УДК 004.03

В.С. ПОХИЛ, А.В. ХАРЫБИН

Военный институт телекоммуникаций и информатизации НТУУ «КПИ», Украина

МЕТОДЫ ОЦЕНИВАНИЯ И ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ БОРТОВЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Приведена концептуальная модель информационной технологии обеспечения, а также методы оценивания и обеспечения функциональной безопасности авиационных бортовых информационно-управляющих систем, основанные на анализе критичности входящих в них элементов для нормального и безотказного выполнения всех функций, связанных с безопасностью и определяющих ее полноту. Предложен метод оценивания и обеспечения функциональной безопасности, в основу которого положен анализ видов, последствий и критичности отказов отдельных элементов, выполняющих функции безопасности, а также основные теоретические положения функциональной безопасности.

Ключевые слова: *бортовая информационно-управляющая система, функциональная безопасность, риск, ущерб, критичность элемента, метод оценивания, метод обеспечения, информационная технология.*

Введение

Безопасность полета летательного аппарата (ЛА) – одно из основных свойств авиационно-транспортной системы, формируемое на этапе ее создания и эксплуатации. Результаты анализа данных об авиапроисшествиях за последние 6 лет свидетельствуют о значительном ухудшении состояния безопасности полетов, а анализ причин возникновения событий и инцидентов в гражданской авиации за последние 10 лет свидетельствуют о том, что приблизительно 80% из них произошли по вине экипажей и диспетчеров управляющих воздушным движением ЛА. Это приводит к тому, что разработчики воздушных судов стараются автоматизировать все большее число функций по управлению самолетом на различных этапах полета, возложив их на бортовые информационно-управляющие системы (БИУС) ЛА, что, в свою очередь, приводит к повышению их ответственности за ФБ ЛА, усложнению,а следовательно, и повышению требований к надежности и функциональной безопасности данных систем. В статье рассматривается методологический аппарат анализа (оценивания) и обеспечения функциональной безопасности БИУС ЛА, как системам критического применения, отказы которых могут с высокой вероятностью привести к возникновению авиационных происшествий и катастроф. Актуальность работы обусловлена необходимостью создания методологического аппарата анализа (оценивания) и обеспечения функциональной безопасности (ФБ) информационно-управляющих систем (ИУС) критического применения (на примере БИУС ЛА), который бы позволил создать информационную технологию (ИТ) обеспечения заданного либо максимально возможного в сложившихся условиях уровня данного свойства.

Анализ литературы [1, 2] по данному вопросу показал отсутствие подобного методологического аппарата для БИУС ЛА, что было обусловлено отсутствием соответствующих требований в технических заданиях на разработку соответствующих бортовых комплексов.

В общем случае сущность ИТ обеспечения ФБ заключается в осуществлении мероприятий по предотвращению сбоев и отказов в работе или восстановлению работоспособности систем, связанных с безопасностью, а также по предоставлению поддержки в принятии решений экипажу в критической ситуации. Основной целью при этом является исключение либо минимизация риска возникновения и развития аварийных ситуаций, способных привести к катастрофическим последствиям (ущербу) при не выполнении функций безопасности БИУС ЛА. Ущерб, возникающий в результате развития аварийных ситуаций на борту ЛА до уровня авиакатастроф, измеряется человеческими жертвами, потерями экологической системы и экономики (социально-экономическим ущербом), и может быть определен технико-функциональным ущербом для БИУС ЛА. Последний в идеале должен сводиться к допустимому для БИУС, не приводящему к снижению уровня ФБ ЛА ниже минимально допустимого. Применение ИТ обеспечения ФБ БИУС ЛА и соответствующих им методов обусловлено необходимостью снижения уровня риска при происшествиях до

уровня допустимого и/или восстановления критического функционала данных систем, выполнение которого необходимо для удержания риска на уровне допустимого.

Целью данной статьи является представление методов обеспечения и анализа (количественного оценивания показателей) ФБ БИУС ЛА, а также общей концепции информационной технологии обеспечения данного свойства на основе указанных методов.

1. Информационная технология обеспечения заданного уровня функциональной безопасности БИУС летательных аппаратов

При рассмотрении аспектов безопасности принят постулат, что абсолютной безопасности не существует - после принятия защитных мер некоторый остаточный риск всегда остается. 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.

В основе будущих ССБ, обеспечивающих ФБ БИУС ЛА, будет использоваться ИТ, гарантирующая удержание рисков в случае отказов либо сбоев (ошибок) в работе подсистем БИУС на допустимом уровне, то есть выполняющая функцию безопасности. Подобная ИТ обеспечения ФБ БИУС ЛА будут использоваться технические средства обеспечения безопасности и совокупность информационных (аналитических и прогностических) методов сокращения риска [1].

При обеспечении ФБ БИУС ЛА в целом на этапе их эксплуатации необходимо непрерывно контролировать степень критичности ее отдельных элементов (подсистем) способных вызвать снижение уровня ФБ и привести к ущербу для БИУС, а следовательно и ЛА. Это позволит своевременно выявить возможные причины невыполнения требований по полноте ФБ и задействовать необходимые средства управления ССБ БИУС (безотказностью) [2-4].

На рис. 1 приведена концептуальная модель ИТ обеспечения ФБ БИУС ЛА, основанная на соответствующих математических методах и средствах анализа (оценивания) и обеспечения ФБ подобных систем.

2. Метод оценивания функциональной безопасности БИУС ЛА

В работе [2] рассмотрен метод оценивания ФБ БИУС ЛА, позволяющий учесть различность функциональной критичности элементов и подсистем БИУС для наступления отказов, приводящих к катастрофическому ущербу. Методологический аппарат, влияющие факторы, реальные показатели надежности и живучести подсистем и элементов БИУС ЛА служат в нем ориентирами при анализе и оценке функциональной безопасности.

С применением данного метода рассматриваемая ССБ представляется в виде графа, вершинам которого соответствуют информационно-коммуникационные узлы (вычислительно-управляющее оборудование, датчики, исполнительные механизмы) и шины обмена данными (сигналами) между ними, соединенные ребрами.

Предлагаемый метод анализа и оценки ФБ БИУС ЛА содержит следующие этапы.

На первом этапе определяются все функции выполняемые отдельной подсистемой, как ССБ.

На втором этапе определяется возможность наступления катастрофического состояния при невыполнения функций системой, путем оценки величины ущерба, который повлечет за собой отказ той или иной функции безопасности ($F_Б$).

С целью оценки нормированного значения ущерба (U_n) используются следующие правила:

- если в результате отказа $F_Б$ подсистемы БИУС ЛА наступят катастрофические последствия, связанные с гибелью людей, значение принимается равным 1;
- если в результате отказа $F_Б$ подсистемы БИУС ЛА возможно наступление катастрофических последствий, но существует компенсирующая ФБ, выполняемая другой подсистемой БИУС либо сочетанием БИУС и членов экипажа, то значение принимается равным 0,75;
- если в результате отказа $F_Б$ подсистемы БИУС ЛА возможно наступление катастрофических последствий, но существует аналогичная ФБ, выполняемая другой подсистемой (резервным контуром), то значение равно 0,5.
- если в результате отказа $F_Б$ подсистемы БИУС ЛА катастрофические последствия не наступают, то значение принимается равным 0.

На третьем этапе проводится анализ критичности всех функций безопасности, для которых значение нормированного показателя ущерба не равно 0 ($U_n \neq 0$), а также относительной критичности отдельных элементов с позиций ФБ.

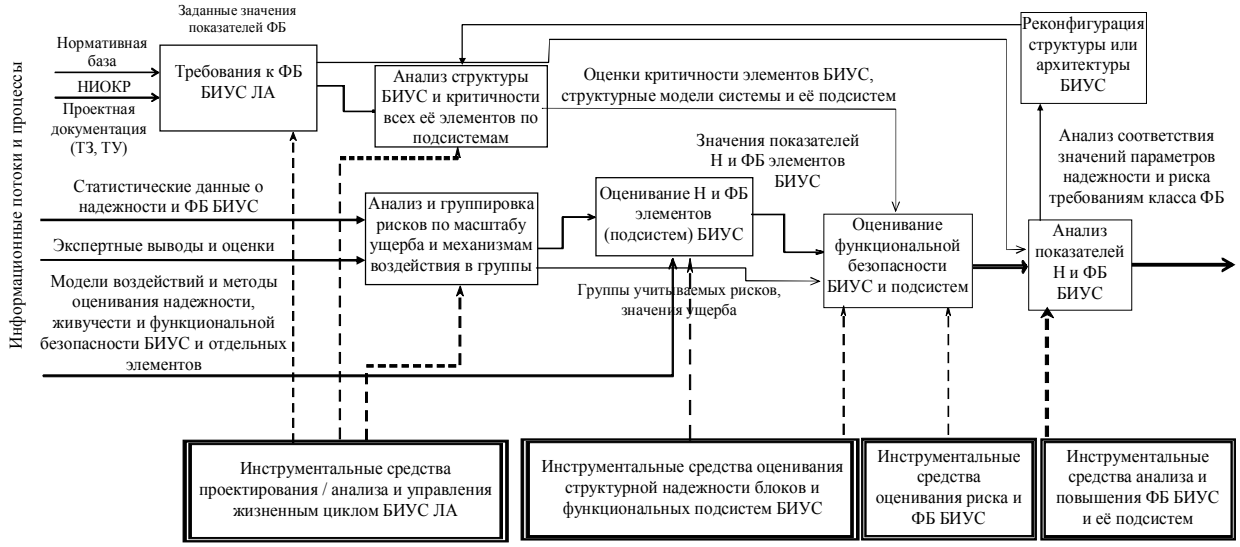

Рис. 1. Концептуальная модель информационной технологии обеспечения функциональной безопасности БИУС летательного аппарата

Данная процедура основана на требованиях по проведению анализа критичности отказов элементов сложных систем, изложенных в [2] и содержит в своем составе четыре основных операции:

– производится разложение графа БИУС на частные подграфы содержащие все элементы, которые участвуют в реализации функций безопасности БИУС. Качественные характеристики выполнения этих $F_Б$ будут определяющими для ФБ системы в целом;

– каждая из данных $F_Б$ подвергается разложению на множество простых задач $\{Z_n\}$ (процессов), выполняемых отдельными элементами БИУС ЛА и обеспечивающими работу подсистемы, связанной с данной $F_Б$;

– определяется кратность использования отдельных элементов подсистем БИУС в решении критических задач (КЗ), обеспечивающих выполнение соответствующих $F_Б$. При этом для каждой из функциональных подсистем формируются матрицы критичности M_{KPn} 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.

– затем производится 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-той подсистемы БИУС путем суммирования значений всех элементов m_{jk} k-того столбца матрицы критичности $M_{KPn}(Z_{jn}, a_k)$;

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

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

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

Результатом проведения 3 этапов оценивания ФБ БИУС ЛА будет i одномерных массивов $V_n(a_k)$, содержащих значения показателя кратности критичности v_k всех элементов критичных подсистем БИУС, связанных с ФБ.

На четвертом этапе проводится операции оценивания функциональной безопасности БИУС

в целом [2], для чего необходимо провести оценивание данного свойства для всех функциональных подсистем, каждая из которых представлена набором элементов, отвечающих за выполнение соответствующей $F_Б$.

Оценивать показатель функциональной безопасности (Fs) отдельной функциональной подсистемы БИУС, выполняющей одну из $F_Б$ (f^*_n), предлагается согласно выражению:

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

где $\nu_{\Sigma n}$ – удельная суммарная критичность n-той функции подсистемы БИУС, выполняющей $F_Б$, для полного множества $F_Б$ системы;

R_n – риск, связанный с ФБ, определяемый по формуле [3]:

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

где: P_{on} – вероятность эксплуатационного отказа n-й $F_Б$ системы, U_n – нормированный в пределах [0, 1] показатель ущерба, возможного при отказе $F_Б$.

Определение степени критичности отдельных элементов (подсистем), которые могут вызвать нарушение или ухудшение работы системы в целом необходимо для обеспечения ФБ БИУС – чтобы определить, повышению надежности каких компонентов БИУС ЛА необходимо уделить внимание в первую очередь и какие средства управления возможно и необходимо применить для этого.

3. Метод обеспечения функциональной безопасности БИУС ЛА

После проведения оценивания необходимо использовать методы обеспечения ФБ БИУС ЛА. Сущность предлагаемого метода сводится к достижению максимальной эффективности проведения следующих групп мероприятий, направленных на повышение ФБ БИУС ЛА:

– повышение надежности и устойчивости информационно-вычислительных процессов в соответствующих подсистемах БИУС, выполняющих $F_Б$, путем внесения программно-алгоритмической, информационной, технической или какой-то иной избыточности;

– применение новых технологических решений для элементов, которые имеют максимальные значения кратности критичности (ν_k) по результатам анализа ФБ данной критической подсистемы для увеличения надежности выполнения ими возложенных на них задач и функций;

– изменение структурно-архитектурной либо алгоритмической организации наиболее критических информационно-вычислительных процессов в БИУС ЛА с целью уменьшения значений кратности критичности (ν_k) элементов, входящих в критические подсистемы БИУС. При этом необходимо стараться добиться максимального уменьшения значений ν_k для элементов, имеющих наименьшие количественные значения показателей надежности и/или максимальные значения ν_k в подсистемах.

По результатам применения указанных мер по повышению ФБ отдельных подсистем и БИУС ЛА в целом производится оценивание ее ФБ и определяется разница в полученных значениях показателей R_n и Fs для каждой из критических функций, после чего проводится анализ эффективности принятых мер по критериям, определяемым отношениями прироста показателей ФБ подсистем БИУС к увеличению затрат и/или ухудшению масс-габаритных показателей БИУС ЛА (при условии сохранения той же полноты и параметров, определяющих эффективность информационно-управляющих процессов в ней). На этапе эксплуатации возможно применение лишь последней из указанных групп мероприятий, поэтому перспективные бортовые подсистемы обеспечения надежности и функциональной безопасности БИУС ЛА, которые, вероятнее всего, будут в них же интегрированы, в ядре соответствующей ИТ обеспечения ФБ будут иметь программно-технические средства на основе алгоритмов достижения максимально возможных значений показателей данных свойств в создавшихся условиях работы БИУС за счет изменения архитектурно-топологических схем выполнения управляющих информационно-вычислительных процессов и перераспределения вычислительных ресурсов подсистем.

Выводы

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

Дальнейшую работу необходимо направить на детализацию метода обеспечения ФБ БИУС ЛА и процедур объективного разложения множества их функций на критические задачи, выполняемые отдельными элементами всех подсистем.

Литература

1. ГОСТ Р МЭК 61508-7-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 7. Методы и средства: [введен

2008-06-01] – М.: ИПК Издательство стандартов, 2007. – 64 с. [Национальный стандарт Российской Федерации].

2. Похил В.С. Метод анализа и оценивания функциональной безопасности авиационных бортовых информационно-управляющих систем / В.С Похил., А.В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2009. – № 8 – С. 104-109.

3. ГОСТ 27.310-95. Анализ видов, последствий и критичности отказов. Основные положения: [введен 1997-01-01] – М.: ИПК Издательство стандартов, 1996. – 20 с. [Межгосударственный стандарт].

4. ГОСТ Р МЭК 61508-5-2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч. 5. Рекомендации по применению методов определения уровней полноты безопасности: [введен 2008-06-01] – М.: ИПК Издательство стандартов, 2007. – 23 с. [Национальный стандарт Российской Федерации].

Поступила в редакцию 1.03.2010

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

МЕТОДИ ОЦІНЮВАННЯ Й ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БОРТОВИХ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ ЛІТАЛЬНИХ АПАРАТІВ

В.С. Похил, О.В. Харибін

Наведено концептуальну модель інформаційної технології забезпечення, а також методи оцінювання та забезпечення функціональної безпеки авіаційних бортових інформаційно-керуючих систем, що засновані на аналізі критичності елементі, що входять до їх складу, для нормального та безвідмовного виконання усіх функцій, які пов'язані із безпекою та визначають її повноту. Запропоновано метод оцінювання і забезпечення функціональної безпеки, в основу якого покладено аналіз видів, наслідків та критичності відмов окремих елементів, що виконують функції безпеки, а також основні теоретичні положення функціональної безпеки.

Ключові слова: бортова інформаційно-керуюча система, функціональна безпека, риск, критичність елементу, метод оцінювання, метод забезпечення, інформаційна технологія.

THE ESTIMATION AND SUPPORTING METHODS OF THE FUNCTIONAL SAFETY OF THE AIRCRAFT ONBOARD CONTROL & INFORMATION SYSTEM

V.S. Pohyl, O.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. A method of evaluating and ensuring the functional safety, which is based on the analysis of species, effects and criticality of failures of individual elements that perform security functions, as well as the basic theoretical principles of functional safety, is proposed.

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

Похил Виктория Станиславовна – соискатель, преподаватель кафедры беспроводных технологий в военных телекоммуникационных системах и сетях, Военный институт телекоммуникаций и информатизации Национального технического университета Украины «Киевский политехнический институт», Полтава, Украина, e-mail:vikulina.85@mail.ru.

Харыбин Александр Викторович – канд. техн. наук, доцент кафедры беспроводных технологий в военных телекоммуникационных системах и сетях, Военный институт телекоммуникаций и информатизации Национального технического университета Украины «Киевский политехнический институт», Полтава, Украина, e-mail:havral@mail.ru.