УДК 629.735

В.С. ПОХИЛ, А.В. ХАРЫБИН

Военный институт телекоммуникаций и информатизации НТУУ «КПИ», Украина

МЕТОД АНАЛИЗА И ОЦЕНИВАНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ АВИАЦИОННЫХ БОРТОВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ

Приведен аналитический обзор понятия функциональной безопасности. Отмечена важность рассмотрения функциональной безопасности как свойства информационно-управляющей системы (ИУС) объекта критического применения. Предложен метод анализа критичности отдельных элементов и оценивания функциональной безопасности бортовой ИУС авиации. Рассмотрен пример проведения анализа критичности отдельных элементов и оценивания функциональной безопасности бортовой ИУС на примере подсистемы связного и вычислительного оборудования самолета Ан-148.

Ключевые слова: *бортовая информационно-управляющая система, функциональная безопасность, риск, метод анализа и оценки, критичность элемента.*

Введение

В последнее время количество полетов в гражданской авиации значительно возросло, и интенсивность воздушного движения продолжает увеличиваться. Существующие авиационные бортовые информационно-управляющие системы (БИУС) не в состоянии обеспечить уровень абсолютной безопасности полетов, как судов гражданского воздушного флота (ГВФ), так и любых других летательных аппаратов в сложившихся условиях, о чем свидетельствует статистика аварий и катастроф судов ГВФ. БИУС летательных аппаратов (ЛА) являются системами критического применения, так как частичная или полная потеря ими работоспособности во время полёта приводит к авариям или катастрофам, имеющим высокую степень тяжести последствий.

В результате анализа безопасности полетов ЛА ГВФ в РФ за 2008 год сделаны выводы, что [1]:

– возросло число происшествий в бизнес-авиации с 55 в 2007 г. до 69 в 2008 г., а число авиакатастроф со смертельным исходом возросло с 17 до 24;

– в частной легкомоторной авиации произошло увеличение авиационных происшествий с 15 в 2007 г. до 29 в 2008 г., из них 14 авиакатастроф закончились гибелью 24 человек;

– в сегменте турбовинтовых самолетов количество катастроф увеличилось в более чем два раза с 5 в 2007 году до 12 в 2008 году.

Безопасность полётов согласно [2] определяется способностью авиационной транспортной системы осуществлять воздушные перевозки без угрозы для жизни и здоровья людей. При рассмотрении вопросов безопасности полётов следует учитывать весьма ощутимые потери, которые несёт общество от авиационных происшествий: не поддающийся подсчёту социальный ущерб, связанный с гибелью людей; чистые экономические потери (потери техники, компенсация за утерянное имущество и т. п.); потери вследствие уменьшения доверия к воздушному транспорту. Это приводит к необходимости проведения научно-исследовательских и опытно-конструкторских работ, направленных на повышение уровня функциональной безопасности БИУС ЛА, в основе которых лежит анализ и оценивание указанного свойства.

Целью данной статьи является описание нового метода анализа и оценивания функциональной безопасности БИУС ЛА гражданской авиации.

1. Функциональная безопасность и стандарты МЭК серии 61508

При рассмотрении аспектов безопасности принят постулат, что абсолютной безопасности не существует – после принятия защитных мер некоторый остаточный риск всегда остается. Безопасность достигается путем уменьшения риска до допустимого уровня, определенного как допустимый риск. В технические средства уменьшения риска могут входить электрические, электронные и программируемые электронные (Э/Э/ПЭ) устройства, оборудование и системы, связанные с безопасностью (ССБ), в том числе оборудование, находящееся под управлением (ОПУ). Уменьшение риска может быть достигнуто и с помощью других систем, связанных с безопасностью, либо внешних средств. Уменьшение риска происходит благодаря выполнению функции безопасности.

Термин «связанный с безопасностью» (safety-related) используется для описания систем, которые

обязаны выполнять определенную функцию или функции для гарантии того, что риски будут удержаны на допустимом уровне. Такие функции, по определению, являются функциями безопасности (safety function).

Функциональная безопасность (functional safety) – часть общей безопасности, которая относится к оборудованию, находящемуся под управлением (ОПУ), и систем ОПУ и зависит от правильности функционирования электрических, электронных, программируемых электронных (Э, Э, ЭП) систем связанных с безопасностью, систем обеспечения безопасности, основанных на других технологиях и внешних средств сокращения риска [4].

Для достижения функциональной безопасности необходимо выполнение двух типов требований: требование к функции безопасности (что функция выполняет), а также требование к полноте безопасности (вероятность удовлетворительного и безотказного выполнения функции безопасности).

Стандарты МЭК серии 61508 регламентируют различные аспекты функциональной безопасности систем Э/Э/ПЭ, обеспечивающих безопасность. В Российской Федерации в качестве национальных стандартов в 2007-2008 гг. приняты русскоязычные аналоги стандартов МЭК указанной серии, получившие обозначения ГОСТ Р МЭК 61508 – приведены в [2 – 6]. Для обеспечения функциональной безопасности БИУС ЛА в целом на ранних этапах их жизненного цикла необходимо определять степень критичности отдельных элементов (подсистем), которые могут вызвать нарушения или ухудшение работы систем, что позволит определить перечень компонентов и средств управления ими, безотказности и функциональной безопасности которых нужно уделять особое внимание при проектировании [7].

2. Метод анализа критичности отдельных элементов и оценки функциональной безопасности БИУС

В работе [8] был предложен метод оценивания живучести информационно-управляющих систем, который позволяет учесть различность функциональной критичности и объектовой живучести элементов и подсистем ИУС. Понятия и характеристики функциональной безопасности систем близки к понятиям теории надежности и живучести. Отличие состоит в том, что в показателях указанных свойств учитываются все реализации опасных отказов, а в характеристиках функциональной безопасности рассматривают и учитывают только отказы, приводящие к катастрофическому ущербу. Статистически таких отказов может быть меньше, чем учитываемых при оценке надежности и живучести. Однако, методы, влияющие факторы, реальные показатели надежности и живучести могут служить ориентирами при анализе и оценке функциональной безопасности БИУС критического применения.

2.1. Модель бортовой информационно-управляющей системы

Структурно-топологическое построение БИУС задается графом G, вершинам а которого соответствуют вычислительно-коммуникационные узлы (бортовое связное, вычислительное, управляющее оборудование) и шины обмена данными (сигналами) между ними.

2.2. Анализ критичности отдельных элементов БИУС с позиций функциональной безопасности

Данная операция основана на требованиях по проведению анализа критичности отказов элементов сложных систем, изложенных в [7] и содержит в своём составе четыре основных этапа.

В общем случае для рассматриваемых БИУС возможно три основных вида отказов элементов (подсистем):

– отказы, не влияющие на выполнение функции безопасности (критичной функции) той или иной подсистемы или БИУС в целом;

– отказы, приводящие к ухудшению точностных и/или временных характеристик выполнения критичной функции подсистемой, но не приводящие к опасному состоянию БИУС или к катастрофическим последствиям объект, в котором используется данная система – отказы приводящие к частично-работоспособному состоянию БИУС;

– отказы, приводящие к критическому состоянию функциональную подсистему БИУС, непосредственно связанную с её функциональной безопасностью, что неизбежно приводит к катастрофическому ущербу для объекта управления.

На первом этапе производится анализ критичности множества функций {F} выполняемых системой, с параллельным разложением графа БИУС на частные подграфы G’ содержащие все элементы, которые участвуют в реализации функций безопасности (ФБ) БИУС, нарушение выполнения которых может привести к катастрофическим состояниям системы. Качественные характеристики выполнения этих ФБ будут определяющими для свойства функциональной безопасности системы.

На втором этапе каждая из данных ФБ подвергается разложению на множество простых задач $\{Z_n\}$ (процессов), выполнение которых отдельными элементами (блоками, узлами, устройствами) обеспечивает работу подсистемы, связанной с этой ФБ.

Третий этап анализа заключается в определении кратности использования отдельных элементов подсистем БИУС в решении критических задач (КЗ), обеспечивающих выполнение соответствующих ФБ. При этом для каждого из i подграфов G'_n формируются матрицы критичности $M_{KPn}(z_{jn},a_k)$ элементов a_k входящих в их состав.

Элементы данных матриц m_{jk} на пересечении строк, соответствующих определенным КЗ z_{jn}, со столбцами, соответствующими элементам a_k анализируемого подграфа, заполняются числовыми значениями в соответствии со следующими правилами:

1) если отказ элемента a_k для данной КЗ z_{jn} относится к виду 1, то значение элемента m_{jk} матрицы $M_{KPn}(z_{jn}, a_k)$ равно 1;

2) если отказ элемента a_k для данной КЗ z_{jn} относится к виду 2, то значение элемента m_{jk} матрицы $M_{KPn}(z_{jn}, a_k)$ равно 0,5;

3) если отказ элемента a_k для данной КЗ z_{jn} относится к виду 3, то элемент m_{jk} матрицы M_{KPn} (z_{jn},c_k) принимает значение 0;

4) если для выполнения данной КЗ z_{jn} используются d параллельно включенных однотипных структурных элементов a_k, входящих в анализируемый подграф G_n, то соответствующий элемент m_{jk} матрицы $M_{KPn}(z_{jn}, a_k)$ примет значение в d раз меньшее значения, определяемого по правилам 1 – 3.

Четвертым этапом анализа является определение количественного значения показателя кратности критичности – v_k для всех структурных элементов a_k каждой из i функциональных подсистем БИУС. Определение количественного значения v_k проводится в следующей последовательности:

1) определение абсолютного значения величины критичности $m_{\Sigma k}$ элемента a_k n-й подсистемы БИУС путём суммирования значений всех элементов m_{jk} k-го столбца матрицы критичности $M_{KPn}(Z_{jn}, a_k)$;

2) вычисление суммарного значения критичности $m_{\Sigma n}$ всех элементов a_k n-й подсистемы БИУС путём суммирования значений $m_{\Sigma k}$ всех элементов a_k, образующих эту подсистему;

3) расчет нормированного значения степени критичности каждого элемента a_k n-той подсистемы БИУС – показателя кратности критичности v_k согласно выражению:

$$v_k = \frac{m_{\Sigma k}}{m_{\Sigma n}}. \qquad (1)$$

Результатом проведения АКОЭ БИУС в соответствии с предложенной методикой будет i одномерных массивов $V_n(a_k)$, содержащих значения показателя кратности критичности v_k всех элементов критичных подсистем БИУС, связанных с функциями безопасности.

2.3 Оценивание функциональной безопасности БИУС ЛА

Для проведения операции оценивания функциональной безопасности БИУС в целом необходимо провести оценивание данного свойства для всех функциональных подсистем, каждая из которых представлена набором элементов, отвечающих за выполнение соответствующей функции безопасности.

Оценивать функциональную безопасность Fs отдельной функциональной подсистемы БИУС, выполняющей одну из ФБ (f^*_n), предлагается согласно выражению:

$$Fs(f^*_n) = 1 - v_{\Sigma n}\cdot R_n, \qquad (2)$$

где $v_{\Sigma n}$ – удельная суммарная критичность n-той подсистемы БИУС, выполняющей ФБ, определяемая аналогично выражению (1), но для полного множества ФБ системы; R_n – риск, связанный с ФБ, определяемый:

$$R_n = P_{on}\cdot U_n, \qquad (3)$$

где P_{on} – вероятность эксплуатационного отказа n-той функции безопасности, U_n – нормированный в пределах [0, 1] показатель ущерба, возможного при отказе ФБ.

С целью определения нормированного значения ущерба используются следующие правила:

1) если в результате отказа ФБ подсистемы БИУС ЛА однозначно наступают катастрофические последствия, связанные с гибелью людей, значение нормированного показателя ущерба U_n равно 1;

2) если в результате отказа ФБ подсистемы БИУС ЛА возможно наступление катастрофических последствий, но существует компенсирующая ФБ, выполняемая другой подсистемой БИУС либо сочетанием БИУС и членов экипажа, то значение нормированного показателя ущерба Un равно 0,75;

3) если в результате отказа ФБ подсистемы БИУС ЛА возможно наступление катастрофических последствий, но существует компенсирующая аналогичная ФБ, выполняемая другой подсистемой (резервный контур), то значение нормированного показателя ущерба U_n равно 0,5.

2.4. Пример анализа критичности отдельных элементов и оценки функциональной безопасности подсистемы связного и вычислительного оборудования БИУС Ан-148

В качестве примера применения предложенного метода и соответствующих ему показателей рассмотрим процесс АКОЭ и оценки функциональной безопасности (ОФБ) подсистемы связного и вычислительного оборудования (ПСВО) БИУС, устанавливаемой на самолетах типа Ан-148 (рис. 1) [9].

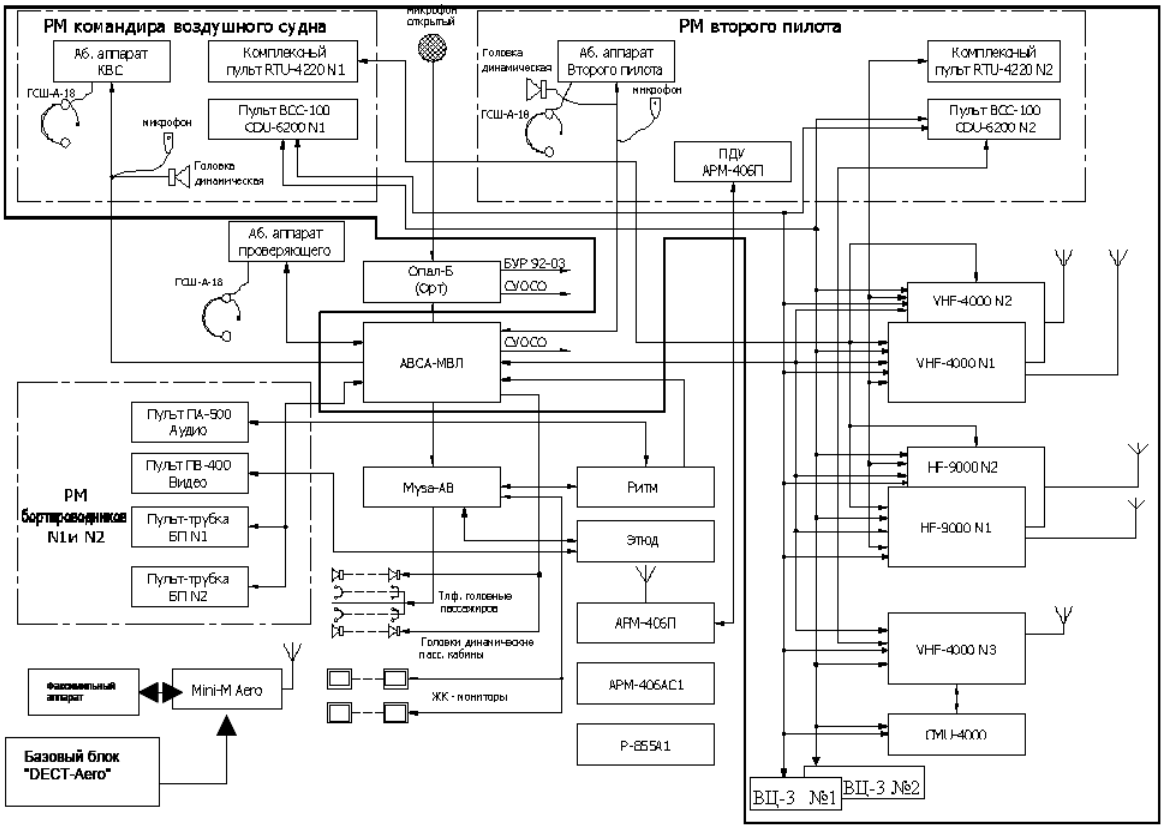

Рис. 1. Структурная схема подсистемы связного и вычислительного оборудования БИУС Ан-148

С использованием предложенного метода необходимо провести АКОЭ и ОФБ важной с точки зрения функциональной безопасности подсистемы БИУС. На первом этапе проводится анализ критичности множества функций, выполняемых данной подсистемой, с целью выделения ФБ. Для рассматриваемой ПСВО БИУС Ан-148 можно выделить такие ФБ:

f^*_1 – расчет, формирование, индикация параметров на CDU для обеспечения автоматического или ручного выдерживания режимов оптимальных по критериям максимальной дальности, максимальной продолжительности полета;

f^*_2 – создание пользовательской базы данных методом ручного ввода с CDU и оперативное изменение плана полета через CDU;

f^*_3 – автоматический полетный контроль собственной работоспособности ВСС-100, а также контроль линии связи с отображением на CDU;

f^*_4 – централизованное управление радиосвязным оборудованием в автоматическом и ручном режиме;

f^*_5 – вычисление и индикация времени пролета контрольных точек запрограммированной траектории (ППМ) и точке на ортодромии, заданных координатой S от текущего ППМ, из условий выполнения полета на оптимальных режимах с учетом информации о текущем состоянии аппаратуры по маршруту, полученных от служб УВД;

f^*_6 – вести двухстороннюю телефонную симплексную радиосвязь с диспетчерскими пунктами аэропортов или с диспетчерами УВД, в зоне которых находится самолет и экипажами других самолетов;

f^*_7 – осуществлять обмен данными и свободными текстовыми сообщениями со службами УВД (данные о метеоусловиях, о разрешениях, выдаваемых службами УВД, данные диспетчерской службы и службы технического обслуживания).

В состав рассматриваемой подсистемы (рис. 2) входят следующие элементы, участвующие в обеспечении указанных ФБ: аппаратура передачи данных (модем) CMU-4000 с радиостанцией УКВ диапазона типа VHF-4000 №3, бортовые вычислители ВЦ-3 №1, №2 вычислительной системы самолетовождения (ВСС-100), пульты управления типа CDU-6200 №1, №2, комплексные пульты настройки радиосистем RTU-4220 №1, №2, радиостанции КВ диапазона HF-9000 №1, №2, радиостанции УКВ диапазона VHF-4000 №1, №2, аппаратура внутренней связи авиационная АВСА-МВЛ.

В обобщенном виде структурная схема взаимосвязи данного оборудования представлена на рис. 2.

Необходимо отметить, что большая часть аппаратуры ПСВО БИУС Ан-148 (за исключением аппаратуры АВСА-МВЛ и бортовых вычислителей ВЦ-3) производится американской корпорацией Rockwell Collins и имеет относительно высокую эксплуа-

тационную надежность. Граф структуры рассматриваемой подсистемы представлен на рис. 3.

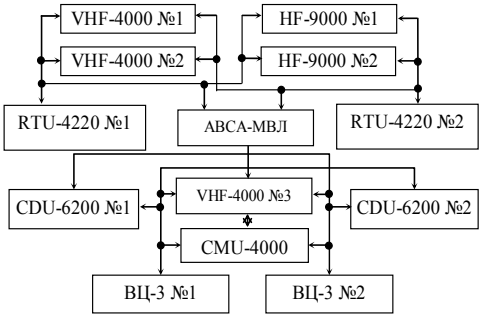

Рис. 2. Структурная схема участка ПСВО БИУС Ан-148, отвечающего за выполнение ФБ

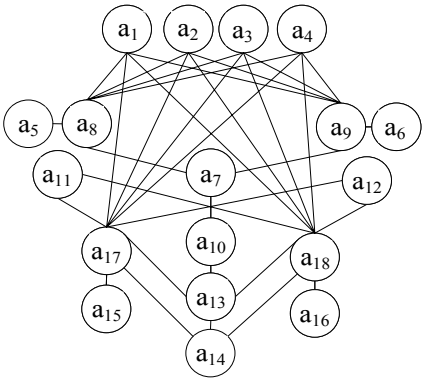

Рис. 3. Граф G(a) участка рассматриваемой ПСВО БИУС Ан-148, обеспечивающего её ФБ

После этого необходимо провести второй этап, сущность которого заключается в анализе критичности задач для выполнения ФБ подсистемы связного и вычислительного оборудования БИУС Ан-148. Для упрощения процедуры проведения данного этапа АКОЭ целесообразным представляется выделение ряда подграфов ФБ из общего графа рассматриваемой подсистемы БИУС Ан-148. Для КрФ f^*_1 подграф будет иметь вид представленный на рис. 4:

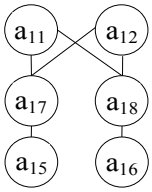

Рис. 4. Подграф $G'_1(a')$ для ФБ f^*_1 оцениваемой подсистемы БИУС Ан-148

В результате разложения ФБ f^*_1 на множество простых критических задач (КЗ) получили следующий перечень (массив $M_{КЗ\,1}$): $Z1_1$ – расчет и формирование в ВЦ-3 (№1, №2) параметров для обеспечения автоматического или ручного выдерживания режимов оптимальных по критериям максимальной дальности, максимальной продолжительности полета; $Z2_1$ – передача полученных данных от ВЦ-3 через шины данных на пульты CDU; $Z3_1$ – индикация параметров на CDU (№1, №2).

На третьем этапе АКОЭ БИУС проводят непосредственное оценивание критичности всех элементов, входящих в соответствующие подграфы КЗ определенной ФБ. Так, в соответствии с предложенным методом оценки критичности отдельных элементов для каждой из ФБ и соответствующих ей КЗ, в три этапа определяется нормированное значение степени критичности всех элементов БИУС. В рассматриваемом примере матрица критичности элементов $M_{КР\,1}$ подграфа $G'_1(a')$, выполняющего ФБ f^*_1, для КЗ из массива $M_{КЗ\,1}$ и абсолютные значения критичности $m_{\Sigma k}$ элементов подграфа $G'_1(a')$ для выполнения ФБ f^*_1 представлены в табл. 1.

Таблица 1

Матрица критичности $M_{КР1}$элементов подграфа $G'_1(a')$ для КЗ из массива $M_{КЗ1}$ (ФБ f^*_1)

	a_{11}	a_{12}	a_{15}	a_{16}	a_{17}	a_{18}
$Z1_1$	0	0	0	0	0,5	0,5
$Z2_1$	0,5	0,5	0,5	0,5	0,5	0,5
$Z3_1$	0,5	0,5	0	0	0	0
$m_{\Sigma k1}$	1	1	0,5	0,5	1	1
ν_{k1}	0,2	0,2	1	1	0,2	0,2

При этом суммарное значение абсолютной критичности всех элементов участка ПСВО БИУС для выполнения ФБ f^*_1 составляет $m_{\Sigma k1} = 5$.

Далее, в соответствии с выражением (1) рассчитываются нормированные значения степени критичности каждого из элементов данной подсистемы БИУС для всех n ФБ, представленные значениями ν_{kn}. Для данной ФБ f^*_1 одномерный массив ν_{k1} нормированных значений степени критичности каждого из элементов рассматриваемого участка ПСВО БИУС Ан-148 представлен в последней строке табл. 1.

Аналогично для всех ФБ определяются нормированные значения степени критичности каждого из элементов ПСВО БИУС, а также суммарные значения их критичности для подсистемы, что позволяет определить перечень компонентов, требующих особого внимания к обеспечению их безотказности в процессе проектирования и эксплуатации, которые приведены в табл. 2. В табл. 3 приведены значения показателей надежности данных элементов.

Фактически показателями безотказности наименее надежного звена в цепи любой ИУС определяется её совокупная надежность, а следовательно, для анализируемых ФБ ПСВО БИУС Ан-148 безотказность их выполнения будет определяться показателями наименее надежных элементов из состава соответствующих им подграфов.

Таблица 2

Нормированные значения степени критичности каждого из элементов участка ПСВО БИУС Ан-148 для перечня рассматриваемых функций безопасности

ν_k	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}
f^*_1	0	0	0	0	0	0	0	0	0	0	0,2	0,2	0	0	0,1	0,1	0,2	0,2
f^*_2	0	0	0	0	0	0	0	0	0	0	0,188	0,188	0	0	0,188	0,188	0,125	0,125
f^*_3	0	0	0	0	0	0	0	0	0	0	0,167	0,167	0	0	0,208	0,208	0,125	0,125
f^*_4	0,083	0,083	0,083	0,083	0	0	0	0	0	0	0,056	0,056	0,167	0,167	0,056	0,056	0,056	0,056
f^*_5	0	0	0	0	0	0	0	0	0	0	0,063	0,063	0,125	0,125	0,188	0,188	0,125	0,125
f^*_6	0,075	0,075	0,075	0,075	0,05	0,05	0,15	0,075	0,075	0,15	0	0	0,15	0	0	0	0	0
f^*_7	0	0	0	0	0	0	0	0	0	0	0,074	0,074	0,185	0,185	0,13	0,13	0,111	0,111
$\nu_{k\Sigma}$	0,158	0,158	0,158	0,158	0,05	0,05	0,15	0,075	0,075	0,15	0,746	0,746	0,627	0,477	0,869	0,869	0,742	0,742

Таблица 3

Показатели надежности отдельных элементов участка ПСВО БИУС Ан-148, выполняющего ФБ

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}	a_{17}	a_{18}
T_o	4000	4000	9000	9000	8000	8000	8000	175200	175200	175200	8000	8000	4000	8000	20000	200000	175200	175200
λ	$2{,}5\cdot\cdot10^{-4}$	$2{,}5\cdot\cdot10^{-4}$	$1{,}11\cdot\cdot10^{-4}$	$1{,}11\cdot\cdot10^{-4}$	$1{,}25\cdot\cdot10^{-4}$	$1{,}25\cdot\cdot10^{-4}$	$1{,}25\cdot\cdot10^{-4}$	$5{,}71\cdot\cdot10^{-6}$	$5{,}71\cdot\cdot10^{-6}$	$5{,}71\cdot\cdot10^{-6}$	$1{,}25\cdot\cdot10^{-4}$	$1{,}25\cdot\cdot10^{-4}$	$2{,}5\cdot\cdot10^{-4}$	$1{,}25\cdot\cdot10^{-4}$	$5\cdot10^{-4}$	$5\cdot10^{-4}$	$5{,}71\cdot\cdot10^{-4}$	$5{,}71\cdot\cdot10^{-4}$
P_o	0,393	0,393	0,199	0,199	0,221	0,221	0,221	0,011	0,011	0,011	0,221	0,221	0,393	0,221	0,095	0,095	0,011	0,011

Результаты оценки безотказности для ФБ ПСВО БИУС Ан-148 приведены в табл. 4.

Таблица 4

Результаты оценки безотказности для ФБ ПСВО БИУС Ан-148

	T_o	λ	P_o
f^*_1	9000	$1{,}11\cdot10^{-4}$	0,199
f^*_2	9000	$1{,}11\cdot10^{-4}$	0,199
f^*_3	9000	$1{,}11\cdot10^{-4}$	0,199
f^*_4	4000	$2{,}5\cdot10^{-4}$	0,393
f^*_5	4000	$2{,}5\cdot10^{-4}$	0,393
f^*_6	4000	$2{,}5\cdot10^{-4}$	0,393
f^*_7	4000	$2{,}5\cdot10^{-4}$	0,393

Последним этапом в проведении анализа и оценивания функциональной безопасности рассматриваемого участка ПСВО БИУС Ан-148 является оценка риска и функциональной безопасности его функций безопасности. Используя предложенный метод, в соответствии с выражениями (1 – 3) получим результаты оценивания, приведенные в табл. 5.

Таблица 5

Результаты оценивания функциональной безопасности ПСВО БИУС Ан-148

	U_n	P_{on}	R_n	$\nu_{\Sigma n}$	$Fs(f^*_n)$
f^*_1	0,5	0,199	0,0995	0,04545	0,99548
f^*_2	0,5	0,199	0,0995	0,07273	0,99276
f^*_3	0,5	0,199	0,0995	0,21818	0,9783
f^*_4	0,75	0,393	0,29475	0,16364	0,95177
f^*_5	0,5	0,393	0,1965	0,07273	0,98571
f^*_6	0,5	0,393	0,1965	0,18182	0,9643
f^*_7	0,5	0,393	0,1965	0,24545	0,95177

Выводы

В статье предложен метод анализа и оценивания функциональной безопасности, в основу которого положен анализ видов, последствий и критичности от отказов отдельных элементов ИУС, выполняющих функции безопасности, а также основные теоретические положения функциональной безопасности.

В результате анализа критичности отдельных элементов БИУС для свойства функциональной безопасности с использованием предложенного метода получаем объективные оценки, отображающие важность того или иного элемента в процессе выполнения (обеспечения) функции безопасности ИУС, что позволяет производить обоснованный выбор элементов, обеспечению безотказности которых необходимо уделять наибольшее внимание на всех этапах жизненного цикла подобного рода систем.

Результатом оценивания функциональной безопасности БИУС являются нормированные значения таких показателей отдельных функциональных подсистем, связанных с безопасностью, как риск и комплексный показатель функциональной безопасности, учитывающий суммарную критичность структурных составляющих подсистемы.

По своему физическому смыслу предложенный комплексный показатель позволяет спрогнозировать изменения уровня безопасности БИУС при отказе той или иной функции безопасности, а также провести ранжирование функциональных подсистем БИУС по степени их влияния на безопасность.

Дальнейшую работу необходимо направить на усовершенствование правил определения нормиро-

ванного показателя ущерба при отказе тех или иных функций, связанных с безопасностью БИУС ЛА и детализацию процедур объективного разделения функций на критические задачи, выполняемые отдельными элементами подсистем ИУС данного класса.

Литература

1. Статистика безопасности полетов деловой авиации за 2008 год [Электрон. ресурс]. – Режим доступа к ресурсу: http://www.business-aviation.ru/analytics/2008.html.

2. ГОСТ РМЭК 61508-1-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 1. Общие требования. – введ. 01.06.2008. – М.: ИПК Изд-во стандартов, 2007. – 50 с.

3. ГОСТ РМЭК 61508-2-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 2. Требования к электрическим /электронным/ программируемым электронным системам, связанным с безопасностью. Введ. 01.06.2008. – М.: ИПК Изд-во стандартов, 2007. – 64 с.

4. ГОСТ РМЭК 61508-4-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 4. Определения и сокращения. Введ. 01.06.2008. – М.: ИПК Изд-во стандартов, 2007. – 64 с.

6. ГОСТ РМЭК 61508-7-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 7. Методы и средства. Введ. 01.06.2008. – М.: ИПК Изд-во стандартов, 2007. – 64 с.

7. ГОСТ 27.310-95. Анализ видов, последствий и критичности отказов. Основные положения. Введ. 01.01.1997. – М.: ИПК Изд-во стандартов, 1996. – 20 с.

8. Харыбин А.В. Метод оценки живучести распределенных информационно-управляющих систем / А.В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2007. - №8 – С. 104 – 109.

9. Самолет Ан-148-100. Стандартная спецификация. – Х.: АНТК им. Антонова, 2003. – 128 с.

Поступила в редакцию 18.02.2009

Рецензент: д-р техн. наук, проф., зав. кафедрой А.Л. Ляхов, Полтавский национальный технический университет им.Ю.Кондратюка, Полтава.

МЕТОД АНАЛІЗУ Й ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ АВІАЦІЙНИХ БОРТОВИХ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ

В.С. Похил, О.В. Харибін

Приведений аналітичний огляд поняття функціональної безпеки. Відзначено важливість розгляду функціональної безпеки як властивості інформаційно-управляючої системи (ІУС) об'єкту критичного застосування. Запропонований метод аналізу критичності окремих елементів та оцінювання функціональної безпеки бортової ІУС цивільної авіації. Розглянутий приклад проведення аналізу для визначення критичності окремих елементів та оцінювання функціональної безпеки бортової ІУС на прикладі підсистеми зв'язного та обчислювального обладнання літака Ан-148.

Ключові слова: бортова інформаційно-управляюча система, функціональна безпека, ризик, критичність елементу.

THE METHOD OF THE FUNCTIONAL SAFETY OF THE AIRCRAFT ONBOARD CONTROL & INFORMATION SYSTEM ANALYSIS AND ESTIMATION

V.S. Pohyl, A.V. Kharybin

The analytical review of concept of functional safety is reduced. Importance of reviewing of functional safety as properties of control & information system (CIS) plant of critical application is noted. The method of the analysis of criticality of separate elements and an estimation of functional safety of the aircraft onboard CIS is offered. The example of carrying out of the analysis of criticality of separate elements and an estimation of functional safety of the onboard CIS on an example of a subsystem of the communication and computing equipment of airplane An-148 is considered.

Keywords: onboard control & information system, functional safety, risk, an analysis and estimation method, criticality of an element.

Похил Виктория Станиславовна – преподаватель кафедры беспроводных технологий в военных телекоммуникационных системах и сетях Военного института телекоммуникаций и информатизации НТУУ «КПИ», Полтава, Украина, vikulina.85@mail.ru.

Харыбин Александр Викторович – канд. техн. наук, доцент кафедры беспроводных технологий в военных телекоммуникационных системах и сетях Военного института телекоммуникаций и информатизации НТУУ «КПИ», Полтава, Украина, havral@mail.ru.