УДК 629.7.017.1

КОНЦЕПЦИЯ ЭКСПЛУАТАЦИОННОЙ МОДЕЛИ ОТКАЗОБЕЗОПАСНОСТИ

С.А. КРОТОВ

Статья представлена доктором технических наук, профессором Смирновым Н.Н.

Предлагается рассмотреть формальное описание эксплуатационной модели отказобезопасности с возможностью коррекции и адаптации параметров при выполнении полетных циклов воздушных судов с учетом непредвиденных событий.

Ключевые слова: отказобезопасность, формирование модели, контроль состояния**.**

На протяжении всего периода эксплуатации самолет должен отвечать существующим требованиям норм летной годности, в том числе требованиям при отказах функциональных систем, представленных в нормативной документации (АП 25.АО, АП 25.1309, FAR 25.1309, CS 25.1309). При этом под оценкой уровня отказобезопасности или оценкой отказобезопасности следует понимать оценку выполнения требований указанной нормативной документации [1]. Однако основное внимание к выполнению таких требований уделяется на стадии проектирования и сертификации воздушного судна (ВС) [2], поэтому ниже предлагается рассмотреть вопросы удовлетворения некоторых требований в процессе эксплуатации ВС. В частности, перед каждым вылетом должны соблюдаться определенные требования, определяемые как условия допуска ВС к эксплуатации. Данные требования главным образом касаются текущего состояния самолетного оборудования, вида (назначения) полета, а также беспрепятственного выполнения необходимых работ по техническому обслуживанию.

Несоответствие эксплуатационным требованиям перед или во время полета, помимо угрозы безопасности полета, может вызвать значительные задержки и привести к тяжелым экономическим последствиям.

Структура полетного цикла

После каждой посадки ВС подготавливается к следующему полету. Самолет инспектируется на предмет выявленных замечаний в ходе полета. Если какой-либо компонент находится в неработоспособном состоянии, решение о выпуске ВС основывается на требованиях к следующему полету. Командир ВС ссылается на утвержденный документ – перечень минимального оборудования (MEL), в котором указываются компоненты со статусом «Допускается» (Go), «Допускается, если» (Go if) и «Не допускается» (No go).

Компоненты со статусом «Допускается» могут оставаться в неисправном состоянии в течение ограниченного периода времени. При этом необходимо принять во внимание возможность последующего критического отказа и его влияние на безопасность полета.

Статус «Допускается, если» подразумевает допустимым наличие неисправного компонента при подготовке ВС к вылету в случае соблюдения условий допуска к эксплуатации и/или специальных ограничений:

«Go-if-o» - данный статус отсылает к порядку действий экипажа ВС;

«Go-if-m» - данный статус отсылает к порядку действий группы технического обслуживания.

Наличие компонентов со статусом «Не допускается» является основанием для запрета полетов.

Основной проблемой является возможность оценить в процессе эксплуатации способность ВС соответствовать установленным требованиям с учетом непредвиденных событий различного рода и своевременно предпринять корректирующие действия для предотвращения неблагоприятной ситуации. Поэтому возникает необходимость иметь контроль над состоянием ВС, чтобы с высоким уровнем достоверности предотвращать события, которые могут возникать в процессе эксплуатации.

В настоящее время активно развиваются программные продукты информационного обеспечения безопасности полетов, надёжности и технической эксплуатации авиационной техники [3]. Широкий спектр поставленных задач способствует скорейшему внедрению в авиации передовых автоматизированных систем и информационных технологий.

Общее описание модели

В данном разделе предлагается рассмотреть структуру модели контроля состояния ВС в процессе эксплуатации [4] с учетом вышеуказанных требований по отказобезопасности. Описание представлено в универсальном виде, которое в дальнейшем может использоваться в языках программирования AltaRica [5] и SAN.

Установим два вида исходных требований:

- минимальные требования (Min_Sys_Req) – требования из документа MEL, которые должны всегда соблюдаться независимо от миссии ВС;
- требования к конфигурации миссии ВС (M_Prof_req) – непосредственно относятся к самому полету.

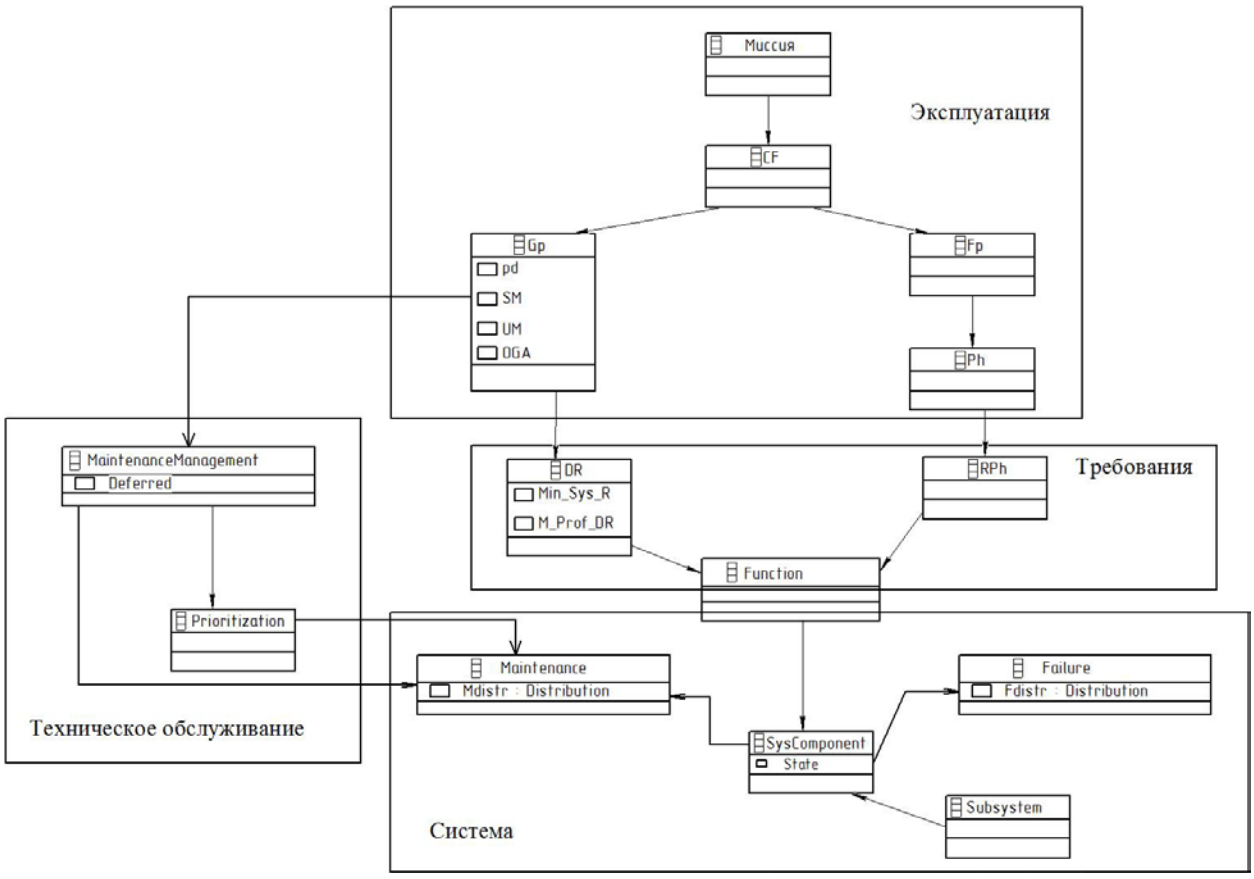

Рисунок. Общее описание модели

На рисунке представлена структура модели, состоящей из четырёх уровней: «Эксплуатация», «Требования», «Система» и «Техническое обслуживание». Рассмотрим поочередно каждый из уровней.

Уровень «Эксплуатация». Здесь и в дальнейшем под «миссией» ВС будем понимать обеспечение ряда полетов для реализации назначенного полетного задания, которые успешно достигаются при рассмотрении и выполнении всех требований предполетного периода на земле и самого полета (полетный период), и состоящие из этапов взлета, полета по заданному маршруту, маневрирования для решения поставленной задачи вылета, возврата на аэродром посадки и посадки [6]. Обозначим предполетный период как Gp (ground period), а полетный период – Fp (flight period). Связь CF=(Fp, Gp) или CF=F·P будет представлять процесс выполнения полета, начиная с действий по подготовке к полету и заканчивая самим полетом. В дальнейшем оператор «•» будет обозначать последовательность действий или интервалов. Миссия ВС состоит из n полетов и определяется следующим выражением: $M = \bullet_{i=1..n} CF_i = \bullet_{i=1..n}(Gp_i,Fp_i)$. Каждый полет может быть разложен на несколько этапов, которые различаются по функциональным возможностям систем ВС, необходимых для успешного выполнения этапа полета. Принимая, что для каждого полета может быть определено *p* этапов, имеем: $Fp=Ph_1 \bullet Ph_2 \bullet \ldots Ph_p$. Каждый этап имеет продолжительность DPh_j.

Обозначим *I* как возникновение какого-либо нарушения во время миссии, это может касаться как самого полета, так и предполетного периода. Нарушение в полете определяется как возникновение нарушения на одном из его этапов. При этом нарушение при выполнении какого-либо этапа определяется потерей полного соответствия требованиям при выполнении данного этапа полета. На данном уровне удовлетворение требованиям фазы Ph_i представляется через булевы переменные RPh_i.

Во время каждого предполетного периода должно быть обеспечено полное соответствие необходимым требованиям, чтобы выполнить следующий полет. Во избежание задержек, все необходимые процедуры должны быть выполнены в установленный срок. Предполетный период может состоять из: а) планового технического обслуживания (SM) и других наземных процедур обслуживания (OGA) или б) планового ТО с последующими процедурами внепланового ТО (UM).

Соответственно каждый предполетный период может быть выражен следующим образом: Gp = SM•UM•OGA. Длительность операций SM и UM зависит от рабочего состояния определенной системы и средств технического обслуживания и ремонта (ТОиР). Процедуры внепланового ТО (UM) обычно возникают при несоответствии условиям допуска ВС к полету (DR). В таких ситуациях, как правило, восстанавливаются компоненты критических систем, необходимых для выполнения полета. Предполетный период имеет определенную длительность pd(Gp), выход за рамки которой обуславливает возникновение задержки полета. Из вышесказанного следует, что для определения уровня «Эксплуатация» модели требуются следующие данные:

- количество полетов *n*, составляющих миссию ВС;
- количество *p* этапов, составляющих полет и их продолжительность DPh_j;
- продолжительность предполетного периода pd(Gp).

Уровень «Требования». Данный уровень описывает требования, которые должны быть удовлетворены для успешного выполнения миссии ВС, определенной в уровне «Эксплуатация», принимая во внимание разделение миссии на последующие полетные и предполетные периоды. Здесь также учитываются требования сохранения отказобезопасности.

Успешное завершение этапов Ph_j полета обуславливается доступностью группы функций f_1, $f_2 \ldots f_{nj}$, выполняемых системой ВС. Таким образом, доступность данных функций сопоставима с удовлетворением требований во время каждого этапа для обеспечения благополучной эволюции ВС. Данные требования, определяемые как RPh_i, могут устанавливаться через булевы выражения, выражающие комбинацию функций, которые должны обеспечиваться для выполнения соответствующего этапа. Кроме того, установленные требования могут выражаться через со-

четание функциональных потерь, которые могут привести к нарушениям на определенном этапе полета.

Требования к допуску ВС, которые должны удовлетворяться во время предполетного периода, могут быть определены схожим путем. Таким образом, установленные требования, обозначенные через булевы выражения, определяются: а) доступностью некоторых необходимых функций f_1, f_2,… f_{nf} и б) возможностью выполнения некоторых задач ТО (обозначим как Ма) в течение запланированного периода pd(Gp): $DR_i = f(f_1, f_2,\ldots f_{nf}, Ma)$.

Обобщая вышесказанное, требования представляют собой сочетание функций, необходимых на эксплуатационном уровне, позволяющих отправить ВС в полет или успешно завершить полетный этап. Требования, установленные для миссии ВС, состоящей из n полетных циклов, являются результатом объединения требований каждого цикла данной миссии. Для полноценного полета CF_i параметры DR_i и $RPh_{j=1...p}$ представляют собой требования, относящиеся к наземной и полетной фазам. Для требований допуска ВС DR_i требуемые функции абсолютно такие же, как и для успешного выполнения полета. Таким образом, мы собрали требуемые сочетания функций, необходимых для каждого полета, и обозначили как Min_Sys_Req. Также мы установили дополнительные требования $M\_Prof\_DR_i$, характерные для рассматриваемой миссии ВС. Данные требования могут относиться к доступности некоторых функций или выполнению работ по техническому обслуживанию, необходимых для выпуска ВС. Таким образом $DR_i = Min\_Sys\_R \wedge M\_Prof\_DR_i$.

Требования, выраженные через булевы выражения, основываются на исправности системных функций. Доступность каждой функции выводится через анализ исправности и способности компонентов систем выполнять поставленные задачи. Распределение между состояниями системных функций и состояниями компонентов систем обеспечивается на системном уровне модели. Более точно функция характеризуется её состоянием, которое определяется условным функционированием исходя из состояния системных компонентов. В дальнейшем будем использовать обозначение $f_{k=1,2,..} = g\ (C_1S, C_2S, \ldots C_{nk}S,)$, где C_1S, C_2S, … $C_{nk}S$ являются переменными, отображающими информацию о состоянии компонентов, задействованных в выполнении функции f_k; g является функцией, формулирующей связь между состояниями компонентов и функцией f_k.

Уровень «Система». Система может быть рассмотрена как ряд компонентов C_1 с различными взаимосвязями между собой. Каждый компонент подвергается событию возникновения отказа и процедурам ТО. В более общем смысле состояние компонента C_1, обозначенное как C_1S, может принимать различные значения, определяемые некоторой областью C_1SD. C_1SD может разделяться на два пространства C_1SD = Operational (C_1SO) ∪ Failed (C_1SF) (рабочее и неисправное). События возникновения отказа и работы по ТО в дальнейшем определяются как изменения значений параметров состояния соответственно от C_1SO к C_1SF и от C_1SF к C_1SO. Описание должно также включать задание распределения вероятностей, описывающее возникновение событий отказов (обозначим как F*distr$_i$)*, а также длительность работ по ТО (обозначим как M*distr$_i$)*. Как правило, для таких событий, характеризуемых интенсивностью отказов λ(t) и интенсивностью восстановления μ(t), принимается экспоненциальное распределение. Также должна быть определена стратегия ТО с установленным уровнем приоритета, касающегося каждого компонента для определения порядка работ ТО при нескольких отказавших компонентах. Таким образом, из вышеописанного следует, что к рассматриваемым характеристикам системных компонентов относится их состояние, закон распределения отказов и закон распределения длительности обслуживания.

Уровень «Техническое обслуживание». Работы по ТО при каждом предполетном периоде характеризуются доступностью ресурсов, а именно рабочими (техниками) и запасными изделиями. Рассматривая обслуживание каждого системного компонента C_1, мы принимаем во внимание воздействие функции MI_{Gp}, которая используется для определения дополнительной временной задержки, определяемой наличием средств ТОиР, необходимых для выполнения конкретных за-

дач во время предполетного периода. В случае отказа нескольких компонентов может применяться работа по очередности, принимая во внимание установленный уровень приоритета.

Сопряжение уровней модели

Связь между уровнем «Эксплуатация» и уровнем «Требования» обеспечивается перечнем требований $((RPh_1, \dots RPh_p)_i, DR_i)_{i=1\dots n}$ в соответствии с этапами полета и предполетными интервалами.

Связь между уровнем «Требования» и уровнем «Система» обеспечивается перечнем функций ($f_1, f_2, \dots f_{nf}$), предоставляемых системой. Сопряжение между уровнями «Система» и «Техническое обслуживание» определяется средствами ТОиР, оказывающими влияние на ТО (MI_{Gp}) системных компонентов. Сопряжение между уровнями «Техническое обслуживание» и «Эксплуатация» определяется информацией о текущем предполетном интервале и возможностью дальнейшего допуска ВС к полету.

Возможные изменения и коррекция модели

Рассмотрим изменения в различных уровнях.

Уровень «Эксплуатация». Изменения касаются определения количества n полетов, параметров каждого полета и предполетного интервала. К параметрам полета относится распределение длительности для этапов Ph_1, $Ph_{1, \dots} Ph_p$. Для предполетного периода параметры относятся к общей продолжительности наземных работ по ТОиР, вычислению длительности плановых работ (SM) и других наземных процедур (OGA).

Уровень «Требования». При изменении параметров миссии ВС функции, необходимые для осуществления полетов, в новом профиле миссии тоже меняются. Описание требований прежде всего состоит из определения сочетаний предустановленных функциональных возможностей. Требования могут указываться посредством выбора ряда ранее установленных параметров или с помощью ввода оператором комбинаций, основанных на выполняемых функциях.

Уровень «Система». К изменениям в системе относятся начальное состояние компонентов, законы распределения отказов и параметры технического обслуживания. Для состояния компонентов определяются изменения параметров в заданной области значений. Для распределения отказов и ТО рассматриваются новые вероятностные функции или их новые значения параметров, чтобы лучше представлять распределение возникновения событий.

Уровень «Техническое обслуживание». В данном уровне корректируется функция влияния технического обслуживания MI_{Gp} на предполетный интервал, включенный в миссию ВС.

Коррекция и адаптация структуры (описания) модели

С внешней точки зрения все изменения будут рассматриваться как изменения конфигурации миссии ВС, состояний компонентов, прогнозирования отказов и определения длительности ТО. Изменение конфигурации миссии ВС вероятнее всего будет включать изменения в нескольких уровнях модели. Это может относиться к уровням «Эксплуатация», «Требования», «Техническое обслуживание». Изменение состояния компонента и прогноза отказов относится к уровню «Система». Внедрение изменений в модель будет происходить с учетом уточнений от внешнего оператора или процесса. Рассмотрим структуру уточнения модели.

Конфигурация миссии ВС. Коррекция новой конфигурации основывается на полете, который предстоит выполнить. Все полетные и предполетные периоды должны указываться в очередности их выполнения. Коррекция конфигурации будет происходить следующим образом.

Детализация полета:

- указание ранее определенного полета, если профиль полета был определен;
- определение нового профиля полета:
  - указание дополнительных требований выпуска ВС (M_Prof_DR);

- указание этапов полета Ph_1, $Ph_{1, \dots}$ Ph_p. Для каждого этапа необходимо указать:
  - длительность DPh_i: оператор указывает расчетное время или функцию распределения вероятности, характеризующую DPh_i;
  - установленные требования, определенные через булевы выражения.

Для уточнения требований оператор может выбрать требования, относящиеся к предустановленному полету или определить самостоятельно, комбинируя перечисленные функциональные зависимости с помощью операторов «И», «ИЛИ», «НЕТ».

Детализация предполетного интервала:

- указание планируемой длительности;
- определение длительности планового ТО (SM);
- определение длительности других наземных процедур обслуживания.

Детализация политики ТО:

- необходимо указание списка функций (MI_{Gp1}, $MI_{Gp2 \dots}$ MI_{Gpn}) в соответствии с предполетными интервалами, включенными в конфигурацию миссии ВС. Функция влияния технического обслуживания не может быть задана бригадой технического обслуживания. Вычисление должно основываться на информации о доступности техников и времени, необходимого для ремонта типовых компонентов.

Состояние компонента:

- необходимо указание нового значения параметра для состояния компонента. Это можно производить через процесс диагностирования компонента, что позволит узнать о состоянии компонента и предоставит информацию о текущем состоянии. Данные могут быть введены непосредственно через оператора.

Прогноз отказа компонента и длительность работ по ТОиР:

- рассматривается описание распределения событий. Новое распределение отказов и длительности ТО могут указываться оператором. Указывается расчет времени до наступления события, который может быть использован в качестве параметров для заданной вероятностной функции.

Конечная модель прежде всего состоит из исходной модели, которая должна дополняться в текущем режиме на основании развития событий. Исходная модель состоит непосредственно из модели системного уровня. В ней представлены только компоненты, структура которых не будет меняться. Таким образом, модель системного уровня построена и все функции, которые могут использоваться на уровне требований, определены. Поскольку требования Min_Sys_Req являются общими для всех миссий, независимо от их конфигураций, они также представлены на уровне требований в исходной модели. Субмодели системного уровня формируются исходя из состояний компонентов основной системы, а распределения событий в роли параметров должны задаваться в конечной модели. Соответственно субмодель системного уровня является выходным параметром состояния функций, необходимых для выражения требований. Требования Min_Sys_Req должны сочетаться с дополнительными требованиями конфигурации миссии ВС, которые должны указываться, основываясь на функции $f_{k=1,n}$ при рассмотрении эксплуатационного уровня. Данная исходная модель параметризируется с учетом информации о начальных состояниях и распределении отказов согласно модели, которая будет использоваться для оценки системной надежности (используя вероятность удовлетворения требований Min_Sys_Req в течение заданного периода).

Выводы

Представленное описание эксплуатационной модели отказобезопасности позволяет контролировать состояние ВС в процессе эксплуатации, учитывая специфику предполетных и полетных интервалов. Уровни модели охватывают спектр важнейших задач на различных этапах эксплуатации, в том числе позволяют заложить требования по отказобезопасности ВС с даль-

нейшим контролем их выполнения. Возможность коррекции и адаптации модели позволяет повысить эффективность процесса технической эксплуатации. Таким образом, представленная модель реализует в некоторой мере принципы системы поддержания летной годности ВС.

ЛИТЕРАТУРА

1. Гершман Ю.С., Неймарк М.С. Проблема полноты оценки уровня отказобезопасности воздушных судов // АвиаСоюз. - 2013. - № 46. - С. 50-52.

2. Кротов С.А. К вопросу о контроле отказобезопасности функциональных систем воздушных судов в процессе эксплуатации // Научный Вестник МГТУ ГА. - 2013. - № 197. - С. 79-84.

3. Ерусалимский М.А. Время действовать. Международная конференция по информационным технологиям поддержания летной годности // АвиаСоюз. - 2006. - № 2. - С. 26-27.

4. Tiassou K., Kanoun K. Online model adaptation for aircraft operational reliability assessment, 6th International Congress, Embedded Real Time Software and Systems, Tolouse: France (2012).

5. Seguin C., Bieber P. Formal assessment techniques for embedded safety critical system. 18th IFIP World Computer Congress, Topical Day on New Methods for Avionics Certification, August 26th, 2004, Tolouse (France).

6. Капитонов С.А. Разработка логической модели безопасности полета летательных аппаратов на основе непосредственного учета функциональных признаков его элементов и систем // Проблемы безопасности полетов. - 2009. - № 3. - С. 27-32.

OPERATIONAL FAIL-SAFE MODEL CONCEPTION

Krotov S.A.

The article considers operational fail-safe model formal description with possible updating and adaptation of parameters during flight cycle accomplishment taking into account unforeseen events.

Key words: fail-safe, model formation, condition monitoring.

Сведения об авторе

Кротов Станислав Александрович, 1989 г.р., окончил МГТУ ГА (2011), аспирант МГТУ ГА, автор 1 научной работы, область научных интересов – эксплуатация воздушного транспорта, поддержание летной годности воздушных судов.