено, что не соответствует действительности. И если учесть, что TLS* вычисляется просто путем манипуляций с четкими формулами в виде ф.р.в., ф.п.р.в., которых тоже нет, а есть только нечеткие функции этого вида, то подобная модель CRM должна быть скорректирована, например, по [3].

Вывод

В ситуации диспетчерского управления движением ВС при стратегии RVSM методологическая основа оценивания безопасности полетов через показатели рисков конфликтов ВС на эшелонах подтверждает необходимость развития новых подходов из ANNEX-19 для нормирования TLS. Нечеткость исходных данных также приводит к необходимости корректировки моделей типа CRM. ■

Литература

1. Fujita M. Frequency of Rare Event Occurrences. ATN/CNS. Tokyo. Japan. EIWAC. 2009.
2. Doc. 9859 AN/470 Руководство по управлению безопасностью полетов (РУБП). 2-е изд. ИКАО, 2009.
3. Куклев Е. А. Оценка рисков катастроф в высоконадежных системах // Труды 13-й Межд. конф. «Проблемы управления безопасностью сложных систем». ИПУ РАН. М.: 2005. С. 55–57.
4. 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. 54–58.
5. Аронов З. И., Александровская Г. Г. и др. Безопасность и надежность технических систем. М.: Логос, 2008.

Подходы к решению задач траекторного управления в активной системе организации воздушного движения

Практическими задачами, в основе решения которых лежит концепция траекторного управления, являются, например, такие как тактическое планирование и организация потоков воздушного движения, формирование и регулирование потоков прилетающих и вылетающих воздушных судов (ВС) в районе аэродрома. В будущем в основу прогноза траекторий в интегрированных системах организации воздушного движения (ОрВД), скорее всего, ляжет использование траекторных данных, рассчитываемых бортовыми системами управления. Но в ближайшей и среднесрочной перспективе в автоматизированных системах ОрВД будут использоваться траекторные данные, рассчитываемые модулями наземного базирования [1].