УДК 629.7

ПОДХОД К ОБЕСПЕЧЕНИЮ ОТКАЗОУСТОЙЧИВОСТИ КОСМИЧЕСКИХ АППАРАТОВ НА ОСНОВЕ АВТОМАТИЗАЦИИ ПРОЕКТИРОВАНИЯ ИНТЕЛЛЕКТУАЛЬНЫХ БОРТОВЫХ ПРОГРАММНЫХ СРЕДСТВ

А. А. Тюгашев

Введение

Современный космический аппарат (КА) представляет собой классический пример сложного технического комплекса (СТК). Сложность здесь подразумевает два важных аспекта. Первый – значительное число входящих в состав комплекса компонент, связанных между собой множеством связей различной природы. Действительно, КА включает целый ряд подсистем: систему автономной навигации, систему терморегулирования, систему энергоснабжения, систему телеметрических измерений, целевую аппаратуру. Каждая из систем, в свою очередь, состоит из множества приборов, агрегатов, датчиков. Всего на борту насчитываются сотни устройств, имеющих большое число параметров, режимов работы, воспринимаемых команд. Второй аспект сложности подразумевает сложное поведение, которое трудно предсказать заранее [1], а описать аналитически – практически невозможно. Неудивительно, что в реальных космических полетах происходят отказы, вызываемые различными причинами, среди которых – аппаратные сбои и ошибки в программном обеспечении.

При этом, учитывая трудоемкость и стоимость создания, для ракетно-космической техники важнейшей характеристикой является надежность. Надежность является комплексной характеристикой, включающей в том числе свойства устойчивости и восстанавливаемости, которые могут также рассматриваться как составляющие живучести – свойства более широкого, подразумевающего способность выполнения целевой задачи при наличии неблагоприятных факторов и в ненормированных условиях функционирования [2]. Отказоустойчивость подразумевает, что КА может адаптироваться к ненормативным условиям и (возможно, с некоторым снижением качества) продолжить выполнение возложенных на него задач в непредвиденных условиях и при воздействии аномальных факторов. Восстанавливаемость означает способность КА вернуться в работоспособное состояние после сбоя или аварии путем, например, реконфигурации бортовых средств, подключения резервных комплектов бортовой аппаратуры и пр.

1. Обеспечение живучести космических аппаратов

Для традиционных машин и механизмов, эксплуатируемых на Земле, восстановление работоспособности обычно подразумевает диагностику и ремонт, проводимые человеком. Ремонт автоматического космического аппарата, находящегося на орбите, как правило, невозможен (известны лишь уникальные случаи, как с космическим телескопом «Хаббл», ремонт которого осуществляли экипажи корабля «Спэйс Шаттл»). Рассчитывать приходится лишь на структурную или функциональную избыточность имеющегося на борту оборудования и на программные средства.

В течение всего срока активного существования (САС) необходимо решать задачу определения множества управляющих воздействий, необходимых для поддержания требуемой для реализации конкретной бортовой функции конфигурации бортовых средств. При этом обязательным является парирование отказа единичного устройства без потери качества или функциональности. В случае диагностики отказа происходит реконфигурация аппаратуры с использованием «горячего» или «холодного» резерва либо перевод КА в один из специальных «безопасных» режимов, в которых развитие аварийной ситуации, способное привести к катастрофической потере работоспособности, исключается.

Важнейшая роль в обеспечении живучести КА возлагается на бортовое программное обеспечение, выполняющее функции контроля и диагностики, а в случае необходимости – управления

в нештатной ситуации (при управлении КА для этого может использоваться специальный «паттерн» управления или режим работы КА в случае возникновения неисправностей [2]).

При разработке алгоритмов контроля и диагностики на основе инженерного анализа бортовой аппаратуры (БА) с учетом имеющихся резервов и предшествующего накопленного опыта эксплуатации выявляется список критических отказов и формируется оценка их важности, разрабатываются диаграммы состояния и временные циклограммы режимов управления [2, 3]. Известны ситуации, когда работоспособность КА в целом (хотя и с некоторым снижением качества) восстанавливается путем использования того или иного бортового оборудования для решения изначально не планировавшихся задач (например, после отказа гироскопических датчиков-измерителей перевод системы стабилизации на использование в качестве основного источника информации звездных датчиков). Достижение этого требует переработки бортовых алгоритмов и программ и загрузки измененного ПО на борт [2].

Традиционным и широко применяемым до сих пор является метод командного телеуправления, который реализуется с привлечением наземного комплекса управления (НКУ) для анализа состояния КА, выработки решений о выдаче соответствующей совокупности управляющих воздействий и выдачи на борт управляющих воздействий в реальном времени [4]. В этом случае в течение всего срока активного существования КА с ним непрерывно должен работать наземный комплекс управления (НКУ). Данный комплекс включает станцию приема телеметрической информации и выдачи на борт командно-программной информации, линии связи этой станции с центром управления полетом (ЦУП), средства ЦУПа по обработке и представлению телеметрической информации, по формированию и выдаче командно-программной информации. Постоянно в состоянии полной готовности должен находиться персонал, отлично владеющий эксплуатационной документацией и способный оперативно и ответственно принимать решения о выдаче команд на борт. Но в этом случае речь может идти о реакции на изменение ситуации на борту не ранее, нежели через несколько минут. Возможно улучшение качества управления за счет, например, интеллектуальной поддержки процессов принятия решения оператором, в том числе с использованием баз знаний. Но потери времени на обмен между КА и Землей, постоянные затраты на поддержание непрерывной работы средств НКУ органически присущи данному методу. В некоторых случаях подключение персонала НКУ вообще не представляется возможным ввиду особенностей орбит КА (например, для низкоорбитальных спутников Земли с коротким интервалом видимости с каждого из наземных пунктов или автоматических межпланетных станций с длительным временем прохождения радиосигнала), что при быстром развитии аномальной ситуации на борту делает последующее вмешательство с Земли уже бесполезным.

Кардинальным решением проблемы является максимальная степень реализации концепции автономного управления. Данный подход подразумевает перенос принятия решений на бортовые средства с оставлением за НКУ только постановки общих задач и целей функционирования и последующего контроля.

Для случая автоматических (беспилотных) КА средства автономного управления приобретают важнейшее значение, обеспечивая сохранение работоспособности и выполнение поставленных перед КА задач без участия человека. Эффективность автономного управления зависит от полноты и корректности хранящихся на борту необходимых для принятия решений знаний и от характеристик механизма принятия решений в условиях ограниченных бортовых вычислительных ресурсов.

Традиционно логика управления КА, в том числе в случае возникновения нештатных ситуаций, жестко «зашита» в код управляющих программ [4, 5]. Однако известны и более гибкие подходы к решению проблемы.

Весьма интересен опыт развивавшейся в СССР с конца 60-х гг. школы ситуационного управления (Д. А. Поспелов, Ю. И. Клыков, Л. С. Загадская и др.) [6]. Подход использовался для решения задач управления, когда другие методы не давали решения. В ситуационных моделях использовались знания об объекте управления и методах управления им, а также применялись такие традиционные для ИИ приемы, как описание ситуаций, складывающихся на объекте управления на ограниченном и формализованном естественном языке, использование псевдофизических логик для оценки и преобразования ситуаций, обучение при накоплении информации в памяти системы, планирование целесообразных действий по управлению и использованию информации от технологов и управленцев.

2. Бортовые базы знаний как средство обеспечения живучести

Значительный опыт имеется в данной проблемной области у ОАО «Информационные спутниковые системы» (г. Железногорск). На борту создаваемых ими аппаратов в составе БПО присутствуют специальные интерпретаторы правил [4, 7], фактически являющиеся упрощенным аналогом машины вывода классической экспертной системы.

Специализированный интерпретатор правил «Дежурный контроль и диагностика» (ДКД), называемый в терминологии Заказчика также «макропрограммой», предназначен для обнаружения и парирования возникающих на борту КА отказов. Разработка правил осуществляется непосредственно специалистами по системам КА с помощью специально созданного проблемно-ориентированного языка. Система формирования правил обеспечивает таблично-ориентированный ввод. После чего происходит преобразование правил в бортовые структуры данных. Правила для интерпретатора ДКД организованы в виде совокупности матриц векторов состояний и связанных с ними последовательностей управляющих действий [7, 8].

Большая часть работы по верификации правил осуществляется на наземном комплексе отладки (НКО). Основу НКО составляет программный имитатор КА, включающий в себя программные модели всего бортового оборудования и штатное бортовое программное обеспечение, работающее в среде программной модели бортового вычислительного комплекса [7]. К моменту готовности КА к запуску количество правил автономного принятия решений достигает нескольких сотен. В процессе эксплуатации это количество обычно увеличивается еще на 20–30 % [4, 7]. Возможность разработки новых правил специалистами по бортовым системам без привлечения программистов делает средства автономного управления эффективным средством «ремонта» и улучшения характеристик КА в течение всего срока активного существования.

Как известно, база знаний обычно входит в состав экспертной системы и представляет собой набор структурированных знаний, часто в форме «ЕСЛИ … ТО…», и описывающих, например, способ вывода некоего заключения на основе имеющихся посылок [9, 10].

Классическая структура подразумевает следующие компоненты:

1) база знаний;

2) человеко-машинный интерфейс (диалоговый компонент);

3) машина вывода («решатель»);

4) средства приобретения знаний (компонент приобретения знаний);

5) подсистема объяснения (объяснительный компонент).

В структуре экспертной системы может также присутствовать база данных. Для случая бортовой базы знаний в базе данных накапливаются статические и динамические параметры, описывающие параметры аппарата, орбиты и пр. Постоянная часть содержит статические данные о КА и других КА группировки, решающих совместно целевую задачу. Переменная часть содержит данные, которые меняются в процессе полета – координаты, скорости, угловое положение КА и других КА [2, 3]. В силу ограниченности бортовых вычислительных ресурсов база должна быть очень компактной.

Обозначим $L = \{\alpha_i\}$ – множество условий (относящихся к значениям контролируемых телеметрических параметров), отображающих ситуацию на борту КА. Из элементов множества L можно сформировать вектор текущего состояния (ВТС) КА. Некоторые векторы будут соответствовать штатным ситуациям, некоторые – аномальным.

$F = \{ f_j \} = K \cup P$ – множество действий, включающее в себя K – множество команд управления (КУ) бортовой аппаратурой (БА) и P – специальных бортовых программ, включенных в паттерн обеспечения живучести.

Правило бортовой базы знаний, направленной на обеспечение живучести КА, может выглядеть в таком случае как отображение $L \rightarrow F$.

Можно разделить бортовую базу знаний на две части. Первая содержит правила установления наличия той или иной нештатной (аномальной) ситуации.

Вторая – правила выхода из данной ситуации, которые могут оперативно пополняться и меняться специалистами с Земли по радиоканалу.

В первой части правила имеют вид $L \rightarrow A$, во второй $A \rightarrow F$ или, более точно, $A \times T \rightarrow F \times T$, где T – множество моментов бортовой шкалы времени, поскольку может иметь значение время проверки тех или иных условий, а выдача управляющего воздействия для восстановления работо-

способности КА – представлять собой не единичный акт, а циклограмму, реализующую набор операций, взаимоувязанных по времени, например:

$$[(\alpha_5, \alpha_3, \leftarrow \alpha_1), 0] \rightarrow <f_1, 0>, <f_2, 100>, <f_3, 260>,$$

где 0, 100, 260 – моменты времени t_i выполнения необходимых действий. Отметим, что некоторые действия могут быть связаны при этом с формированием условий, входящих в L (приданием им значений истинности или ложности).

Таким образом, в сравнении с традиционными правилами вывода базы знаний, в которых фигурируют в обеих частях предикаты (условия), например, $\alpha_1 :- \alpha_2, \alpha_3, \alpha_5$, означает, что при истинности α_2, α_3 и α_5 истинным нужно считать и α_1, мы можем сказать, что аналогом правой части будет являться логический вектор (вектор текущего состояния), а левой части – как предикат, который необходимо считать истинным в данном случае, так и набор привязанных к моментам времени определенных действий.

В широком смысле упомянутый набор операций может включать алгоритмы реакции на нештатные ситуации, диагностики систем, алгоритмы принятия решений, перехода в случае необходимости в заранее предусмотренные устойчивые состояния.

Формализация, структуризация и использование правил по управлению КА могут рассматриваться как неотъемлемая часть технологии информационной поддержки изделия (CALS-технологии) [5].

Отметим, что в описанных бортовых средствах не происходит самостоятельного порождения новых знаний, новых правил, что делает весьма актуальной проблему создания и развития средств приобретения знаний по управлению живучестью КА.

При этом, как известно, весьма важной проблемой при использовании любых баз знаний является их наполнение [6, 9, 10]. Нередка ситуация, когда эксперт – носитель необходимых знаний, не являющийся математиком или специалистом в области информационных технологий, испытывает затруднения при формализованном их представлении, необходимом для внесения в машину. Еще одной существенной проблемой является обеспечение таких свойств, как непротиворечивость и целостность вносимых в базу знаний. Посредником здесь может выступать специалист – инженер по знаниям, однако в подобном случае нельзя полностью исключать возникновения эффекта «испорченного телефона».

Между людьми, участниками процесса, могут возникать недопонимание, использование различных систем понятий и пр. С целью разрешения данного противоречия используются различные подходы, например, использование диалоговых подсистем, взаимодействующих с пользователем на естественном языке (ЕЯ) или некоем подмножестве ЕЯ (язык «деловой прозы», см., например, [6] и пр. Система может даже «уметь» задавать пользователю уточняющие вопросы. Однако даже диалоговый режим с последовательным уточнением не может полностью исключить неточности и ошибки в силу таких особенностей ЕЯ, как неточность и многозначность.

3. Средства визуализации и графического конструирования правил бортовой базы знаний

Говоря о знаниях и интеллектуальных системах вообще, имеет смысл обратить внимание на графическую форму представления информации [11, 12]. Человек привык жить в материальном мире, ему довольно трудно разбираться с «виртуальными», информационными объектами, коими по своей сути являются программы. При этом одной из наиболее естественных форм представления (восприятия) информации для человека является графический образ. К этой форме человек прибегает всякий раз (возможно неявно для себя), когда необходимо решать действительно сложные задачи. Человеческая культура «визуально ориентирована», достаточно упомянуть фотографии, кинофильмы, телевидение, презентации. В качестве типичных эпитетов для графического представления используются «дружественный», «интуитивный», «простой», «привлекательный», «понятный», «запоминающийся» и пр. Графика позволяет использовать метафору – представление новых или необычных для пользователя явлений через другие явления, хорошо ему известные из повседневной жизни [9]. Можно отметить удачное соответствие графики требованиям этапов постановки задачи и проектирования. Использование визуального представления позволяет создавать более компактные и наглядные спецификации. Упрощается понимание в процессе взаимодействия инженеров-системщиков, математиков и пр. Преимущества визуального представ-

ления за счет улучшения координации и взаимопонимания участников работ, дают возможность повышения производительности труда.

В настоящее время под руководством автора по заказу АО «ИСС» проводятся опытно-конструкторские работы по созданию СИПР МП – системы интеллектуальной поддержки процессов проектирования и верификации макропрограмм интегрального управления. Разрабатываемое инструментальное программное обеспечение должно по требованиям технического задания «без швов» интегрироваться с существующими форматами и программным обеспечением. Необходимо обеспечить возможность визуализации структуры ранее созданных с применением использовавшихся ранее представлений и инструментов правил; изменения (графического редактирования) существующих правил с адекватным отражением всех изменений в имеющейся бортовой базе правил формата Заказчика; конструирования в специальном программном средстве новых правил «с нуля».

На данный момент (стадия опытного образца) был создан инструмент, позволяющий визуализировать и конструировать макропрограммы дежурного контроля и диагностики, выполняемые на борту периодически и контролирующие текущие параметры объекта с целью выявления сигнатур аномальных ситуаций (АС).

Визуальное представление позволяет с использованием специально разработанной совместно с заказчиками нотации представлять правила базы знаний. Представление позволяет моментально (симультанно) увидеть суть посылок и заключений. Разработан редактор, с помощью которого можно отображать в наглядной эргономичной форме правила базы знаний (рис. 1).

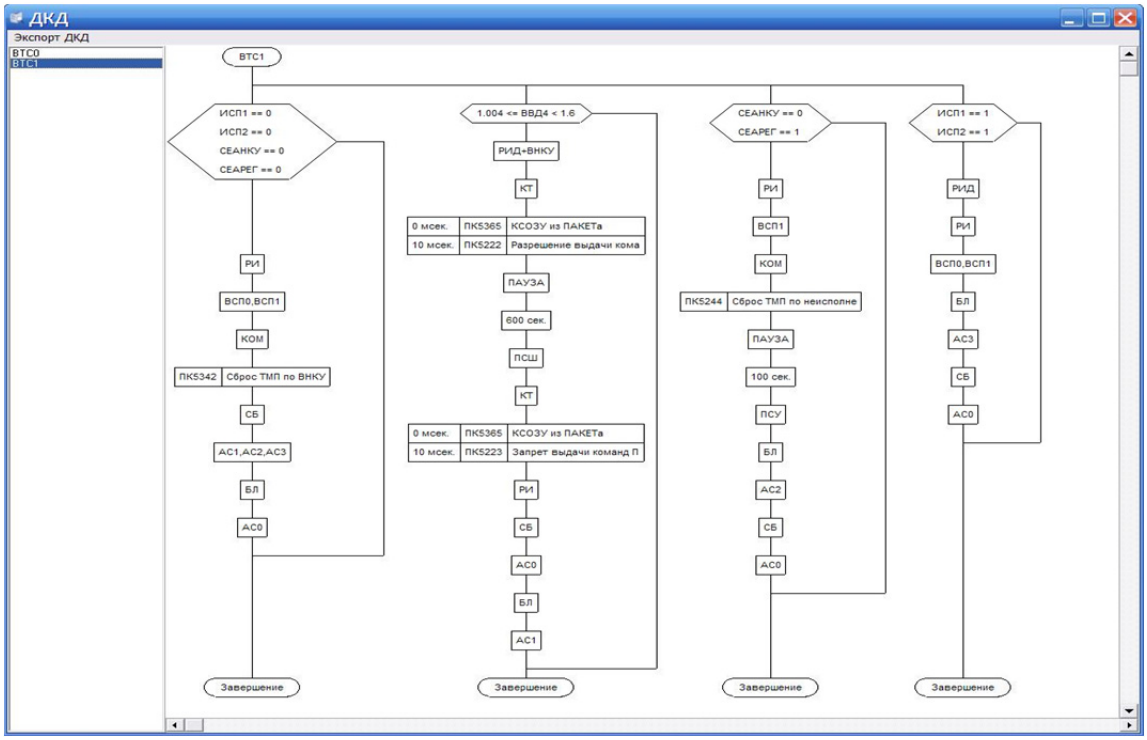

Рис. 1. Экран средств визуализации и графического конструирования правил

Исходно нотация основана на классических блок-схемах алгоритмов и программ, однако во многом учтены идеи В. Д. Паронджанова [12], обеспечивающие наглядность, ясность, быстроту и целостность восприятия схем. В частности, пересечения линий строго запрещены. При использовании графического примитива, соответствующего условию, ветвь «Да» всегда идет по вертикали вниз, «Нет» – направо. Самый «наихудший» или «редкий» случай отображается как можно правее. Макропрограмма представляет собой группу правил, отображаемую неким аналогом схемы «силуэт» Паронджанова. «Силуэт» состоит из вертикальных ветвей. В каждой ветви при использовании разработанной совместно с представителями Заказчика визуальной нотации фигурирует одно условие (имеющее как правило сложный характер и соответствующее частному вектору состояния СТК), в случае истинности которого выполняются расположенные ниже действия [13, 14].

В связи с тем, что в структуре макропрограмм существуют команды для перехода к анализу другого правила, был также разработан визуализатор связей. Макропрограмма представляется графом, в котором множество ребер отражает связи между группами правил (рис. 2).

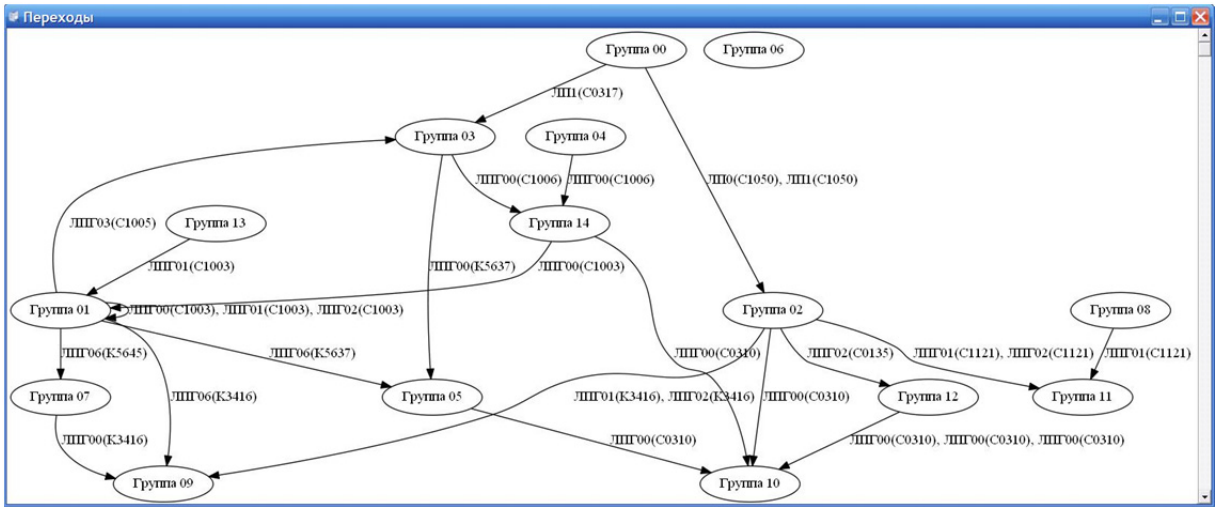

Рис. 2. Экран визуализации связей между группами правил

При этом, помимо средств визуализации и графического конструирования правил, СИПР МП подразумевает разработку:

– интегрирующей оболочки;

– средств автоматизации верификации правил;

– средств автоматизированной генерации документирования;

– системы контроля версий документации и наборов правил базы знаний.

Интегрирующая оболочка позволяет выбрать проект (набор правил, соответствующий макропрограмме), с которым предстоит работать. Средства автоматизации верификации на основе структуры правил способны автоматически подготавливать исходные данные и в перспективе запускать процесс автоматической верификации макропрограмм. Система документирования позволяет автоматически создавать требуемый набор документов с использованием шаблонов.

Таким образом, использование СИПР МП должно позволить улучшить понимание разработчиками правил принятия решений в нештатных ситуациях, повысить удобство изменения правил и добавления новых, сократить трудоемкость и сроки, в конечном счете – повысить надежность автономного управления КА.

Список литературы

1. Мостовой, Я. А. Лекции по управлению сложными техническими системами : учеб. пособие / Я. А. Мостовой. – Самара : ФГБОУ ВПО ПГУТИ, 2014 – 192 с.
2. Методы обеспечения живучести низкоорбитальных автоматических КА зондирования Земли: математические модели, компьютерные технологии / А. Н. Кирилин, Р. Н. Ахметов, А. В. Соллогуб, В. П. Макаров. – М. : Машиностроение, 2010. – 425 с.
3. Принципы диагностики системы управления космического аппарата / А. И. Заведеев, А. Ю. Ковалев, А. С. Сыров, М. А. Шатский // Системы управления беспилотными космическими и атмосферными летательными аппаратами : тез. докл. науч.-техн. конф. – М. : МОКБ «Марс», 2010. – 362 с.
4. Хартов, В. В. Автономное управление космическими аппаратами связи, ретрансляции и навигации / В. В. Хартов // Авиакосмическое приборостроение. – 2006. – № 6. – С. 29–33.
5. Тюгашев, А. А. Пути повышения надежности и качества программного обеспечения в космической отрасли / А. А. Тюгашев, И. А. Ильин, И. Е. Ермаков // Управление большими системами : сб. тр. / Ин-т проблем управления им. В. А.Трапезникова РАН. – М., 2012. – Вып. 39. – С. 288–299.
6. Поспелов, Г. С. Искусственный интеллект – основа новой информационной технологии / Г. С. Поспелов. – М. : Наука, 1988. – 186 с.
7. Колташев, А. А. Эффективная технология управления циклом жизни бортового программного обеспечения спутников связи и навигации / А. А. Колташев // Авиакосмическое приборостроение. – 2006. – № 12. – С. 20–25.

8. Кочура, Е. В. Разработка макропрограмм интегрального управления космическими аппаратами / Е. В. Кочура // Вестник СибГАУ. – 2011. – Т. 1. – С 105–107.
9. Федунов, Б. Е. Проблемы разработки бортовых оперативно-советующих экспертных систем / Б. Е. Федунов // Известия РАН. Теория и системы управления. – 1996. – № 5. – С. 147–159.
10. Гаврилова, Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский. – СПб. : Питер, 2001. – 384 с.
11. Тюгашев, А. А. Графические языки программирования и их применение в системах управления реального времени / А. А. Тюгашев. – Самара : Изд-во Самар. науч. центра РАН, 2009 – 159 с.
12. Пароджанов, В. Д. Дружелюбные алгоритмы, понятные каждому / В. Д. Пароджанов. – М. : ДМК Пресс, 2010. – 464 с.
13. Северцев, Н. А. Системный анализ определения параметров состояния и параметры наблюдения объекта для обеспечения безопасности / Н. А.Северцев // Надежность и качество сложных систем. – 2014. – № 1. – С. 4–10.
14. Юрков, Н. К. Оценка безопасности сложных технических систем / Н. К. Юрков // Надежность и качество сложных систем. – 2014. – № 2. – С. 13–19.

Тюгашев Андрей Александрович
доктор технических наук, профессор,
кафедра компьютерных образовательных технологий,
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
(197101, Россия, г. Санкт-Петербург, Кронверкский пр., 49)
E-mail: tau797@mail.ru

Аннотация. *Актуальность и предмет исследования*. Проблема отказов в космических полетах остается одной из наиболее важных и сложных. Важнейшую роль в обеспечении отказоустойчивости играют бортовые программные средства автономного управления. *Методы*. В отличие от прямого кодирования правил управления в случае возникновения неисправностей, в коде бортового программного обеспечения намного более гибким и экономным является подход на основе интеллектуальных средств, например, бортовых интерпретаторов правил реального времени. Правила при этом могут быть в оперативном режиме изменены по радиоканалу с Земли. Существенно, что правила могут быть заданы проектантами и другими специалистами, не являющимися профессиональными программистами. В работе предложено применение для этого интуитивно понятной визуальной нотации. *Результаты*. Разработан визуальный язык для эргономичного представления правил бортовых интеллектуальных средств автономного управления. Созданные инструментальные средства позволяют визуализировать ранее построенные правила управления, а также строить новые в графическом конструкторе. Ведется работа над средствами автоматизации верификации правил и средствами автоматизации документирования. *Выводы*. Эргономичное представление правил позволяет улучшить взаимопонимание в коллективе разработчиков правил, сократить число неточностей и ошибок, за счет этого повысить надежность космических миссий.

Tjugashev Andrej Aleksandrovich
doctor of technical science, professor,
sub-department of computer educational technologies,
St. Petersburg National Research University
of Information Technologies, Mechanics and Optics
(197101, 49 Kronverksky avenue, Saint Petersburg, Russia)

Abstract. *Background*. The problem of dependability remains one of the most important in modern space missions. The onboard autonomous control software plays a key role in Fault Tolerance. *Methods*. In contrast to rigid method when control logic is to be implemented in program source code, we utilize onboard intelligent real-time interpreter of rules. Rules for autonomous control in contingencies can be operatively uploaded and updated from the Earth by radio. The main idea of the proposed method is integration of onboard intelligent software with the power of visual representation. *Results*. The Visual Domain Specific Language for ergonomic representation of the rules of onboard intelligent autonomous control programs has been designed. The easy-to-understand form allows reducing influence of human factor. The non-programmer can specify and refine rules using specially developed Toolset. Future works include development of rules verification tool and automated documentation generation tool. *Conclusions*. The ergonomic representation of the rules allows decreasing of misunderstanding in project team and reducing the number of inaccuracies and errors. Eventually, one can improve the dependability of Space Missions.

Ключевые слова: бортовая база знаний реального времени, космический аппарат, отказоустойчивость, автономное управление, визуальное конструирование, автоматизация тестирования программ, автоматизация документирования.

Key words: knowledge base, spacecraft, fault tolerance, independent management, visual design, software test automation, document automation.

УДК 629.7

Тюгашев, А. А.

Подход к обеспечению отказоустойчивости космических аппаратов на основе автоматизации проектирования интеллектуальных бортовых программных средств / А. А. Тюгашев // Надежность и качество сложных систем. – 2016. – № 2 (14). – С. 9–16.