

РИСК-ОРИЕНТИРОВАННЫЙ ПОДХОД К УПРАВЛЕНИЮ БЕЗОПАСНОСТЬЮ СЛОЖНЫХ СИСТЕМ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ АНАЛИЗА КРИТИЧНОСТИ ЭКСПЛУАТАЦИОННЫХ СИТУАЦИЙ

Е.А. Куклев

Санкт-Петербургский государственный университет гражданской авиации
Россия, 196210, Санкт-Петербург, ул. Пилотов, 38
E-mail: ekuklev@mail.ru

Ключевые слова: редкие события, уравнение катастрофы, риск, шанс.

Аннотация: В статье оцениваются уровни состояния безопасности систем с применением подхода Fuzzy Sets – без использования вероятностных показателей возможности возникновения негативных событий в исследуемых системах. Введены «индикаторы безопасности» в форме интегральных уровней риска поражения сложных систем от внешних воздействий. Применена расчетная схема вычисления индикаторов на основе риск-ориентированного подхода ИКАО-НАСА (ICAO - NASA).

1. Введение

Устанавливается единство взглядов на проблемы безопасности в сферах финансов, военных операций, экологии, техногенных проектов, в теории безопасности полетов ВС и в области борьбы с глобальным терроризмом. Даются основы теории «принятия решения в условиях неопределенности», что пока еще недостаточно освещено в публикациях. Вопросы комплексной безопасности систем с редкими событиями наиболее эффективно решаются по схемам NASA (НАСА) и ICAO (ИКАО). Это объясняется тем, что классические показатели (вероятностные) могут быть недостоверными при недостаточных объемах статистических данных о редких событиях, например, в обстановке с угрозой проявления «терроризма». Вероятностный анализ безопасности (ВАБ) не содержит решения указанных методологических проблем. Целью работы является обоснование необходимости внесения ряда компромиссных поправок (корректировок) в российские стандарты по менеджменту безопасности систем на основе риск-ориентированного подхода [1]. Это относится к принятию решения вопроса в стандартах по оценке уровней безопасности об отказе от понятия , что «риск-это вероятность возникновения неблагоприятного события с «ущербом» для рассматриваемой системы». Действительно, «вероятность» – это статистически детерминированное число, позволяющее измерить «количество случайности» на основе моделей Гаусса. В задачах «с редкими событиями» (с вероятностью «почти ноль») целесообразно переходить к методам Fuzzy Sets и к построению моделей сложных систем, определенных на нечетких

подмножествах с помощью недистрибутивных булевых решеток- «по шкале «Беркли» (NASA). Суть вопроса в том, что предлагается устранить некорректность известных деклараций об управлении безопасностью или рисками при их традиционной трактовке по ВАБО в форме: «риск – это вероятность возникновения негативного события». Комплексные показатели оценки качества различных систем определяются при риск-ориентированный подходе на множестве величин, заданных в разных топологических пространствах для разнородных факторов опасности. Перспективные разработки базируются на нечеткой булевой логике ситуационного анализа событий с применением имитационных моделей, но без Метода – Монте Карло, без математических ожиданий, дисперсий и функций плотностей распределения вероятностей (п.р.в.). Главным является составление уравнения катастрофы в виде функции конъюнкций логических переменных для обнаруженных превентивно сценариев развития критических ситуаций, отражающих «пути к катастрофе» (по Рябинину И.А.) на минимальных сечениях функциональных отказов систем. В сфере экономики уже в 2005 г. было принято и доказано, что безопасность систем следует оценивать с помощью сценариев событий и без понятий о вероятностях событий, если соответствующая статистика отсутствует [2] – Шеломицкий А.Г.

Актуальность темы и риск-ориентированный подход в современной трактовке (по NASA-ICAO [3] основан на применении нечеткой логики развития ситуаций в системах и является единственным инструментом исследования безопасности полетов и анализа антагонистических конфликтов при редких событиях без применения ВАБ, но в рамках так называемого метода Fuzzy Sets. Только риск-ориентированный подход и его, в некотором смысле, эквивалент в форме минимакса, могут обеспечить корректное прогнозируемое (проактивное) управление состояниями систем на основе анализа результатов мониторинга факторов риска при угрозах различного типа. Некорректность № 1 при ВАБ – «неприменимо для «редких событий»; некорректность № 2 – «недопустимое применение понятий «вероятность риска» (забавно: «вероятность вероятности события»).

2. Предпосылки

«Безопасность» рассматривается как «состояние системы», в которой «риск» возникновения «ущерба» (заданного вида) мал в сравнении с приемлемым уровнем риска прогнозируемого вреда или ущерба персоналу, имуществу при заданных условиях функционирования системы и при «четкой» (ясной) определенной угрозе нарушения штатного состояния системы, т.е. при угрозе безопасности. В работах Центра ГА в Нидерландах (в Амстердаме, Нидерланды) автором Levinson Nancy, 2013 [4], объявлено, что старая концепция «РИСКА» по ИКАО может быть скорректирована в соответствии со смыслом понятия «состояния» опасности и неопределенного (или нечеткого) элемента – типа события. «Риск» – это не событие, а степень и мера предполагаемого (прогнозируемого) вреда (опасности) при вполне определенной (заданной) угрозе с набором опасных факторов [5]. Простота основной идеи БЕЗОПАСНОСТИ сформулирована в формуле ИАТА (1):

(1) $ABC - (able\ BE\ careful).$

Ранее (ошибочно) на основании стандарта ИСО 31000 (ИАТА и др.) было сформулировано: «РИСК- ЭТО РЕЗУЛЬТАТ ВОЗДЕЙСТВИЯ НА СИСТЕМЫ НЕКОТОРОЙ НЕОПРЕДЕЛЕННОСТИ», что должно быть исправлено. В действительности на системы могут воздействовать только физические возмущения с определенными параметрами, которые, конечно, могут быть и неизвестны заранее и быть четкими или нечеткими,

но от этого их воздействия на системы не меняются. Новая модель описания концепции риска по ИКАО на основе идеи о редких событиях имеет вид [1]:

(2) *Risk Concept: Likelihood & Severity of Harm.*

При новом подходе в теории БП по формуле (2), согласно NASA к Fuzzy Sets, удастся устранить ряд некорректностей и противоречий в документах по ВАБ. При редких событиях понятие среднего риска (через произведение малой вероятности на значение большого ущерба) не имеет практического смысла. Из (2) вытекает, что риск по NASA – это нечеткая «Мера количества опасности, которая оценивается через «матрицу риска» и «индикаторы», отражающие результаты нечеткой импликации элементов некоторого универсального множества (базового носителя информационного модуля). Из этого вытекают соотношения или сочетания элементов L (likelihood) и H (ущерб) из (2), которые могут быть заданы только в виде пар элементов, но никак не в виде скалярного произведения «вероятности» и «ущерба», дающих «средний риск», который так распространен в ВАБ. (Здесь по (2) – это грубая ошибка), т.к. знак & – это символ логической операции (and), дающий комбинацию в виде пары элементов (a,b), что и отражено в матрицах анализа рисков по NASA, Boeing, ..., МЧС и в др.. При этом удастся установить иерархию определений риска, угроз, факторов опасности, точек уязвимости, систем, точек риска, рисков события, точек бифуркации процессов (возможности появления опасных событий типа рискованных событий), профилактика угроз с учетом факторов опасности.

3. Постановка и схема решения задачи

Необходимо сконструировать на основе (2) имодель риска по NASA как «прогнозируемого нечеткого количества опасности» \hat{R} и составить формулу рискового события R, позволяющую определять и интегральное значение введенной нечеткой величины риска \hat{R} , и индикаторы опасности $I(\hat{R})$ – при необходимости. При таком подходе целесообразно определять понятие риска как «меры опасности» на основе концепции «Малинецкого Г.Г.» и «Буркова С.А.» [5]. Такой подход оказывается более экономичным и обеспечивает применение метода конструирования прогнозируемых «сценариев нечетких ситуаций», задаваемых «уравнениями катастрофы» в виде «конъюнкций факторов» с четким набором признаков факторов и критичностью сценария. Но мера возможности подобного сценария является нечеткой (неопределенной или «неистинной») – по Л. Заде [1]), что адекватно отражает ситуацию с событиями, возникающими «с вероятностью «почти ноль»». Метод Монте-Карло при этом как инструмент исследований свойств случайных процессов полностью исключается, как не имеющий смысла (случайные процессы по «Гауссу» в разрабатываемых моделях отсутствуют, т.к. изучаются события с вероятностью «почти ноль»). Предлагается новое универсальное определение понятия риска (на основе теории нечетких подмножеств из некоторых универсальных множеств элементов, составляющих сложные системы без вероятностных показателей для редких событий (при вероятностях событий – «почти ноль»). Понятие рискового события R естественно выводится из (2): функционально это событие всегда описывается достоверно (истинно – через функции реальных элементов системы системы). Но свойства этого события – негативные и нечеткие по возможностям возникновения с мерой μ [5] последствий в виде ущерба HR. Событие R – это класс событий (из СИГ-МЫ АЛГЕБРЫ F), составленный из элементарных событий (из случаев ω – «омега») в виде:

$$(3) \quad R = R(\zeta | \mu, H_R, L_R, \Sigma_0),$$

где ζ – первый аргумент, задающий механизм и форму неопределенности заданного вида γ_i из известного классификатора ИПУ РАН [5]; μ – нечеткая мера возможности возникновения рискованного события в виде потери функции системы с ущербом Σ_0 – условия сценария развития процесса в виде цепи (пути); $(|)$ – знак свойства события которое задается в (3) условиями, характеризующими эти события. При этом LR – цепь событий из σ -сигмы алгебры, $E(\Omega)$ – некоторое функциональное пространство исходов Ω , задаваемого в аксиоматике Колмогорова А.Н. – в вероятностном пространстве. Но подобное пространство здесь рассматривается как усеченное, как было показано выше, поскольку оно не существует на множестве нечетких событий, возникающих с вероятностью «почти ноль» – без априорных вероятностей, подобное пространство теперь заменяется некоторой системой типа «алгебра» с набором стандартных операций, представленных в Fuzzy Sets. Устанавливается нечеткое множество \tilde{R} : прогнозируемая опасная нечеткая рискованная ситуация – с учетом значимости нечетких оценок количества опасности в заданном состоянии Символ \tilde{R} обозначает значимость или критичность цепи событий – в форме R , ведущих к катастрофе с уровнем \hat{R} так, как это принято на практике:

«риск большой», «...малый», «...приемлемый», «...незначительный»...

Формула для определения интегрального уровня риска \hat{R} как количества опасности будет

$$(4) \quad \hat{R} = \hat{f}(\hat{R}|\Sigma_0) = \hat{f}(\mu, \tilde{H}_p|\Sigma_0).$$

Нечеткая мера μ – появления рискованного события задается по схеме НАСА в виде: «очень редко», «иногда», «редко», «нечасто», «часто» и т.п. Но этот уровень \hat{R} надо оценить по схеме выбора нечетких предпочтений, хотя бы по [2]. Мера μ и индикаторы риска при данном подходе выражаются через «Количество опасности» \hat{R} в виде функции от принятого двухэлементного множества типа кортежа \tilde{R} для исследуемой нечеткой ситуационной модели прогнозируемой рискованной обстановки

$$(5) \quad \tilde{R} \rightarrow \hat{R} : \rightarrow \hat{R} = \hat{f}(\tilde{R}|\Sigma_0) = \hat{f}(\mu, H_R|\Sigma_0 L_R).$$

Понятие скаляра – «среднего риска», иногда применяемого на основе (2) в авиации, некорректно, если события, обозначаемые как редкие типа гауссовых $R(\xi)$, имеют свойства (3). Из (3) видно, что мера μ - нечеткая, которую невозможно вычислить в ВАБ при отсутствии статистики по μ , поскольку появление рискованного события R из (3) происходит с вероятностью «почти ноль». При этом используются матрицы оценки рисков [2, 3] – по NASA, FAA, МЧС [5]. Поэтому некорректное понятие «прогнозируемая» («угадываемая») вероятность события не должно применяться.

Термин «вероятность непоявления катастрофы» – некорректный и недопустимый. В соответствии со здравым смыслом понятий «состояния» опасности или безопасности системы и элемента типа «события» принимаются основные определения:

а) «Катастрофа» (как явление и возможное событие) заложена в систему и только ждет своего проявления (Дж. Ризон, проф. MIT – NASA) [5].

б) «Риск» – это не событие, а степень и мера предполагаемого (прогнозируемого) «количества» вреда (опасности) при вполне определенной (заданной) угрозе Z_R с набором опасных факторов $\varphi_i \in \Phi = \{\varphi_i|\Sigma_0\}$.

в) Недопустимо (нельзя) заменять понятие «возможности» традиционным понятием «вероятность», т.к. вероятность это уже мера количества случайности возникновения событий в гауссовых моделях. По определению, вероятность – это статистически детерминированная мера количества случайности возникновения событий в гауссовых моделях.

4. Расчетные схемы в аксиоматике рисков по Fuzzy Sets

Основная задача, связанная с поиском «окон уязвимости», вытекает из сущности методов многокритериальных оценок свойств систем единого обобщенного показателя типа «эффективность», «надежность», «безопасность», «уязвимость», «приемлемость», «экономичность», «эргономичность», «конкурентоспособность» и т.п. [5]. Конструируется «Уравнение катастрофы» (по методу минимального сечения) в виде конъюнкций факторов опасности или отказов систем, приводящих к функциональному отказу [5]. Вводятся функции алгебры логики (четкие и нечеткие) событий; определяющих пути (цепи) к катастрофе (или к конфликту). Структура цепи L_R – четкая, т.к. это – сценарии [5]: их много, в общем случае это множество – счетное, что не имеет никакого значения при оценке интегрального уровня рисков \hat{R} составленное в виде набора (конъюнкции) логических признаков факторов φ_i . Условие $U_R = 1$ обозначает катастрофу:

$$(6) \quad R \rightarrow L_R \Rightarrow U_R = (\varphi_1 \wedge \varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_k) = 1.$$

Это обозначает, что при вполне определенной угрозе Z_R , возникающей в точке уязвимости и, по-существу, определяющей нечеткую длину интервала уязвимости, в конце каждого интервала происходит бифуркация (разветвление и обрыв процесса) в виде события R – неудачи (катастрофы, аварии) или «невозникновение» этого события, но возникновение события обратного – в виде B – удачи (шанса выживания). Таким образом, прогнозируемое количество опасности \hat{R} всегда соответствует выделенной угрозе, и оно должно быть найдено заранее до прогнозируемого момента времени возникновения бифуркации, т. е. события R . Из этого следует, что условия возможного возникновения рискового события задаются уравнением U_R в форме четкой функции алгебры логики от логических переменных φ_i – факторов, составляющих угрозу Z_R :

$$U_R = (\varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_k),$$

где φ_i – факторы, но определенные в форме логических переменных, которые по обозначению знака дают признак прогнозируемой причины или условия, которые определяют возможность возникновения катастрофы. Возможно введение более сложного уравнения катастрофы типа комплекса условий для альтернативных вариантов возникновения класса событий типа R_Σ в виде дизъюнкции конъюнкций:

$$U_{R\Sigma} = V U_{Ri} = V_j (\varphi_0 \wedge \varphi_1 \wedge \varphi_2 \wedge \dots \wedge \varphi_k).$$

Логическое значение $U_R = 1$ обозначает возможность осуществления катастрофы при указанных условиях.

5. Заключение

Определено основное (новое по стандарту) понятие риск – обобщенная мера количества опасности в прогнозируемых (проактивных) рисковом событиях в состоянии опасности для избранной системы.

Список литературы

1. Гипич Г.Н., Куклев Е.А., Евдокимов В.Г., Шапкин В.С. Риски и безопасность авиационных систем | Монография. М.: ФГУП ГосНИИ ГА, 2013. 232 с.
2. Aviation Security Global Risk Context Statement. Montreal: ICAO, 2016.
3. Younosy A. 10 Things You Should Know about SMS. Washington: FAA, 2012.

4. Малинецкий Г.Г., Кульба В.В., Косяченко С.А., Шнирман М.Г. и др. Управление риском. Риск. Устойчивое развитие. Синергетика. М.: Наука, 2000, 431 с.
5. Шоломицкий А.С. Теория риска. (Выбор при неопределенности и моделирование риска). М.: ВШЭ, 2005.
6. Kuklev E., Zhilinskiy V. Accident Risk Assessment for Highly Reliable Aviation Systems in Emergency Situations // Transport and Telecommunication. 2018. Vol. 19, No. 1. P 59-63. DOI 10.2478/ttj-2018-0006.