УДК 62-501.72:681.326.7 DOI: 10.18698/2308-6033-2022-5-2180

Обеспечение отказоустойчивости в многомашинных вычислительных системах дистанционного зондирования Земли при ограниченных аппаратурных ресурсах

© И.В. Ашарина[1,2], В.Ю. Гришин[1], В.Г. Сиренко[1]

[1]АО «НИИ «Субмикрон», Москва, Зеленоград, 124460, Россия
[2]НИУ МИЭТ, Москва, Зеленоград, 124498, Россия

Рассмотрены вопросы построения сбое- и отказоустойчивых систем управления группировками космических аппаратов дистанционного зондирования Земли. Определено понятие комплекса, отказоустойчиво выполняющего целевую задачу, в данном случае — задачу обнаружения целевого события и наблюдения за его поведением или развитием (т. е. мониторинга целевого события). Предложена иерархическая структура организации группировки космических аппаратов. Обоснована необходимость применения динамической избыточности, позволяющей существенно увеличить траекторию самоуправляемой деградации и, соответственно, сроки активного существования группировки космических аппаратов. Сложность проблемы заключается в обеспечении достоверности полученных результатов при появлении большого количества целевых событий, которыми могут быть как природные явления, так и события, носящие техногенный характер. Предложен подход, позволяющий уменьшить аппаратурную избыточность, т. е. вести мониторинг большего числа событий с помощью группировки космических аппаратов меньшей мощности. Доказана возможность применения предложенного подхода без потери гарантоспособности системы.

Ключевые слова: *распределенная многомашинная вычислительная система; сбое- и отказоустойчивость; динамическая избыточность; враждебная неисправность, дистанционное зондирование Земли, группировки космических аппаратов*

Введение. Построение сбое- и отказоустойчивых систем управления группировками космических аппаратов (КА) дистанционного зондирования Земли (ДЗЗ), выполняющих задачи мониторинга целевых событий (таких как лесной пожар, взрыв, активное поведение вулкана, сход снежной лавины, запуск чужой ракеты и т. д.), представляет собой сложную и актуальную проблему, особенно в настоящее время, когда экологические и техногенные катастрофы не только наносят существенный урон экономике, но и создают угрозы экосистемам и человеческим жизням, порой ставя на грань выживания целые регионы. Сложность разрешения этой проблемы существенно возрастает при появлении большого числа таких целевых событий.

Предполагается, что существует группировка малых КА известной структуры, в которой КА всегда имеют информационную связь между собой, причем не обязательно «каждый-с-каждым». Считается, что

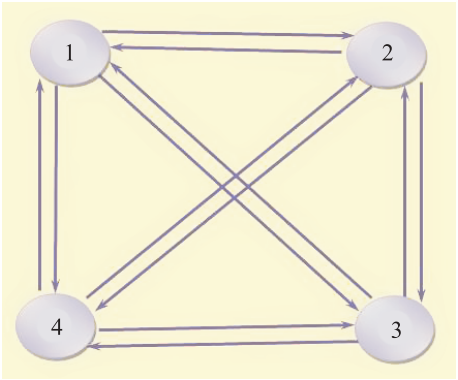
структура такой системы не нарушается при движении КА по своим орбитам, принципы ее построения полностью укладываются в принципы построения распределенных многомашинных вычислительных систем (РМВС) [1, 2]. Здесь под РМВС понимаются одноранговые (пиринговые), гетерогенные системы — сильно связанные информационно-управляющие системы, возможно, с неоднородными вычислителями и разнотипными каналами межмашинных связей (дуплексные, симплексные и широковещательные каналы связи). В случае наличия симплексных или широковещательных каналов связи моделью РМВС будет ориентированный граф (орграф).

На каждом КА находится неизбыточный вычислитель, являющийся цифровой вычислительной машиной (ЦВМ), управляющий КА, выполняющий целевые задачи и содержащий информацию о структуре сети. Далее под КА понимаются именно их вычислители. В качестве модели неисправности принято наличие кратных враждебных (так называемых Византийских) неисправностей [3] вычислителей КА, при которых сбое- и отказоустойчивость решаемых задач обеспечивается наличием комплекса [1, 2] из $n \geq 3\mu + 1$ КА (вычислителей, ЦВМ), где μ — отказоустойчивость, т. е. допустимое количество неисправных элементов комплекса. Здесь ***комплексом*** называется совокупность ЦВМ, отказоустойчиво выполняющая одну целевую задачу (например, методом программной репликации), удовлетворяющая определенным структурным требованиям [1, 2], в которой каждая исправная ЦВМ может определить вектор согласованных значений всех ЦВМ этого комплекса. Назовем комплекс, выделяемый для мониторинга *i*-го целевого события ($ЦС_i$), комплексом мониторинга $ЦС_i$.

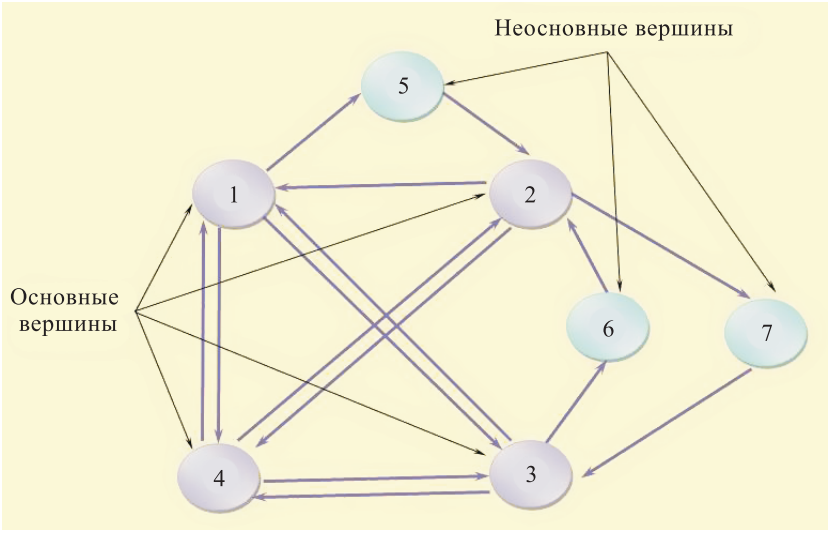
Цель исследования — разработка модели поведения распределенной сбое- и отказоустойчивой системы управления группировкой малых КА ДЗЗ в условиях появления большого количества целевых событий.

Основные принципы построения отказоустойчивого комплекса. Комплекс является необходимым инструментом при организации сбое- и отказоустойчивых вычислений на основе репликации задач в системах с динамической избыточностью и управляемой деградацией. При таком подходе к обеспечению сбое- и отказоустойчивости и при параллельном решении в системе нескольких задач, взаимно обменивающихся информацией, необходимо наличие в системе нескольких комплексов, каждый из которых решает одну из задач и в каждом из которых допускается наличие определенного для данного комплекса количества неисправных ЦВМ. Такие системы называются многокомплексными.

Полным орграфом называется орграф, имеющий пару разнонаправленных дуг между любыми двумя вершинами (рис. 1, *а*). Орграфы являются гомеоморфными, если существуют их изоморфные преобразования, образующиеся в результате подразбиения дуг (рис. 1, *б*) [4].



а



б

Рис. 1. Примеры полного орграфа (*а*) и орграфа, гомеоморфного полному (*б*)

Комплекс должен удовлетворять следующим структурным требованиям: в системном графе T комплекса имеется подграф H, полный или гомеоморфный полному графу (орграфу) M с количеством вершин более 3μ. Вершины подграфа H, взаимно однозначно соответствующие вершинам полного графа M, называются основными и составляют множество X. Остальные вершины графа T называются неосновными и составляют множество N. Наличие такого подграфа H является первой частью (Ч1) достаточных условий достижения взаимного информационного согласования (ВИС) в графе T. Второй

составной частью достаточных условий достижения ВИС в комплексе согласования является часть Ч2: для каждой его неосновной вершины существуют исходящие из этой вершины и далее непересекающиеся пути не менее чем к $2\mu+1$ конечным основным вершинам. Последней составной частью достаточных условий достижения ВИС в комплексе согласования является часть Ч3: для каждой его неосновной вершины существуют входящие и ранее не пересекающиеся пути не менее чем от $2\mu+1$ начальных основных вершин [1, 2]. Пример орграфовой модели комплекса для $\mu=1$ с выполняющимися условиями Ч1, Ч2, Ч3 показан на рис. 2.

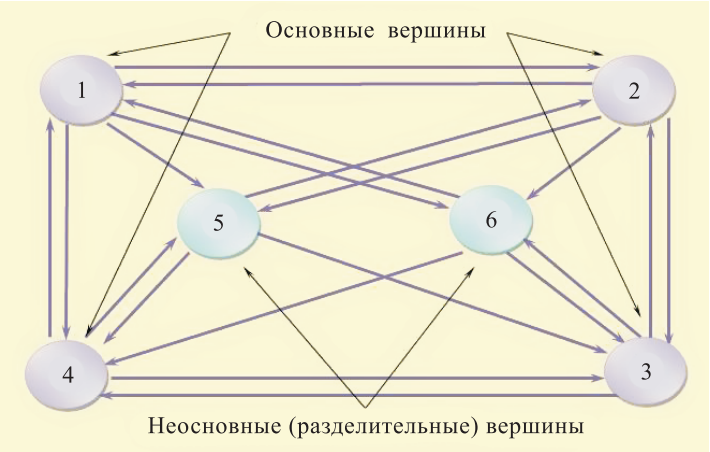


Рис. 2. Пример орграфовой модели комплекса для $\mu=1$

Для системы комплексов, взаимодействующих по индивидуальным средам межкомплексного обмена, должны выполняться достаточные структурные условия осуществления системного ВИС [1, 2].

Для необслуживаемых сбое- и отказоустойчивых РМВС, в которых обнаружение и идентификация проявлений неисправности некоторой неизбыточной ЦВМ осуществляются автоматически исправными ЦВМ этой системы, была введена ***градация проявлений неисправности по типу***, учитывающая необходимость и сложность их обработки в процессе целевой работы РМВС и определяющая ее последующие действия:

1) сбой ЦВМ — самоустраняющееся нарушение нормального функционирования аппаратуры вследствие кратковременных воздействий внешних и внутренних факторов на некоторый элемент (или совокупность элементов) [5];

2) программный сбой ЦВМ, внешним признаком которого считается проявление заранее оговоренной совокупности сбоев этой ЦВМ, приводящей к сбою в программном обеспечении (критерий программ-

ного сбоя); в случае программного сбоя необходимо проведение специальных действий по восстановлению вычислительного процесса в сбившейся ЦВМ;

3) отказ ЦВМ, объявляемый при проявлении заранее оговоренной совокупности ее программных сбоев (критерий отказа ЦВМ) либо обнаруживаемый при ее тестовом или системном диагностировании. При отказе необходима изоляция неисправной ЦВМ и либо включение вместо нее запасной ЦВМ, если она имеется, а также информационное восстановление этой включенной запасной ЦВМ и втягивание ее в необходимую целевую работу системы, либо выполнение самоуправляемой деградации системы.

Выделение структуры РМВС. Практическое решение сложной проблемы обеспечения сбое- и отказоустойчивости многозапросных РМВС состоит в организации параллельного выполнения поступивших запросов, для каждого из которых создается многокомплексная (многозадачная) сбое- и отказоустойчивая прикладная система, параллельно выполняющая множество $Z = \{Z_1, Z_2, \ldots, Z_t\}$ взаимодействующих целевых задач, для каждой Z_i сформирован *комплекс* K_i *этой задачи*, а также сбое- и отказоустойчивые *среды межкомплексного взаимодействия* $W_{i \to j}$, обеспечивающие достижение системного ВИС (рис. 3).

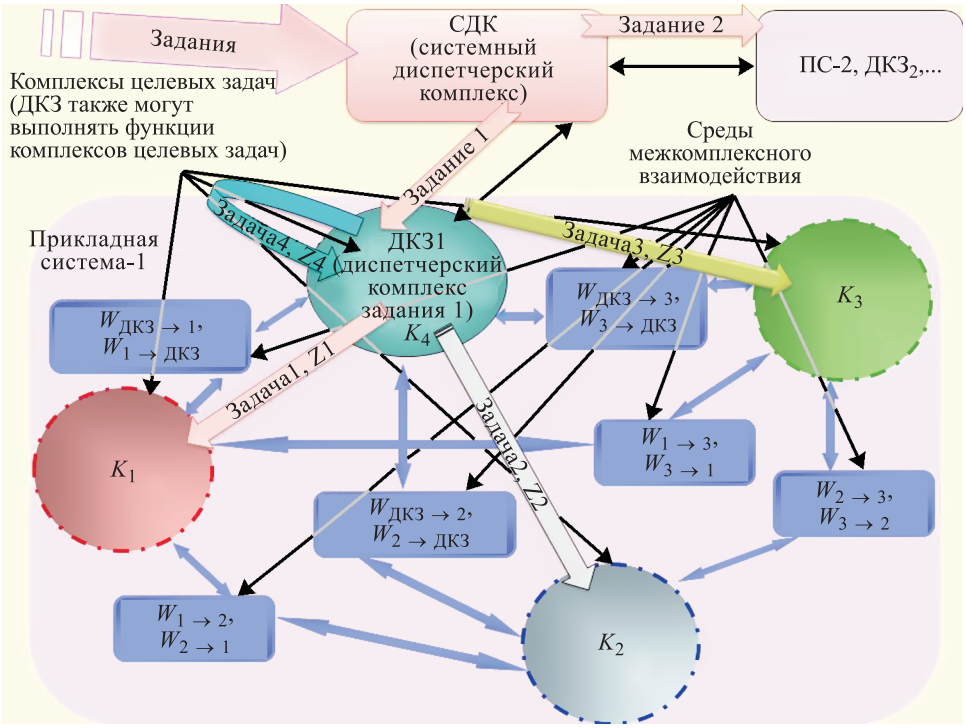


Рис. 3. Пример схемы многокомплексной распределенной многомашинной вычислительной системы

Организация формирования РМВС происходит следующим образом. На основе сети произвольной, но известной структуры необходимо выделить РМВС. На первом этапе выплняется начальная проверка, по итогам которой происходит формирование таблицы технического состояния (ТТС) для построения РМВС и затем выделение в сети сбое- и отказоустойчивого системного диспетчерского комплекса (СДК), являющегося управляющим органом РМВС. В роли СДК может выступать отдельный комплекс, имеющий достаточную степень сбое- и отказоустойчивости, или подсистема РМВС либо вся РМВС в целом, которая в определенные временные промежутки способна объединяться в специальный комплекс, выполняющий функции СДК.

Системному диспетчерскому комплексу известны структура РМВС, маршруты, временные кванты передачи и форматы получаемых и передаваемых сообщений. СДК строит индивидуальный алгоритм каждой ЦВМ РМВС и размещает его в памяти соответствующей ЦВМ в виде скомпилированной резидентной программы, а также обеспечивает синхронный запуск всех индивидуальных алгоритмов в определенный момент времени работы РМВС. СДК контролирует работу всех комплексов РМВС по их отчетам, управляет процессами реконфигурации и восстановления допустимой целевой работы РМВС при программных сбоях и отказах ЦВМ, самоуправляемой структурной и функциональной деградации РМВС, перевода части РМВС или РМВС в целом в состояние безопасного останова и последующего вывода РМВС из этого состояния.

Далее осуществляется выделение прикладной системы. В общем случае СДК получает задание, состоящее из нескольких задач, и в соответствии с поступившим заданием строит необходимое количество комплексов. Один из комплексов в случае необходимости может выполнять функции диспетчерского комплекса задания (ДКЗ). При этом допускается наличие неисправностей враждебного типа, в том числе и вызванных внешними воздействиями.

Затем выполняются синхронизация ЦВМ (с точностью до неделимого далее временного отрезка — ***кванта***, в течение которого происходит обмен сообщениями между соседними ЦВМ) и запуск работы прикладной системы на выполнение целевого задания.

В процессе функционирования вычислители всех КА выполняют тестовое и функциональное диагностирование с целью обнаружения возникших неисправностей, а также взаимное информационное согласование полученных результатов диагностирования.

Изначально задача была поставлена следующим образом. В сети ЦВМ известной структуры необходимо выделить определенное количество пронумерованных непересекающихся комплексов. Для каждого i-го комплекса задан диапазон допустимого количества

неисправных ЦВМ, которое задано также и для каждой среды межкомплексного взаимодействия. Необходимо в предложенной сети выделить (если это возможно) такие указанные непересекающиеся комплексы и среды межкомплексного взаимодействия, что в них при наличии допустимого количества неисправных ЦВМ обеспечивается возможность достижения системного ВИС [1, 2].

Динамическая избыточность позволяет системе самостоятельно, без участия обслуживающего персонала:

а) обнаруживать и идентифицировать возникающие допустимые неисправности по месту возникновения и по типу;

б) восстанавливать вычислительный процесс при сбоях и программных сбоях;

в) реконфигурировать систему при отказах с включением в рабочую конфигурацию запасных элементов;

г) осуществлять управляемую деградацию системы с сохранением и допустимым снижением заданных характеристик производительности, пропускной способности и сбое- и отказоустойчивости;

д) переводить систему в состояние безопасного останова при исчерпании доступных системных ресурсов или при возникновении недопустимых неисправностей.

Особенности построения РМВС на основе группировки КА ДЗЗ. В отличие от исходной задачи, решенной в [1, 2], для группировок КА ДЗЗ выделение комплексов и сред межкомплексного взаимодействия имеет следующие особенности. В случае появления каждого нового целевого события формируется соответствующий комплекс мониторинга этого целевого события с учетом вычисленных зон обслуживания и трассы полета КА [6], т. е. выделение комплекса происходит в динамическом режиме. Если целевые события появляются в большом количестве, то через некоторое время может наступить момент исчерпания ресурсов РМВС, когда не удается выделить отдельный комплекс для мониторинга возникшего целевого события. Возможно несколько подходов к решению возникшей проблемы. Остановимся на одном из них, заключающемся в попытке выделения пересекающихся комплексов, основанной на следующих положениях.

Поведенческая модель группировки такова. Все КА группировки под управлением СДК ведут наблюдение за предписанной областью поверхности Земли, периодически обмениваясь сообщениями, которые могут носить как целевой, так и диагностический характер. В случае обнаружения первого целевого события все КА группировки обмениваются сообщениями о его возникновении. Из числа тех КА, которые «видят» первое целевое событие, выделяется первый комплекс с числом КА $n_1 \geq 3\mu_1 + 1$ (μ_1 — отказоустойчивость первого

комплекса), целью которого является подробное наблюдение за развитием первого целевого события. Остальные КА группировки продолжают наблюдение за предписанной областью поверхности Земли.

В случае возникновения последующих целевых событий аналогичным образом из оставшихся КА выделяются следующие комплексы, между которыми выделяются среды межкомплексного взаимодействия, необходимые для согласования данных между комплексами. Согласованная информация передается заинтересованным службам. Таким образом, РМВС является многозадачной и, следовательно, многокомплексной.

Особенности построения РМВС для данной целевой задачи делают процесс формирования РМВС еще более сложным и многокритериальным:

- выделение комплексов происходит в момент обнаружения целевого события;
- в формировании комплекса принимают участие не все КА группировки, а лишь те, которые «видят» целевое событие, т. е. с учетом вычисленных зон обслуживания КА (среда межкомплексного взаимодействия формируется из любых свободных КА полностью в соответствии с [1, 2]);
- при формировании комплекса необходимо учитывать «степень приближенности» элементов группировки КА к месту нахождения целевого события, т. е. необходимо учитывать данные, содержащиеся в таблицах высоты, трассы полета КА и другие характеристики.

Назовем комплекс, который выделен для наблюдения за состоянием и поведением (для мониторинга) i-го целевого события, ***комплексом мониторинга*** $ЦС_i$. Комплекс мониторинга $ЦС_i$ выделяется в РМВС с учетом построенных таблиц высоты, трассы, областей покрытия, высоты Солнца и, если необходимо, яркости целевого события.

В данной работе используется следующее определение сбое- и отказоустойчивости РМВС: «…под ***отказоустойчивостью*** РМВС понимается ее способность правильно выполнять предусмотренные целевые задачи в условиях возникновения допустимых совокупностей одновременных неисправностей (сбоев и отказов) допустимых моделей и допустимых последовательностей таких совокупностей» [3]. При этом РМВС представляется в виде совокупности взаимосвязанных, далее неделимых элементов [3], и любая неисправность или их любое одновременное сочетание внутри такого отдельного элемента считается отдельной одиночной неисправностью РМВС, а количество одновременно неисправных элементов в РМВС — кратностью существующих неисправностей, которая задает подход в их разработке, основанный на предварительном построении требуемых траекторий управляемой реконфигурации и деградации такой системы и последующем ее проектировании

в соответствии с этими траекториями. В начале этих траекторий осуществляется замена отказавших элементов на запасные с последующим восстановлением в них необходимой целевой работы. При отсутствии запаса выполняется переход к целевой работе со сниженными уровнями сбое- и отказоустойчивости или осуществляется предусмотренная функциональная деградация системы посредством исключения из исполняющихся целевых задач наименее приоритетных, с расформированием их комплексов и переводом составляющих их ЦВМ в запас. При достижении критического уровня сбое- и отказоустойчивости и возникновении следующей неисправности, а также при возникновении недопустимых неисправностей система должна переходить в режим безопасного останова и ожидания указаний из внешней среды, предусмотренных при проектировании РМВС, с последующим выполнением этих указаний.

Решение задачи мониторинга целевых событий при ДЗЗ сопровождается ***сложностями на этапе реконфигурации РМВС*** при обнаружении неисправных КА, т. е. уже в начале траектории самоуправляемой деградации. В случае идентификации неисправности в комплексе мониторинга $ЦС_i$ резервные КА выбираются из тех, что «видят» $ЦС_i$ и не принадлежат комплексу мониторинга $ЦС_j$ ($i \neq j$), т. е. даже при наличии резерва им не всегда можно воспользоваться.

При решении поставленной целевой задачи возможно появление одной из двух проблем, подлежащих решению: а) целевые события возникают в таком количестве, что для наблюдения за каждым из них невозможно сформировать комплекс с заданной степенью отказоустойчивости вследствие недостаточной мощности группировки (рис. 4), что может сказаться на возможности обеспечения достоверности передаваемых данных; б) возникает более одного целевого события на небольшой площади, которые «видит» лишь ограниченное число КА группировки, что создает проблемы с обеспечением ее гарантоспособности [7].

К разрешению проблемы можно подойти следующим способом. Согласование информации в полносвязной системе (т. е. такой, моделью которой является полный граф (орграф)) может быть двух типов:

1) все согласуемые значения исправных ЦВМ должны быть одинаковыми, и тогда аппаратурная избыточность по количеству ЦВМ для вычисления согласованного значения должна быть не менее $2\mu + 1$, временная избыточность — один раунд взаимообменов согласуемыми значениями между всеми ЦВМ;

2) согласуемые значения исправных ЦВМ могут быть разными — в этом случае аппаратурная избыточность для вычисления согласованного значения составляет не менее $3\mu + 1$, временная избыточность — не менее $\mu + 1$ раундов взаимообменов (при допущении возможности возникновения неисправностей враждебного типа) [3, 8, 9].

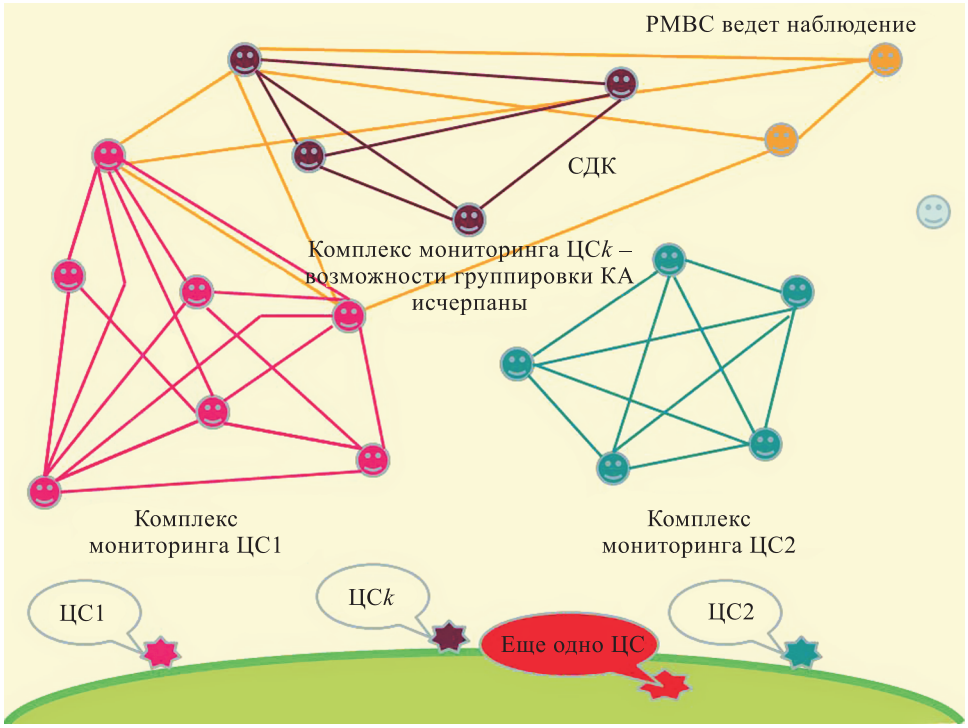


Рис. 4. Схема массового возникновения целевых событий $ЦС_1$, $ЦС_2$, …, $ЦС_k$

Считаем, что данные, получаемые при мониторинге одного целевого события разными КА и, соответственно, обрабатываемые вычислителями этих КА, одинаковые (в пределах погрешности), а диагностическая информация, получаемая в результате выполнения функционального и тестового диагностирования, — разная. Допустимая погрешность, определяемая целевой задачей, составляет по радиометрическому разрешению приборами видимого и ближнего инфракрасного излучения 0,1…0,5 %, для задач, решаемых инфракрасными радиометрами, — 0,1…0,2 К, для задач, решаемых радиолокаторами с синтезированной апертурой, — 0,1…1,0 дБ. По разрешению на местности для разных классов ДЗЗ необходимо обеспечивать от полуметра до десятков километров, следовательно, погрешность определяется уровнем разрешения [10].

В соответствии с видами согласования в комплексе мониторинга $ЦС_i$ можно выделить комплексы двух типов: комплексы задач ($КЗ_{i\_i}$, $КЗ_{i\_j}$, …) первого типа, каждый из которых выполняет мониторинг одного целевого события, и комплекс согласования ($КС_i$) второго типа — комплекс, которым, собственно, и является комплекс мониторинга $ЦС_i$, обладающий необходимой структурой для выполнения процесса ВИС.

Комплекс $КЗ_{i\_j}$ осуществляет репликацию *j*-й целевой задачи (мониторинг *j*-го целевого события) с взаимообменом копиями результатов и вычислением «правильного» значения путем усреднения результатов, не выходящих за рамки погрешности. Значения, отличающиеся более чем на значение допустимой погрешности, игнорируются. Подграф системы, порожденный вершинами из $КЗ_{i\_j}$, является полным.

После завершения решения *j*-й целевой задачи все ЦВМ комплекса целевой задачи $КЗ_{i\_j}$, на которых она решалась, обмениваются полученными данными и сравнивают их.

Будем считать ***синдромом*** совокупность органически связанных между собой признаков, объединенных единым механизмом возникновения и развития. По результатам сравнений в каждой *t*-й ЦВМ из $КЗ_{i\_j}$ строится локальный синдром $ЛС^{t}_{i\_j}$ состояния комплекса задачи. При решении в *i*-м комплексе согласования $КС_i$ нескольких целевых задач строится совокупность их локальных синдромов $ЛС^{q}_{i\_i}$, $ЛС^{t}_{i\_j}$, ….

Построенные синдромы передаются в основные ЦВМ [1, 2] $КС_i$. В результате согласования в каждой исправной ЦВМ РМВС образуется полный набор синдромов всех ЦВМ РМВС, принимающих участие в решении целевых задач. При согласовании в $КС_i$ всех полученных локальных синдромов $ЛС_i$ получается согласованный синдром $СС_i$ *i*-го комплекса согласования. Процесс системного ВИС позволяет построить в каждой *t*-й исправной ЦВМ *i*-го комплекса согласования согласованный синдром РМВС $СС^{t}_{РМВС}$ с его последующей обработкой.

В соответствии с согласованным синдромом РМВС $СС^{t}_{РМВС}$ в каждой исправной ЦВМ РМВС формируется подозреваемая область неисправностей. Проявление неисправности ЦВМ *t* в ЦВМ *l* приводит к построению во всех исправных ЦВМ логического выражения подозреваемой области неисправностей. Конъюнкция этих выражений преобразуется к виду дизъюнкции конъюнкций; одинаково построенное выражение в каждой исправной ЦВМ определяет неисправность, т. е. гарантоспособность РМВС не нарушается.

Пример выполнения системного ВИС построенных синдромов в двухкомплексной РМВС. В качестве примера рассмотрим приведенную на рис. 5 двухкомплексную РМВС, состоящую из комплексов согласования $КС_1$ и $КС_2$ и сред межкомплексного взаимодействия $СВ_{1\to2}$ и $СВ_{2\to1}$. Для каждого комплекса и для каждой среды

межкомплексного взаимодействия задана своя степень отказоустойчивости, соответственно, μ_1, μ_2, $\mu_{1\to2}$, $\mu_{2\to1}$. В каждом комплексе согласования выделены комплексы задач.

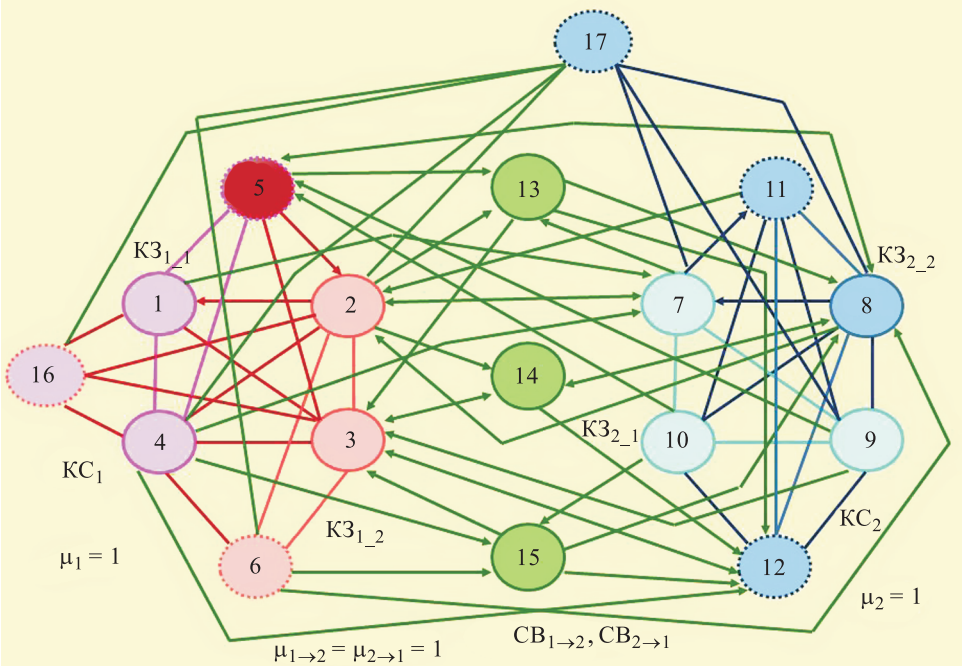


Рис. 5. Пример двухкомплексной РМВС с выделенными комплексами задач

Пусть в комплексе $КС_1$ имеется неисправность вычислителя. РМВС должна принять согласованное решение о наличии и месте неисправности и о возможности реконфигурации РМВС путем замены неисправной ЦВМ комплекса $КС_1$ на другую ЦВМ $КС_1$. В комплексе согласования $КС_1$, основными ЦВМ которого являются ЦВМ 1, 2, 3, 4, выделены два комплекса задачи $КЗ_{1\_1}$ (ЦВМ 1, 4, 5) и $КЗ_{1\_2}$ (ЦВМ 2, 3, 6), а в комплексе согласования $КС_2$ с основными ЦВМ 7, 8, 9, 10 — два комплекса задачи $КЗ_{2\_1}$ (ЦВМ 7, 9, 10) и $КЗ_{2\_2}$ (ЦВМ 8, 11, 12) для решения целевых задач.

В $КЗ_{1\_1}$ ЦВМ 5 передает в ЦВМ своего комплекса задачи неправильные результаты, поэтому ЦВМ 1 и 4 строят синдромы $ЛС^1_{1\_1} = (0_1, 0_4, 1_5)$ и $ЛС^4_{1\_1} = (0_1, 0_4, 1_5)$, где 0_i — признак отсутствия проявления неисправности, 1_i — признак проявления неисправности i-й ЦВМ. ЦВМ 5 строит синдром $ЛС^5_{1\_1} = (0_1, 0_4, 0_5)$. Считаем, что неисправность ЦВМ 5 проявляется только в виде неправильного решения

целевой задачи. Остальные ЦВМ комплекса согласования $КС_1$ строят локальные синдромы $ЛС^2_{1\_2} = (0_2, 0_3, 0_6)$, $ЛС^3_{1\_2} = (0_2, 0_3, 0_6)$, $ЛС^6_{1\_2} = (0_2, 0_3, 0_6)$ соответственно. В комплексе согласования $КС_2$ проявлений неисправностей нет, поэтому все ЦВМ комплекса $КС_2$ строят синдромы $ЛС^7_{2\_1} = (0_7, 0_9, 0_{10})$, $ЛС^9_{2\_1} = (0_7, 0_9, 0_{10})$, $ЛС^{10}_{2\_1} = (0_7, 0_9, 0_{10})$, $ЛС^8_{2\_2} = (0_8, 0_{11}, 0_{12})$, $ЛС^{11}_{2\_2} = (0_8, 0_{11}, 0_{12})$, $ЛС^{12}_{2\_2} = (0_8, 0_{11}, 0_{12})$. Построенные синдромы передаются в основные ЦВМ соответствующих комплексов согласования (1, 2, 3, 4 — для комплекса $КС_1$; 7, 8, 9, 10 — для комплекса $КС_2$). В результате стандартного процесса ВИС [1, 2] в каждой основной исправной ЦВМ комплекса согласования $КС_1$ будут построены согласованные значения синдромов $СС_1 = \{(0_1, 0_4, 1_5)^1, (0_1, 0_4, 1_5)^4, (0_1, 0_4, 0_5)^5, (0_2, 0_3, 0_6)^2, (0_2, 0_3, 0_6)^3, (0_2, 0_3, 0_6)^6\}$, и в каждой основной исправной ЦВМ комплекса согласования $КС_2$ будут построены согласованные значения синдромов $СС_2 = \{(0_7, 0_9, 0_{10})^7, (0_7, 0_9, 0_{10})^9, (0_7, 0_9, 0_{10})^{10}, (0_8, 0_{11}, 0_{12})^8, (0_8, 0_{11}, 0_{12})^{11}, (0_8, 0_{11}, 0_{12})^{12}\}$, где $(0|1_p, 0|1_q, 0|1_s)^l$ — значение $ЛС^l$, построенного для ЦВМ p, q, s.

Для ЦВМ 16 и 17, не участвующих в решении целевых задач, согласуются некоторые заранее известные значения, например значения их порядковых номеров.

В соответствии с построенными синдромами в каждой исправной ЦВМ комплекса согласования $КС_1$ формируется область подозреваемых значений: в ЦВМ 1 такой областью будет (1V5), в ЦВМ 4 — (4V5). Затем в каждой исправной ЦВМ строится конъюнкция дизъюнкций (1V5)(4V5), которая преобразуется к виду 1·4V1·5V1·4V5·4V5·5 = 5, т. е. ЦВМ 5 идентифицируется как неисправная.

Если предположить, что неисправность ЦВМ 5 имеет «враждебный» характер неисправности и ведет себя «злонамеренно», то она может, например, построить локальный синдром вида $ЛС^5_{1\_1} = (1_1, 1_4, 0_5)$. Тогда каждая исправная ЦВМ сформирует область подозреваемых значений (1V5)(4V5)(1V4V5), что при преобразовании также позволит идентифицировать ЦВМ 5 как неисправную.

По результатам всех перечисленных действий строится вектор согласованных значений состояния каждой ЦВМ, где Θ_i — согласо-

ванное значение состояния каждой ЦВМ $КС_1$ [11] (рис. 6, *а*). Аналогичные действия, выполняемые комплексом согласования $КС_2$, в котором не было проявлений неисправностей ни у одной из ЦВМ, участвующих в решении целевых задач, приводят к построению вектора согласованных значений состояния каждой ЦВМ этого комплекса согласования (рис. 6, *б*).

Θ_1	Θ_2	Θ_3	Θ_4	Θ_5	Θ_6	Θ_{16}
0	0	0	0	1	0	*N*16

а

Θ_7	Θ_8	Θ_9	Θ_{10}	Θ_{11}	Θ_{12}	Θ_{17}
0	0	0	0	0	0	*N*17

б

Рис. 6. Вектор согласованных значений $КС_1(а)$ и $КС_2(б)$

Межкомплексное согласование [1, 2] дает возможность сформировать вектор согласованных значений РМВС. Анализ структуры РМВС позволяет сделать вывод о возможности замены ЦВМ 5 на ЦВМ 16, которая не участвует в решении целевых задач комплекса согласования $КС_1$.

Для реконфигурации РМВС необходимо выполнить целый комплекс технических мероприятий, которые выходят за рамки данной работы.

При идентификации программного сбоя ЦВМ в некотором задачном комплексе (далее — восстанавливаемый, подлежащий самовосстановлению задачный комплекс) информацию об этом событии данный задачный комплекс передает в СДК, который анализирует все выполняемые в задачных комплексах целевые процессы и взаимодействия между ними, определяет период времени восстановления, на который восстанавливаемый задачный комплекс может быть выведен из процесса решения предписанной ему целевой задачи, и сообщает об этом данному комплексу, а также всем другим комплексам, взаимодействующим с ним. Кроме того, СДК сообщает всем этим взаимодействующим между собой комплексам алгоритмы их работы, во-первых, во время этого периода и, во-вторых, после его завершения в случае как успешного, так и неуспешного восстановле-

ния. При наступлении периода восстановления все взаимодействующие между собой задачные комплексы выполняют предписанные им из СДК целевые и восстанавливающие действия и по окончании периода восстановления сообщают в СДК об успешных или неуспешных его результатах. В свою очередь, СДК, получив эти сообщения, принимает решения по дальнейшей организации целевого вычислительного процесса.

Все описанные действия по восстановлению в РМВС целевой работы в случаях идентификации допустимых совокупностей неисправностей должны быть в достаточной степени синхронизированными и согласованными для всех исправных ЦВМ из РМВС. Синхронность обеспечивается путем организации в РМВС непрерывной работы подсистемы единого системного времени, включающей средства как начальной, так и промежуточной синхронизации автономных часов в отдельных элементах системы.

Согласованность действий и принимаемых решений в различных ЦВМ и подсистемах РМВС гарантируется применением алгоритмов ВИС. Достижимость ВИС составляет концептуальную основу создания отказоустойчивых алгоритмов для решения основных задач организации распределенных вычислений.

Заключение. Вопросы оптимизации характеристик РМВС (временных, аппаратурных, информационных) имеют большую практическую значимость, поскольку связаны с такими важнейшими свойствами РМВС, как производительность и живучесть [13]. А в области группировки КА ДЗЗ это не только весь спектр вопросов, связанных с безопасностью, экологией и возможными экономическими потерями, но еще и вопросы финансирования запуска КА.

Предложенный метод позволяет решить проблему минимизации мощности группировка КА ДЗЗ без потери гарантоспособности решаемых целевых задач определенного класса.

Перспективные способы решения проблемы недостаточной мощности группировки КА заключаются в следующем:

1) не снижая степени отказоустойчивости каждого комплекса обеспечить его наблюдение за бóльшим числом ЦС (т. е. применить переход к многозадачному режиму вычислителей, находящихся на КА). Такой подход приведет к существенному усложнению программного обеспечения каждого КА. Однако он гарантирует достоверность передаваемой информации, реализация его программно и технически вполне возможна, хотя и с соблюдением ряда ограничений;

2) строить комплексы пересекающимися, т. е. такими, где один КА может принадлежать разным комплексам. Это наиболее трудоемкий и наукоемкий способ, для которого потребуется разработка новых моделей при построении РМИУС, однако он и более перспективный, позволяющий максимально использовать вычислительные возможности каждого КА.

ЛИТЕРАТУРА

[1] Ашарина И.В., Лобанов А.В. Выделение комплексов, обеспечивающих достаточные структурные условия системного взаимного информационного согласования в многокомплексных системах. *Автоматика и телемеханика*, 2014, № 6, с. 115–131.

[2] Ашарина И.В., Лобанов А.В. Выделение структурной среды системного взаимного информационного согласования в многокомплексных системах. *Автоматика и телемеханика*, 2014, № 8, с. 146–156.

[3] Лобанов А.В. Модели замкнутых многомашинных вычислительных систем со сбое- и отказоустойчивостью на основе репликации задач в условиях возникновения враждебных неисправностей. *Автоматика и телемеханика*, 2009, № 2, с. 171–189.

[4] Нефедов В.Н., Осипова В.А. *Курс дискретной математики*. Москва, Издательство МАИ, 1992, 263 с.

[5] Дианов В.Н. Диагностика сбоев в электронной аппаратуре. *Вестник МГТУ им. Н.Э. Баумана*. *Сер. Приборостроение*, 2007, № 2, с. 16–47.

[6] Микрин Е.А., Михайлов М.В. *Навигация космических аппаратов по измерениям от глобальных спутниковых навигационных систем.* 2-е изд. Москва, Издательство МГТУ им. Н.Э. Баумана, 2018, 345 с.

[7] Лобанов А.В. Организация сбое- и отказоустойчивых вычислений в полносвязных многомашинных вычислительных системах. *Автоматика и телемеханика*, 2000, вып. 12, с. 138–146.

[8] Авиженис А. Отказоустойчивость — свойство, обеспечивающее постоянную работоспособность цифровых систем. *ТИИЭР*, 1978, т. 66, № 10, с. 5–25.

[9] Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. *J. ACM.*, 1980, vol. 27, no. 2, pp. 228–234.

[10] Lamport L., Shostak R., Pease M. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems,* 1982, vol. 4, no. 3, pp. 382–401.

[11] Владимиров В.М., Дмитриев Д.Д., Дубровская О.А. и др., *Дистанционное зондирование Земли.* В.М. Владимиров, ред. Москва, ИНФРА-М; Красноярск, Сиб. федер. ун-т, 2021, 196 с.

[12] Ашарина И.В. Метод построения отказоустойчивого распределенного алгоритма системного взаимного информационного согласования в сетецентрических информационно-управляющих системах. В сб.: *Материалы X Всероссийской научно-технической конференции «Научные чтения по авиации, посвященные памяти Н.Е. Жуковского», Москва, 17–18 апреля 2014 г.* Москва, 2014, с. 135–138.

Статья поступила в редакцию 09.03.2022

Ссылку на эту статью просим оформлять следующим образом:

Ашарина И.В., Гришин В.Ю., Сиренко В.Г. Обеспечение отказоустойчивости в многомашинных вычислительных системах дистанционного зондирования Земли при ограниченных аппаратурных ресурсах. *Инженерный журнал: наука и инновации*, 2022, вып. 5. http://dx.doi.org/10.18698/2308-6033-2022-5-2180

Ашарина Ирина Владимировна — канд. техн. наук, старший научный сотрудник АО «НИИ «Субмикрон»; доцент НИУ МИЭТ. e-mail: asharinairina@mail.ru

Гришин Вячеслав Юрьевич — канд. техн. наук, 1-й заместитель генерального директора, Гл. конструктор. e-mail: grishin@se.zgrad.ru

Сиренко Владимир Григорьевич — д-р техн. наук, профессор, заместитель генерального директора по перспективным проектам. e-mail: vgsirenko@mail.ru

Ensuring fault tolerance in multicomputer systems for Earth remote sensing with limited hardware resources

© I.V. Asharina[1,2], V.Yu. Grishin[1], V.G. Sirenko[1]

[1]JSC Scientific Research Institute Submicron, Moscow, Zelenograd, 124460, Russia
[2]National Research University of Electronic Technology MIET,
Moscow, Zelenograd, 124498, Russia

The paper centers on the problems of developing failure- and fault-tolerant systems for Earth remote sensing satellite constellation control. The study defines the concept of a complex that fail-safely performs a target task, in this case, the task of detecting a target event and monitoring its behavior and development, i. e. monitoring the target event, and gives a hierarchical satellite constellation structure. Findings of the research show that it is necessary to use dynamic redundancy, which can significantly increase the trajectory of self-controlled degradation and, accordingly, the satellite constellation active life. The complexity of the problem lies in ensuring the reliability of the results obtained when a large number of target events, both natural and man-caused, occur. The study introduces an approach to reduce hardware redundancy, i.e. monitor a larger number of events using a lower power satellite constellation, and proves that is possible to use the approach without losing the system reliability.

Keywords: *distributed multicomputer system, failure- and fault-tolerance, dynamic redundancy, hostile malfunction, Earth remote sensing, satellite constellations*

REFERENCES

[1] Asharina I.V., Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2014, no. 6, pp. 115–131.
[2] Asharina I.V., Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control*, 2014, no. 8, pp. 146–156.
[3] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control,* 2009, no. 2, pp. 171–189.
[4] Nefedov V.N., Osipova V.A. *Kurs diskretnoy matematiki* [Discrete Mathematics Course]. Moscow, MAI Publ., 1992, 263 p.
[5] Dianov V.N. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie — Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, 2007, no. 2, pp. 16–47.
[6] Mikrin E.A., Mikhaylov M.V. *Navigatsiна kosmicheskikh apparatov po izmereniyam ot globalnykh sputnikovykh navigatsionnykh system* [Spacecraft navigation by measurements from global satellite navigation systems]. 2nd ed., Moscow, BMSTU Publ., 2018, 345 p.
[7] Lobanov A.V. *Avtomatika i telemekhanika — Automation and Remote Control,* 2000, no. 12, pp. 138–146.
[8] Avizhenis A. *Proceeding of the IEEE,* translated into Russ., 1978, vol. 66, no. 10, pp. 5–25.
[9] Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. *J. ACM.*, 1980, vol. 27, no. 2, pp. 228–234.
[10] Lamport L., Shostak R., Pease M. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 1982, vol. 4, no. 3, pp. 382–401.

[11] Vladimirov V.M., Dmitriev D.D., Dubrovskaya O.A., et al. *Distantsionnoe zondirovanie Zemli* [Remote sensing of the Earth]. Moscow, INFRA-M Publ.; Krasnoyarsk, SibFU Publ., 2021, 196 p.

[12] Asharina I.V. Metod postroeniya otkazoustoychivogo raspredelennogo algoritma sistemnogo vzaimnogo informatsionnogo soglasovaniya v setetsentricheskikh informatsionno-upravlyayuschikh sistemakh [A method for developing a fault-tolerant distributed algorithm for systemic mutual information coordination in network-centric information and control systems]. In: *Materialy X Vserossiyskoy nauchno-tekhnicheskoiy konferentsii «Nauchnye chteniya po aviatsii, posvyashchennye pamyati N.E. Zhukovskogo», Moskva, 17–18 aprelya 2014 g.* [Proceedings of the X All-Russian Scientific and Technical Conference "Scientific readings on aviation dedicated to the memory of N.E. Zhukovsky", Moscow, April 17–18, 2014]. Moscow, 2014, pp. 135–138.

Asharina I.V., Cand. Sc. (Eng.), Senior Research Fellow, JSC Scientific Research Institute Submicron; Assoc. Professor, National Research University of Electronic Technology MIET. e-mail: asharinairina@mail.ru

Grishin V.Yu., Cand. Sc. (Eng.), First Deputy General Director, JSC Scientific Research Institute Submicron, Chief Designer. e-mail: grishin@se.zgrad.ru

Sirenko V.G., Dr. Sc. (Eng.), Professor, Deputy General Director for Advanced Projects, JSC Scientific Research Institute Submicron. e-mail: vgsirenko@mail.ru