УДК 621.398 DOI 10.18698/2308-6033-2016-07-1511

Метод определения факторов риска для автоматизированной системы управления полетами космических аппаратов

© А.Г. Андреев[1], Г.В. Казаков[1], В.В. Корянов[2]

[1]ФГБУ «4 ЦНИИ» Минобороны России, Королёв Московской обл., 141091, Россия
[2]МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Множество известных способов классификации тех или иных объектов связано с построением деревьев классификации по признакам, выбираемым, как правило, исходя из физического смысла решаемой задачи. К таким признакам не предъявлялись какие-либо формальные требования. В статье поставлена и решена задача получения полного, неизбыточного и непротиворечивого множества факторов риска, которые являются основой разработки соответствующих средств их нейтрализации. При решении поставленной задачи использованы бинарные отношения и необходимый математический аппарат теории множеств, проведено строгое математическое доказательство полученного результата. Описано применение изложенной теории к практике определения факторов риска для автоматизированной системы управления полетами космических аппаратов.

Ключевые слова: *автоматизированная система управления, космический аппарат, надежность, программное обеспечение, фактор риска.*

Введение. Качество автоматизированной системы управления полетами космических аппаратов (АСУ КА) зависит от воздействия на нее различных факторов риска. Источники факторов риска (ИФР) являются отправным пунктом при разработке механизмов обеспечения требуемого качества системы [1–8]. Многочисленность факторов риска и источников их возникновения требует выделения из их полного состава основных факторов, в значительной мере влияющих на информационную устойчивость АСУ КА. Одним из подходов к классификации ИФР для АСУ КА является использование бинарных отношений и математического аппарата теорий множеств. Такой подход позволяет выделить множество факторов риска, обладающих свойствами полноты, непротиворечивости и неизбыточности, а также определить механизмы их обнаружения и нейтрализации.

Классификация источников факторов риска АСУ КА. Определение множества факторов риска для качества функционирования АСУ КА базируется на рассмотрении ее предметной области. Содержательное описание предметной области АСУ КА включает такие основные понятия, как структура системы, входная, промежуточная и выходная информация. Качество АСУ КА определяется на основе анализа факторов риска на всех этапах ее жизненного цикла.

Автоматизированная система управления полетами КА является организационно-технической системой, включающей персонал и комплекс средств автоматизации его деятельности, который предназначен для реализации установленных функций, обеспечивающих выполнение задач полета данным типом КА. К таким функциям относятся формирование, контроль синтаксической и семантической правильности сформированных данных полета КА и ввод их в базы данных звеньев АСУ и на специальный носитель информации системы управления КА.

Фактором риска АСУ КА называется явление, действие или обстоятельство случайного или преднамеренного характера, способное нарушить функционирование системы с нанесением целям ее применения неприемлемого ущерба. Другими словами, к факторам риска относятся те, воздействие которых ухудшает качество системы, нанося определенный ущерб целям применения КА.

Данные полета КА, успешно прошедшие синтаксический и семантический контроль, называются *функционально пригодными* или *реализуемыми*. Реализуемые данные включают массив информации D в специальной структуре, использование которого позволит КА выполнить задачи полета с учетом энергетических возможностей КА.

Структура данных Д полета КА представляет собой кортеж вида

$$\text{Д} = \langle SI_1,\ D,\ SI_2 \rangle, \tag{1}$$

где SI_1, SI_2 — служебная информация начала и конца массива данных соответственно.

Под *реализуемой задачей полета* (ЗП) будем понимать массив данных в специальной структуре, содержащий данные полета КА, и уставки ЗП, использование которых позволит КА выполнить эти задачи с учетом ограничений, накладываемых энергетическими и конструктивно-техническими характеристиками КА и его системы управления.

Структура ЗП представляет собой кортеж вида

$$\text{ЗП} = \langle SI_3,\ D,\ U,\ SI_4 \rangle, \tag{2}$$

где SI_3, SI_4 — служебная информация начала и конца массива ЗП соответственно; U — уставки ЗП.

Для того чтобы провести корректное выделение значимых факторов риска, необходимо определить их полный непротиворечивый и в то же время неизбыточный состав. Для этого проводится классификация ИФР с использованием предлагаемого далее подхода, который заключается в построении корневого дихотомического дерева признаков классификации ИФР.

Можно доказать, что при таком подходе к классификации ИФР будет получено полное, непротиворечивое и неизбыточное множество факторов риска $\{ФР_j\}$, которое используется для разработки адекватных механизмов их нейтрализации в целях обеспечения заданного уровня показателя качества АСУ КА. Корневое дихотомическое дерево признаков классификации определим следующим образом.

Корневым дихотомическим деревом Δ_2 *признаков классификации* называется дерево, из каждой вершины которого выходят ровно две ветви, соединенные с вершинами, соответствующими двум взаимоисключающим признакам классификации.

Докажем теорему о том, что корневое дихотомическое дерево является основой для полного учета ИФР нарушения качества АСУ КА.

Обозначим множество классифицируемых объектов (т. е. ИФР) через M. Определим некоторую совокупность признаков p_1, p_2, …, p_n, …, p_N классификации и определим на множестве M отношение A, означающее обладание признаком p_n. Пусть элемент x множества M обладает признаком p_n, обозначим это как $x(p_n)$. Покажем, что в данном случае отношение A является эквивалентностью.

Если $x(p_n)$, справедливо очевидное соотношение xAx (рефлексивность).

Если $x(p_n)$ и $y(p_n)$, то из xAy следует, что yAx. Это утверждение следует непосредственно из определения отношения A (симметричность).

Пусть теперь $x(p_n)$, $y(p_n)$, $z(p_n) \in M$. Тогда из xAz и zAy следует, что xAy (транзитивность). Это тоже очевидно, поскольку все элементы x, y, z обладают одним и тем же признаком p_n.

Рассмотренные три свойства отношения A определяют его как отношение эквивалентности. Докажем следующую лемму.

Лемма. Для любых элементов x и y, принадлежащих множеству M, справедливо утверждение

$$(M_X = M_Y) \vee (M_X \cap M_Y = \varnothing),$$

где M_X — подмножество множества M, которому принадлежит элемент x в силу отношения A; M_Y — подмножество множества M, которому принадлежит элемент y в силу того же отношения A; $\varnothing$ — символ пустого множества; $\vee$ — логическое ИЛИ.

Доказательство. Предположим, что пересечение $M_X \cap M_Y \neq \varnothing$, и докажем, что в этом случае имеет место равенство $M_X = M_Y$. Если выполнено условие $M_X \cap M_Y \neq \varnothing$, то существует некоторый элемент $z \in M_X \cap M_Y$. Тогда из определений подмножеств M_X и M_Y следует справедливость xAz и yAz. Из симметрич-

ности отношения A следует, что имеет место отношение zAy, а из транзитивности отношения A следует, что из выполнения xAz и zAy вытекает справедливость отношения xAy.

Выберем произвольный элемент $q \in M_Y$. По определению имеем yAq. Из xAy и yAq следует, что xAq, т. е. $q \in M_X$. Отсюда

$$M_Y \subseteq M_X . \tag{3}$$

Выберем теперь произвольный элемент $z \in M_X$, для которого выполнено zAx. По симметрии отношения A имеем xAz. Из транзитивности отношения A имеем yAx и xAz, откуда следует справедливость yAz. Значит, $z \in M_Y$. Следовательно,

$$M_X \subseteq M_Y . \tag{4}$$

Из условий (3) и (4) следует равенство $M_X = M_Y$, что и требовалось доказать.

Теперь можно воспользоваться следующей теоремой [9]: если отношение A на множестве M обладает свойствами рефлексивности, симметричности и транзитивности, то существует разбиение $\{M_1, M_2, \ldots, M_n\}$ этого множества такое, что отношение xAy выполнено тогда и только тогда, когда x и y принадлежат одному и тому же классу разбиения.

Разбиение множества M определяется как система (конечная или бесконечная) непустых подмножеств множества M, обладающая свойствами:

а) покрытия множества M:

$$M = \{M_1 \cup M_2 \cup M_3 \cup \ldots\}; \tag{5}$$

б) отделимости множеств M_i и M_j:

$$M_i \cap M_j = \varnothing \, (i \neq j).$$

Пусть при выделении классов объектов из множества M используются дихотомические признаки:

p_1 — объект принадлежит подмножеству (классу) M_1;

p_2 — объект не принадлежит подмножеству (классу) M_1 (относится к подмножеству (классу) M_2).

В силу доказанной леммы образованные с помощью этих двух признаков классы подмножеств M_1 и M_2 множества M не пересекаются $(M_1 \cap M_2 = \varnothing)$.

Множества M_1 и M_2 являются покрытием всего множества *M*, что следует из свойства (5) и сущности признаков классификации: «объект принадлежит множеству M_1 или нет».

Исходя из леммы и теоремы о разбиении множества *M*, на котором определено отношение эквивалентности *A*, покажем, что корневое дихотомическое дерево порождает полноту, неизбыточность и непротиворечивость классов классифицируемых объектов. Множество всех возможных объектов (т. е. множество всех ИФР) обозначим через *M*.

Теорема. Корневое дихотомическое дерево признаков классификации источников возникновения объектов порождает полное, непротиворечивое и неизбыточное множество классифицируемых объектов.

Доказательство. Пусть при выделении классов объектов из *M* используются указанные ранее дихотомические признаки: p_1 и p_2. Тогда в силу (5) $M = \{M_1 \cup M_2\}$.

Допустим, что существует элемент $x \in M$, который не принадлежит ни одному из двух классов M_1 или M_2 множества *M*. Тогда этот элемент либо не обладает ни признаком p_1, ни признаком p_2, либо обладает обоими признаками одновременно.

Если элемент *x* не обладает ни одним из признаков, то имеет место противоречие, поскольку признаки p_1 и p_2 определяют дихотомию и элемент *x*, не обладающий ни одним из признаков, не может являться элементом множества *M*, т. е. $x \notin M$.

Допустим теперь, что элемент *x* обладает одновременно двумя признаками. Поскольку признаки p_1 и p_2 дихотомичны, то ни один объект не может обладать двумя взаимоисключающими признаками по определению, и в этом случае также имеет место противоречие ($x \notin M$).

Таким образом, доказано, что любой элемент $x \in M$ должен обладать либо признаком p_1, либо признаком p_2, что определяет свойства полноты и неизбыточности объектов, входящих в классы объектов M_1 и M_2.

Докажем теперь свойство непротиворечивости. Поскольку любой элемент из множества *M* может обладать только одним из признаков p_1 или p_2, то элемент *x*, обладающий признаком p_1, принадлежит подмножеству M_1 ($x \in M_1$) и не принадлежит подмножеству M_2 ($x \notin M_2$), а элемент *y*, обладающий признаком p_2, принадлежит подмножеству M_2 ($y \in M_2$) и не принадлежит подмножеству M_1 ($y \notin M_1$).

Таким образом, элементы x и y в силу отношения A могут принадлежать только разным классам, что и определяет свойство непротиворечивости элементов, входящих в классы M_1 и M_2.

Точно так же доказываются свойства полноты, непротиворечивости и неизбыточности для семейств, видов, подвидов, групп, типов объектов и т. п., если для их классификации используются дихотомические признаки (признаки p_3 и p_4, образующие семейства объектов, признаки p_5 и p_6, образующие виды объектов, и т. д.). Теорема доказана.

Следствие. Если для какого-либо уровня дерева Δ имеется ряд признаков $p_1, p_2, ..., p_K$, которые составляют полную группу, то это дерево классификации, не являясь дихотомическим, порождает полное, неизбыточное и непротиворечивое множество классифицируемых объектов.

Доказательство. Если на каком-либо *i*-м уровне дерева Δ выделены признаки $p_1, p_2, ..., p_K$, образующие полную группу (вероятность появления одного из этих признаков равна единице), то соответствующее множество M_i можно представить в виде покрытия:

$$M_i = \{M_{1i} \cup M_{2i} \cup M_{3i} \cup ... \cup M_{ki} \cup ... \cup M_{Ki}\},$$

где $M_{ji} \cap M_{ki} = \varnothing$ при $j \neq k$.

В соответствии с доказанной теоремой любой элемент $x \in M_i$ должен принадлежать только одному из подмножеств M_{ki}. Отсюда следует, что множество M_i разбито на непересекающиеся классы и элементы этих множеств образуют полное, непротиворечивое и неизбыточное множество классифицируемых объектов, распределенных по признакам $p_1, p_2, ..., p_K$.

Таким образом, полнота, неизбыточность и непротиворечивость уровней классификации (классов, семейств, видов, подвидов, групп, типов и т. п.) ИФР позволяет утверждать, что они охватывают всю сферу их возникновения. Следует отметить, что между висячими вершинами дихотомического дерева Δ_2 и факторами риска не существует биективного соответствия, поскольку один и тот же источник может реализовать несколько их видов и, наоборот, один и тот же фактор риска может быть реализован несколькими видами источников.

Определение состава источников факторов риска АСУ КА. В соответствии с доказанной теоремой классификация ИФР может быть проведена следующим образом.

Выделяют **два класса** ИФР: *субъективные* и *объективные* [10]. Очевидно, что признаки классификации (p_1 — «объективный ИФР»

и p_2 — «субъективный ИФР») образуют полную группу и определяют два класса подмножеств M_1 и M_2, которые являются покрытием множества *M* всех ИФР.

Класс субъективных ИФР подразделяют на **два семейства**: *внешние* и *внутренние* [10]. Очевидно, что признаки классификации p_3 — «внешний ИФР» и p_4 — «внутренний ИФР» также образуют полную группу, поскольку это взаимоисключающие признаки, и порождают подмножества M_{11}, M_{12} и M_{21}, M_{22}, которые являются покрытием соответствующих подмножеств M_1 и M_2 ($M_1 = M_{11} \cup M_{12}$; $M_{11} \cap M_{12} = \varnothing$; $M_2 = M_{21} \cup M_{22}$; $M_{21} \cap M_{22} = \varnothing$).

Семейства внешних и внутренних источников класса субъективных ИФР подразделяют на **два вида**: p_5 — *преднамеренные* и p_6 — *непреднамеренные*.

Очевидно, что класс объективных ИФР не может быть разбит на эти же семейства, поскольку он содержит только непреднамеренные источники. По этой причине класс объективных ИФР подразделяют на следующие **два семейства**: p_7 — «*внешняя среда АСУ КА*» и p_8 — «*внутренняя среда АСУ КА*».

По такому же принципу проводят дальнейшую декомпозицию ИФР.

Рассмотрим **систему факторов риска** как результат классификации их источников, которая соответствует проведенной классификации всех сфер возникновения ИФР. Следует отметить, что приведенная схема классификации не является единственной. Можно, например, провести классификацию по этапам жизненного цикла АСУ КА, признакам смыслового содержания ИФР или каким-либо иным признакам. Однако какой бы вид классификационной схемы ни был избран, для обеспечения полноты, непротиворечивости и неизбыточности она должна удовлетворять условиям доказанной теоремы (или ее следствию).

Исходя из приведенных структур данных полета КА (1) и задач полета (2), факторы риска можно представить в виде возможности осуществления на этапе эксплуатации АСУ КА разрушающих информационных воздействий (РИВ). Эти воздействия могут быть реализованы лицами из числа оперативного и обслуживающего персонала системы либо по злоумышленным мотивам, либо случайным образом (табл. 1).

Очевидно, что из перечисленных факторов риска наиболее опасным является фактор, связанный с подменой данных полета КА, определяющих координаты точки выведения КА.

Таблица 1

Факторы риска на этапе эксплуатации АСУ КА и последствия разрушающих информационных воздействий

Фактор риска	Последствия от РИВ
Преднамеренные РИВ	
Искажение данных полета КА	Невозможность чтения информации Получение нереализуемых данных полета КА Доставка КА не в назначенные точки
Подмена данных полета КА	Доставка КА в точки, определенные злоумышленниками
Разрушение (стирание) данных полета КА или их блокировка	Невозможность осуществления запуска КА
Раскрытие данных полета КА злоумышленниками	Заблаговременное принятие мер по максимизации ущерба аварийного запуска КА с использованием разных мероприятий
Искажение констант ЗП	Невозможность выполнения КА поставленной задачи
Подмена констант ЗП	Невозможность осуществления запуска КА либо аварийное завершение запуска, в том числе и на старте
Разрушение (стирание) уставок ЗП или их блокировка	Невозможность осуществления запуска КА
Непреднамеренные РИВ	
Искажение данных полета КА	Невозможность чтения информации Получение нереализуемых данных полета КА Доставка КА не в назначенные точки
Разрушение (стирание) данных полета КА или их блокировка	Невозможность осуществления запуска КА
Искажение констант ЗП	Невозможность выполнения КА поставленной задачи
Разрушение (стирание) уставок ЗП или их блокировка	Невозможность осуществления запуска КА

Высокая степень компьютеризации процесса подготовки данных полета КА дает возможность злоумышленникам использовать не только традиционные средства нарушения этого процесса, но и относительно новое оружие — информационное. Этот вид оружия основан на создании источников, порождающих преднамеренные угрозы информационной безопасности (ИБ) данных полета КА (преднамеренные ИФР). Эти угрозы направлены на нарушение основных характеристик ИБ данных: конфиденциальности, целостности, доступности.

Нарушение ИБ определенного объема этих данных приведет к неприемлемому ущербу — невыполнению целей функционирования АСУ КА по подготовке данных полета КА.

Не менее опасны по последствиям и случайные угрозы нарушения основных свойств ИБ данных, обрабатываемых средствами АСУ

КА. Поскольку эти угрозы не являются скрытыми, их можно выявить и устранить до сдачи АСУ КА в эксплуатацию, обеспечивая тем самым требуемый уровень ее информационной устойчивости.

Одним из основных принципов системного подхода к исследованию информационной устойчивости АСУ КА является рассмотрение ее во взаимосвязи с окружающей средой, которая порождает факторы, нарушающие штатный процесс функционирования системы.

Для АСУ КА основные факторы риска порождаются ее внешней и внутренней средой, которые можно представить в виде сфер появления ИФР (табл. 2).

Таблица 2

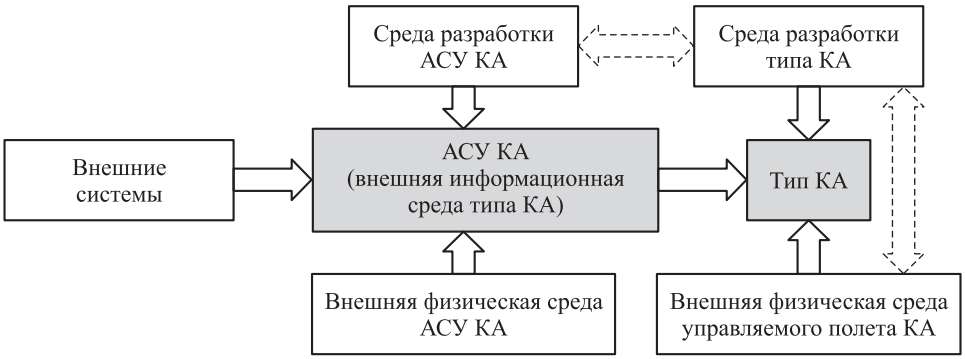
Сферы появления источников факторов риска

Локальная среда	Объект локальной среды	Задачи локальной среды
Внешняя среда АСУ КА		
Среда разработки АСУ КА	Средства подготовки данных	Разработка программного обеспечения (ПО) и технических средств (ТС) подготовки данных полета КА
	Средства взаимодействия с внешними системами	Разработка средств взаимодействия с внешними системами
Среда разработки типа КА	Системы и агрегаты КА	—
	ПО системы управления КА	Разработка средств выведения КА
Внутренняя среда АСУ КА		
Физическая среда АСУ КА	Здания, в которых размещены элементы АСУ КА	—
	Помещения с элементами АСУ КА, в том числе и выделенные помещения	—
Информационная среда АСУ КА	Основные ТС и системы (ОТСС)	Выбор ТС и программных (программно-аппаратных) средств подготовки данных полета КА
	Вспомогательные ТС и системы (ВТСС)	Выбор систем энергоснабжения и систем поддержания температурно-влажностного режима (СПТВР)

Поскольку АСУ КА является специфической системой, основная функция которой заключается в своевременной подготовке данных полета КА, в качестве ИФР необходимо учитывать и перечисленные в табл. 2 элементы внешней среды типов КА.

К особенностям элементов этого вида внешней среды АСУ КА относится отсутствие в ней прямых факторов риска, которые тем не менее необходимо учитывать, поскольку, как следует из определения

АСУ КА, невыполнение КА поставленной задачи оценивается как результат нарушения предписанных функций АСУ КА, что, по сути, является фактором риска. В свою очередь, для типа КА как объекта потребления информации АСУ КА следует принять во внимание не только его внешнюю среду в виде среды разработки типа КА, которая должна учитываться в среде разработки АСУ КА, но и внешнюю физическую среду, которая также должна учитываться в среде разработки типа КА, а следовательно, и в среде разработки АСУ КА. Элементы внешней среды АСУ КА и их взаимосвязи представлены на рисунке.



Элементы внешней среды АСУ КА и их взаимосвязи

В соответствии с классификацией ИФР рассмотрим результирующий состав субъективных (непреднамеренные и преднамеренных) факторов риска, порождаемых каждым из элементов внешней среды АСУ КА (табл. 3).

Таблица 3

Факторы риска, порождаемые элементами внешней среды АСУ КА

Элемент внешней среды	Фактор риска	
	непреднамеренный	преднамеренный
Разработчик ПО АСУ КА	Ошибочные решения по определению облика ПО АСУ КА Ошибки и просчеты в проектных решениях, касающихся ПО подготовки данных полета КА Ошибки в алгоритмах формирования и контроля данных полета КА Ошибки в программах ПО АСУ КА Недочеты в документации для ПО АСУ КА	Проектные «закладки» в составе и облике ПО АСУ КА Алгоритмические «закладки» в алгоритмах подготовки данных полета КА Программные «закладки» в программах подготовки данных полета КА Разглашение сведений о структуре и характеристиках ПО АСУ КА и ее комплекса средств защиты

Окончание табл. 3

Элемент внешней среды	Фактор риска	
	непреднамеренный	преднамеренный
Разработчик ТС АСУ КА	Ошибочные решения по определению облика ТС АСУ КА Ошибки в проектных решениях по ТС подготовки данных полета КА Ошибки в коммутации ТС АСУ КА Дефекты в ТС АСУ КА Недочеты в документации для ТС АСУ КА	Технические «закладки» в ТС подготовки данных полета КА Разглашение сведений о структуре, характеристиках ТС АСУ КА и комплекса ее средств защиты
Среда разработки ТС АСУ КА	Низкая надежность ТС АСУ КА Низкая производительность ТС АСУ КА	–
Среда разработки ПО АСУ КА	Низкая надежность ПО Низкая производительность программных средств, используемых в процессе подготовки данных полета КА	–

Неучет или неправильная организация взаимодействия среды разработки типа КА и среды разработки АСУ КА порождает следующие *основные факторы риска, которые непреднамеренно может инициировать разработчик ПО АСУ КА*:

- отсутствие или низкая достоверность контроля параметров системы управления КА;
- отсутствие или низкая достоверность контроля параметров, определяющих выполнение поставленной задачи.

Неучет или организация неправильного взаимодействия среды разработки типа КА со средой разработки АСУ КА порождает невозможность обеспечения выполнения поставленной задачи, если в системе управления КА и АСУ КА не будут учтены требования к их построению. Следовательно, при разработке алгоритмов подготовки данных полета КА должны учитываться необходимые средства контроля параметров данных полета КА.

Существующая система разработки ПО подготовки данных полета КА порождает еще один специфический *преднамеренный фактор риска, который реализуется разработчиком специального ПО (СПО) АСУ КА*: невозможность достоверного контроля выполнения ЗП, поскольку отсутствует учет несоответствия системы команд и вычислительных возможностей ПЭВМ, на которых реализовано СПО, системе команд и вычислительных возможностей бортовой цифровой вычислительной машины, на которой реализованы алгоритмы функционирования системы управления КА.

Для определения факторов риска, порождаемых недостатками организационно-технических мер и средств проведения качественных межведомственных испытаний (МВИ) разработанного СПО АСУ КА, необходимо рассмотреть существующую в настоящее время организационную структуру процесса разработки ПО АСУ КА.

Структура процесса разработки СПО АСУ КА порождает *факторы риска, связанные с действиями заказчика*. К преднамеренным факторам риска относятся решения заказчика об отсутствии алгоритмов функционирования СПО АСУ КА у представителя заказчика, об отсутствии возможности контроля СПО АСУ КА представителем заказчика на своих тестовых вариантах, об отсутствии утвержденной методики, по которой определяют обоснованное число испытаний СПО АСУ КА, необходимое для подтверждения требуемого значения показателя его надежности, а также утвержденной методики оценки показателя надежности ПО АСУ КА.

К непреднамеренным факторам относятся собственно отсутствие указанных алгоритмов функционирования СПО, невозможность контроля СПО на тестовых вариантах заказчика, а также отсутствие вышеперечисленных утвержденных методик.

К факторам риска, определяющим эксплуатационные характеристики качества АСУ КА, относятся следующие:

- сбои (отказы) ТС, реализующих информационную технологию, которая лежит в основе процесса функционирования АСУ КА;
- ошибочные действия персонала (оперативного, обслуживающего, сопровождающего);
- преднамеренное внедрение избыточных средств защиты;
- преднамеренное проектирование недостаточных средств защиты или средств защиты с низкими значениями показателей стойкости и чувствительности.

Последние два фактора риска могут быть непреднамеренно реализованы в результате недостаточно полного и корректного анализа влияния средств защиты как на информационную безопасность АСУ КА, так и на ее оперативность. В этом случае имеем *факторы риска, реализованные разработчиком АСУ КА непреднамеренным образом*:

- наличие избыточных средств защиты;
- наличие недостаточных средств защиты или средств защиты с низкими значениями показателей их качества (чувствительности и стойкости).

Источником факторов риска могут быть также вопросы организации МВИ разработанного СПО АСУ КА, за качество проведения которых несет ответственность заказчик. В этом случае имеем следующий *фактор риска, преднамеренно реализованный разработчиком*: допущение саботажа проведения МВИ (невыполнение требований технического задания, бездоказательное утверждение разработ-

чика, что представленный им продукт (т. е. СПО) является правильным, нарушение сроков сдачи СПО и т. п.).

Физическая среда АСУ КА в части ОТСС порождает такие *факторы риска*, как несанкционированный доступ неуполномоченных лиц:

а) в помещения со средствами вычислительной техники;

б) к автоматизированным рабочим местам.

Внутренняя информационная среда также служит источником ФР (табл. 4).

Таблица 4

Факторы риска, порождаемые внутренней информационной средой АСУ КА

Элемент внутренней информационной среды	Фактор риска
ПО ОТСС	«Зацикливание» программы «Зависание» программы
ТС ОТСС	Сбои ТС Отказы ТС Паразитные электромагнитные излучения и наводки
Система энергоснабжения, относящаяся к ВТСС	Сбои ТС, приводящие к кратковременному изменению напряжения Отказы ТС, приводящие к прекращению электропитания на длительный срок
СПТВР	Сбой ТС СПТВР, приводящий к кратковременному нарушению температурно-влажностного режима Отказ ТС СПТВР, приводящий к длительному нарушению температурно-влажностного режима

Перечисленные факторы риска не являются равнозначными ни с точки зрения мер и средств для нейтрализации ИФР, ни с точки зрения необходимых на нее затрат. Более того, существуют ИФР, которые не учитываются в алгоритмах СПО АСУ КА. К таким источникам относятся системы и агрегаты КА.

Существуют ИФР для нейтрализации которых не требуется проводить специальные научные исследования. Например, для нейтрализации ИФР, связанных с действиями заказчика, необходимо совершенствовать организационно-технические меры, направленные на обеспечение требуемого качества данных полета КА. Эффективность этих мер была доказана как теоретически, так и практически при запусках КА.

Для нейтрализации источников таких факторов риска, как недочеты в документации для ПО и ТС АСУ КА, необходимо повысить ответственность разработчика за выпуск технической и эксплуатационной документации, а в техническом задании на разработку АСУ КА должны быть указаны в явном виде требования к полноте и обоснованности документации, чтобы недочеты в документации расценивались как невыполнение требований технических заданий.

Для того чтобы защитить информационные ресурсы АСУ КА от угроз нарушения их безопасности, необходимо разработать как модель угроз, так и модель защиты, которые позволяли бы определять полный состав механизмов защиты.

Заключение. В настоящей статье предложен новый подход к классификации источников факторов риска АСУ КА. Такой подход позволил получить полное, непротиворечивое и неизбыточное множество факторов риска, для которых могут быть определены общие механизмы их обнаружения и нейтрализации. Полнота, неизбыточность и непротиворечивость полученных факторов риска доказаны математически строго в виде леммы, теоремы и ее следствия.

ЛИТЕРАТУРА

[1] Макаров Д.А., Розенберг М.Я., Шильников А.Б. О факторах риска в процессе разработки программного обеспечения. *Вестник ЮУрГУ*, 2009, № 37 (170), с. 85–92.

[2] *ГОСТ Р ИСО/МЭК 16085–2007. Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения*. Москва, Стандартинформ, 2009, 31 с.

[3] *Развитие организационных и методологических аспектов теории и практики расследования причин происшествий на объектах ракетной, ракетно-космической и авиационной техники*. Королёв, ФГУП ЦНИИмаш, 2015, 334 с.

[4] Гулевич С.П., Веселов Ю.Г., Прядкин С.П., Тырнов С.Д. Анализ факторов, влияющих на безопасность полета беспилотных летательных аппаратов. Причины авиационных происшествий беспилотных летательных аппаратов и способы их предотвращения. *Наука и образование*, 2012, № 12. DOI 10.7463/1212.0500452

[5] Белим С.В., Богаченко Н.Ф. Применение метода анализа иерархий для оценки рисков утечки полномочий в системах с ролевым разграничением доступа. *Информационно-управляющие системы*, 2013, № 6, с. 67–72.

[6] Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков. *Инженерный журнал: наука и инновации*, 2012, вып. 3. DOI 10.18698/2308-6033-2012-3-127

[7] Булдакова Т.И. Нейросетевая защита ресурсов автоматизированных систем от несанкционированного доступа. *Наука и образование*, 2013, № 5. DOI 10.7463/0513.0566210

[8] Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели. *Наука и образование*, 2013, № 11. DOI 10.7463/1113.0645489

[9] Шрейдер Ю.А., Шаров А.А. *Системы и модели*. Москва, Радио и связь, 1982, 152 с.

[10] Романов В., Бутуханов А. Рискообразующие факторы: характеристика и влияние на риски. *Сб. «Моделирование и анализ безопасности, риска и качества в сложных системах»*. Санкт-Петербург, Омега, 2001. URL: http://www.aup.ru/articles/finance/9.htm (дата обращения 01.09.2015).

Статья поступила в редакцию 10.05.2016

Ссылку на эту статью просим оформлять следующим образом:

Андреев А.Г, Казаков Г.В., Корянов В.В. Метод определения факторов риска для автоматизированной системы управления полетами космических аппаратов. *Инженерный журнал: наука и инновации*, 2016, вып. 7.

http://dx.doi.org/10.18698/2308-6033-2016-07-1511

Статья подготовлена по материалам доклада, представленного на XL Академических чтениях по космонавтике, посвященных памяти академика С.П. Королёва и других выдающихся отечественных ученых — пионеров освоения космического пространства, Москва, МГТУ им. Н.Э. Баумана, 26–29 января 2016 г.

Андреев Анатолий Георгиевич — канд. техн. наук, старший научный сотрудник ФГБУ «4 ЦНИИ» Минобороны России. Автор более 60 работ в области надежности автоматизированных систем управления. e-mail: kgv.64@mail.ru

Казаков Геннадий Викторович — канд. техн. наук, доцент, начальник управления ФГБУ «4 ЦНИИ» Минобороны России. Автор более 50 работ в области надежности автоматизированных систем управления. e-mail: kgv.64@mail.ru

Корянов Всеволод Владимирович — канд. техн. наук, доцент, первый заместитель заведующего кафедрой «Динамика и управление полетом ракет и космических аппаратов» МГТУ им. Н.Э. Баумана. Автор более 40 публикаций.
e-mail: vkoryanov@bmstu.ru

Method for determining risk factors for the spacecraft flight automated control system

© A.G. Andreev[1], G.V. Kazakov[1], V.V. Koryanov[2]

[1]Federal State Budgetary Institution 4th Central Research Institute of the Ministry of Defense of the Russian Federation, Korolev, Moscow region, 141091, Russia
[2] Bauman Moscow State Technical University, Moscow, 105005, Russia

Classification of objects is a well-studied problem which solved many important practical tasks. There is a variety of classification methods, which are related to the construction of trees according to the features selected, as a rule, from the physical meaning of the problem to be solved. But no formal demands were made of these features. The article posed and solved the problem of obtaining a complete, non-redundant and consistent set of risk factors that are the basis for developing appropriate tools to neutralize them. We solve the problem by using binary relations and mathematical apparatus of the theory of sets and give a rigorous mathematical proof of the result. Moreover, we show the practical application of this method to the practice of determining risk factors in relation to the spacecraft flight automated control system.

Keywords: *automated control system, spacecraft, reliability, software, risk factor.*

REFERENCES

[1] Makarov D.A., Rozenberg M.Ya., Shilnikov A.B. *Vestnik YuUrGU — Bulletin of the South Ural State University,* 2009, no. 37 (170), pp. 85–92.

[2] *GOST R ISO/MEK 16085–2007. Menedzhment riska. Primenenie v protsessakh zhiznennogo tsikla sistem i programmnogo obespecheniya* [State Standard 16085–2007. Risk management. Application in system lifecycle and software processes]. Moscow, Standartinform Publ., 2009, 31 p.

[3] *Razvitie organizatsionnykh i metodologicheskikh aspektov teorii i praktiki rassledovaniya prichin proishestviy na obyektakh raketnoy, raketno-kosmicheskoy i aviatsionnoy tekhniki* [Development of organizational and methodological theory and practice aspects of investigating the reasons of accidents at the units of rocket, rocket and space and aviation machines]. Korolev, Moscow region, Federal State Unitary Enterprise Central Research Institute Mechanical Engineering, 2015, 334 p.

[4] Gulevich S.P., Veselov Yu.G., Pryadkin S.P., Tyrnov S.D. *Nauka i obrazovanie — Science and Education*, 2012, no. 12. DOI 10.7463/1212.0500452

[5] Belim S.V., Bogachenko N.F. *Informatsionno-upravlyayushchie sistemy — Information and Control Systems*, 2013, no. 6, pp. 67–72.

[6] Buldakova T.I., Mikov D.A. *Inzhenernyy zhurnal: nauka i innovatsii — Engineering Journal: Science and Innovation,* 2012, no. 3. DOI 10.7463/0513.0566210

[7] Buldakova T.I. *Nauka i obrazovanie — Science and Education*, 2013, no. 5. DOI 10.7463/0513.0566210

[8] BuldakovaT.I., MikovD.A. *Nauka i obrazovanie — Science and Education*, 2013, no. 11. DOI 10.7463/1113.0645489

[9] Shreider Yu.A. *Sistemy i modeli* [Systems and models]. Moscow, Radio i svyas Publ., 1982, 152 p.

[10] Romanov V., Butukhanov A. Riskoobrazuyushchie faktory: kharakteristika i vliyanie na riski [Risk generating factors: characteristics and influence on

risks]. V sbornike "*Modelirovanie i analiz bezopanosti, riska i kachestva v slozhnykh sistemakh*" [In coll. papers "Modeling and analysis of safety, risk and quality in complicated systems"]. St. Petersburg, Scientific Production Association Omega, 2001. Available at:
http://www.aup.ru/articles/finance/9.htm (accessed September 01, 2015).

Andreev A.G. (b. 1941) Cand. Sci. (Eng.), Senior Research Scientist of Federal State Budgetary Institution 4th Central Research Institute of the Ministry of Defense of the Russian Federation. Author of more than 60 works in the field of automated control system reliability. e-mail: kgv.64@mail.ru

Kazakov G.V. (b. 1964) Cand. Sci. (Eng.), Assoc. Professor, head of the Federal State Budgetary Institution 4th Central Research Institute of the Ministry of Defense of the Russian Federation. Author of more than 50 works in the field of automated control system reliability. e-mail: kgv.64@mail.ru (SPIN-code: 8553-9753).

Koryanov V.V. (b. 1982) graduated from Bauman Moscow State Technical University in 2006. Cand. Sci. (Eng.), Assoc. Professor of the Department of Dynamics and Control of Rocket and Spacecraft Flight. Author of more than 20 works in the field of ballistics modelling and dynamics of spacecraft and descent vehicle motion.
e-mail: vkoryanov@bmstu.ru