Уманский А.Б., Яцук Г.Е., Ананьин А.С.
АО «НПО автоматики им. академика Н.А. Семихатова», Екатеринбург, Россия

ОСОБЕННОСТИ ПРОГРАММНО-АППАРАТНОЙ РЕАЛИЗАЦИИ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ МАЛОГАБАРИТНЫМ АВТОНОМНЫМ ПОДВОДНЫМ АППАРАТОМ

В работе рассматривается проблема реализации аппаратной и программной составляющих цифровой части системы управления (СУ) малогабаритного подводного аппарата с учетом требований надежности и сохранения работоспособности при одной возможной неисправности в условиях длительного автономного функционирования. Рассматривается подход по сокращению массогабаритных характеристик (ГМХ) многоканальной резервированной системы посредством реализации ее архитектуры на базе межканальных связей типа «точка-точка» с использованием принципа информационно-временного резервирования с голосованием по принципу «два из трех» на программном уровне. Разработана малогабаритная трехканальная управляющая вычислительная система (ВС). Каждый канал содержит в себе процессор, постоянное запоминающее устройство (ПЗУ), оперативное запоминающее устройство (ОЗУ), интерфейсную перепрограммируемую логическую интегральную схему (ПЛИС). Каналы связаны друг с другом последовательным интерфейсом, взаимодействие с периферийными устройствами реализуется по дублированным унифицированным интерфейсам, подключаемым непосредственно к процессору и ПЛИС. Программное обеспечение (ПО) реализовано с использованием компактной операционной системы реального времени. В каждом канале функционирует несколько потоков управления, в том числе и фоновый поток сканирования ПЗУ на наличие сбоев, с последующим восстановлением сбойных участков независимо от штатных алгоритмов. Реализация трехканальной архитектуры ВС с типами связей «точка – точка» между каналами и дублированными связями для взаимодействия с внешними системами обеспечивает выполнение предъявленных требований по надежности и живучести для длительного автономного функционирования. Заложенный комплекс программных средств контроля, парирования сбоев и восстановления обеспечивает работоспособность системы в условиях возникновения кратковременных разовых сбоев. Это позволяет управляющему вычислителю не только реализовать выполнение всей совокупности задач, решаемых подводным аппаратом в реальном масштабе времени, но и с большой долей вероятности обеспечить живучесть СУ в условиях воздействия внешних дестабилизирующих факторов.

Ключевые слова: вычислительная система, управление, надежность, программное обеспечение.

Авторы заявляют об отсутствии возможных конфликтов интересов.

Для цитирования: Уманский А.Б., Яцук Г.Е., Ананьин А.С. Особенности программно-аппаратной реализации вычислительной системы для управления малогабаритным автономным подводным аппаратом. Труды Крыловского государственного научного центра. 2018; специальный выпуск 1: 191–197.

УДК 629.57:681.3.06 DOI: 10.24937/2542-2324-2018-1-S-I-191-197

Umanskii A., Yatsuk G., Ananyin A.
Scientific and Production Association of Automatics named after academician N.A. Semikhatov, Yekaterinburg, Russia

SPECIFICS OF SOFTWARE/HARDWARE IMPLEMENTATION OF COMPUTER CONTROL SYSTEM FOR SMALL-SIZE AUTONOMOUS UNDERWATER VEHICLES

The paper deals with the issues related to software & hardware implementation of digital control system for a small-size underwater vehicle supporting reliable operation and sustained functional performance in case of a potential failure during long-term autonomous operation. A weight & size minimization approach is considered based on the point-to-point architecture using the two-out-of-three voting principle at software level. A miniature three-channel computer control system is developed. Each channel comprises a processor, ROM, RAM, and FPLD. The channels are linked by a serial interface. Interaction with periph-

erals is done via standard duplicate interfaces linked directly to the processor or FPLD. The software is implemented on a compact real-time operating system. Each channel has a number of control flows, including background ROM scanning to detect malfunctions and correct errors independently from standard algorithms. The three-channel architecture featuring point-to-point links between channels and duplicate interaction with external systems provides required level of reliability and survivability for long-term autonomous operation. The built-in system of program tools for control, correction of errors and restoration of functions supports reliable operation of the system even in case of short-term one-time errors. It enables the control computer not only to handle all multiple tasks of AUVs but also to ensure excellent level of the control system survivability under unfavourable external effects.

Key words: computer system, control, reliability, software.

Authors declare lack of the possible conflicts of interests.

For citations: Umanskii A., Yatsuk G., Ananyin A. Specifics of software/hardware implementation of computer control system for small-size autonomous underwater vehicles. Transactions of the Krylov State Research Centre. 2018; special issue 1: 191–197 (in Russian).

UDC 629.57:681.3.06 DOI: 10.24937/2542-2324-2018-1-S-I-191-197

Введение
Introduction

При проектировании СУ для подвижных объектов ответственного применения или с большим сроком активной эксплуатации необходимо учитывать вероятность выхода из строя какого-либо элемента СУ даже при ее хранении. Для парирования отказов аппаратуры применяются различные способы резервирования: структурное, временное, информационное, функциональное, программно-алгоритмическое, нагрузочное. Однако введение структурного резервирования увеличивает ГМХ, что не удовлетворяет требованиям, если объект управления имеет малые размеры. Введение других видов резервирования требует временных запасов для решения целевой задачи. Поэтому проектируемая ВС должна иметь в составе оптимальный набор резервируемых сущностей, достаточных для обеспечения требуемой надежности.

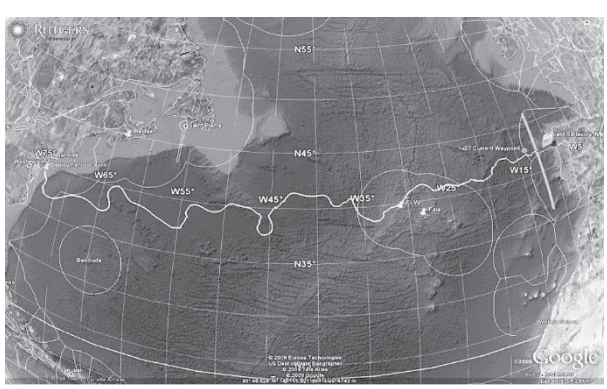

Рис. 1. Маршрут трансатлантического перехода Scarlet Knight

Fig. 1. Transatlantic route of Scarlet Knight

В качестве целевой платформы применения предлагаемой системы рассматриваются малые необитаемые аппараты со сроками автономного функционирования от нескольких месяцев до нескольких лет. К таким аппаратам, например, относятся подводные глайдеры. Как известно, область применения таких подводных аппаратов очень широка, начиная от мониторинга районов Мирового океана для научных работ и заканчивая использованием в военных целях. На рис. 1 представлен пример маршрута длиной 7500 км, пройденного глайдером Scarlet Knight за 8 месяцев.

Как отмечалось выше, при разработке подобных СУ одним из основных требований является обеспечение надежности, которое включает требования по сохранению работоспособности при возникновении одной возможной неисправности в процессе эксплуатации. Поэтому ключевой особенностью данной разработки является необходимость обеспечения длительной работоспособности цифровой части системы, которая должна быть реализована на отечественной элементной базе, в условиях возможных сбоев и отказов при жестких ограничениях на массу, габариты и энергопотребление, а также обеспечение самовосстановления после сбоев без вмешательства извне.

Выбор оптимальной архитектуры вычислительной системы

Choice of optimum architecture for computer system

Архитектура ВС выбиралась исходя из обозначенных выше требований по ограничениям на ГМХ (использование только отечественной элементной базы и длительный срок эксплуатации). Были рассмотрены различные варианты архитектур бортовых цифровых вычислительных систем (БЦВС), в том числе различные виды канального резервирования.

Одноканальная БЦВС не имеет структурного резерва. Любой возникший отказ на этапе хранения или на этапе эксплуатации приведет к отказу всей системы. Применение двухканальных БЦВС требует внесения в структуру дополнительных элементов контроля функционирования, вследствие чего увеличивается ГМХ. Также использование двухканальных СУ влечет за собой увеличение сложности, накладных расходов при выполнении и времени разработки ПО. При рассмотрении трехканальных СУ был сделан вывод о том, что наличие трех синхронно работающих каналов позволяет обнаружить канал с нарушенным функционированием посредством выдаваемой им информации в соседние каналы по принципу «два из трех». При этом усложнение ПО не столь значительно в сравнении с двухканальной БЦВС.

Традиционно в разработках БЦВС НПО автоматики (НПОА) используются троированные вычислительные структуры. При этом БЦВС организованы по магистрально-модульному принципу. Модули собираются в вычислительную систему посредством установки на общесистемной магистрали требуемого для данной СУ набора базовых модулей, взаимодействие между которыми осуществляется центральным резервированным вычислителем малой разрядности. Типовая резервированная структура БЦВС разработки НПОА представлена на рис. 2.

Как видно из рисунка, типовая структура содержит по меньшей мере пять узлов (три вычислителя, узел синхронизации и выборки решений, интерфейсные узлы), реализованных в виде отдельных модулей.

В целях сокращения ГМХ оптимальным решением является отказ от использования внутрисистемных магистралей и выделенных управляющих модулей с возложением системных и диспетчирующих функций на ПО БЦВС в трехканальном исполнении. Надежность обеспечивается реализацией принципа информационно-временного резервирования с голосованием по принципу «два из трех» на программном уровне. При этом взаимодействие с периферийными устройствами реализуется по унифицированным интерфейсам, подключаемым непосредственно к вычислительным каналам. Структурная схема устройства представлена на рис. 3, внешний вид – на рис. 4. Каждый канал имеет собственный процессор, оперативную память, постоянную память, интерфейсную ПЛИС. Каждый процессор связан с двумя другими по межканальному интерфейсу SpaceWire типа «точка – точка». Взаимодействие с периферийными устройствами реализовано на базе контроллеров интерфейса в составе процессоров и ПЛИС:

- дублированных кодовых линий связи (ЛС) типа RS-485, SPI; для обеспечения взаимодействия с устройствами даже в случае отказа одного из каналов, устройства подключатся дублированной ЛС минимум к двум каналам;
- троированных дискретных сигналов с портов ввода/вывода общего назначения процессора, использующихся для управления внешними устройствами, питанием процессоров (необходимо для перезапуска канала имеющего отрицательный результат контроля работоспособности).

Каждый канал ВС имеет:

- двухъядерный процессор 1892ВМ8Я производства ОАО НПЦ «Элвис»;
- сегнетоэлектрическое ЗУ 1666РЕ014 производства ОАО «Интеграл»;
- интерфейсные ПЛИС 5576ХС2Т производства КТЦ «Электроника».

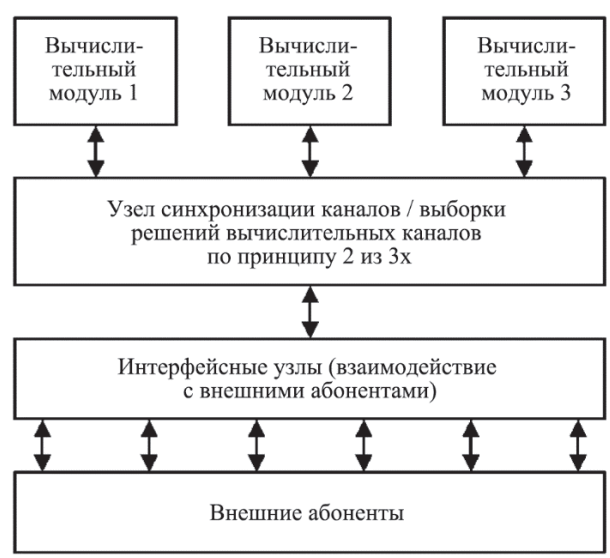

Рис. 2. Структура типовой трехканальной бортовой цифровой вычислительной системы НПО автоматики

Fig. 2. Structure of a standard on-board digital system (Scientific &Production Association of Automatics)

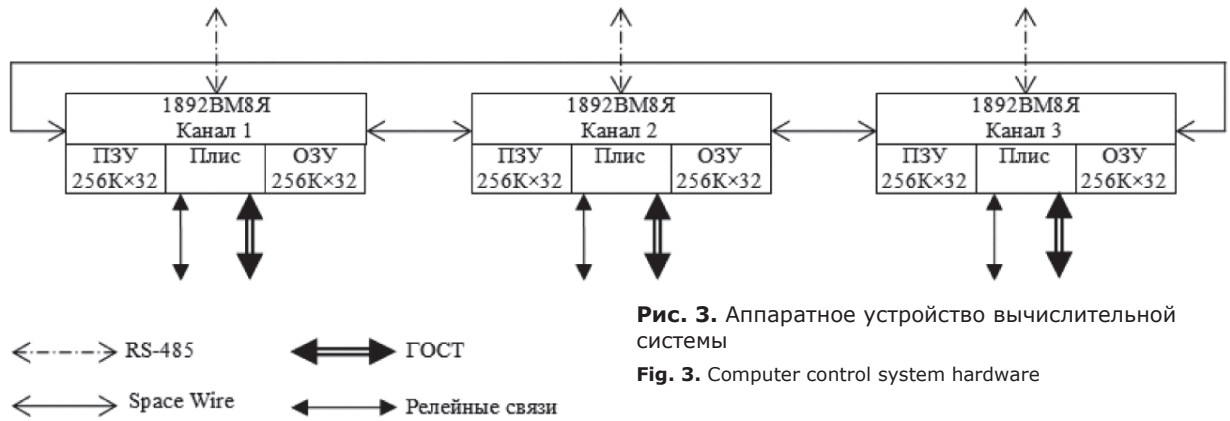

Рис. 3. Аппаратное устройство вычислительной системы

Fig. 3. Computer control system hardware

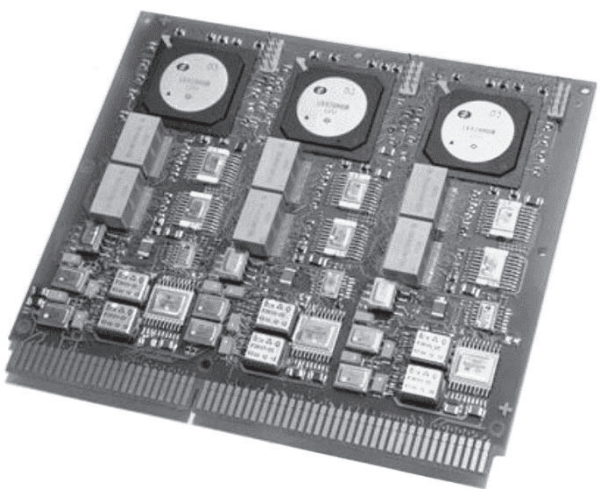

Рис. 4. Внешний вид малогабаритной трехканальной вычислительной системы

Fig. 4. External view of the miniature three-channel computer system

Программное обеспечение вычислительной системы

Software of computer system

ПО ВС разработано с учетом требований надежности, которые включают в себя предсказуемость работы в условиях жесткого реального времени с автоматическим парированием нештатных ситуаций в условиях автономного функционирования.

Исходный код ПО ВС написан на языке программирования Си. ПО подразделяется на программы для работы с аппаратурой – системное программное обеспечение (СПО), и программы для работы с объектом управления – функциональное программное обеспечение (ФПО). Практически весь состав СПО представляет собой операционную систему реального времени (ОСРВ), а ФПО является абстракцией верхнего уровня, использующей интерфейсы ОСРВ. Таким образом, СПО отвечает за обмен с внешними устройствами и исполнительными органами. ФПО отвечает за отработку логической части алгоритмов.

С учетом условий длительного функционирования была поставлена задача парирования периодических сбоев с последующим восстановлением вычислительного процесса (ВП).

Основой аппаратно-программной реализации парирования сбоев и восстановления является распределенный между тремя каналами программный модуль принятия решений об исправности каналов. Все три канала решают одну и ту же задачу, формируя в определенные моменты времени одну и ту же обменную информацию для внешних абонентов (ВА). Перед выдачей информации ВА каналы обмениваются между собой этой информацией по межканальному интерфейсу. Далее в каждом канале производится сравнение информации со всех трех каналов по принципу «два из трех». При успешном сравнении канал, физически подключенный к абоненту, осуществляет взаимодействие с ним. По факту успешного завершения обмена принятая информация транслируется в соседние каналы.

В случае сбоя при обмене парирование осуществляется повтором информации по основной и резервной ЛС. При устойчивом нарушении взаимодействия по обеим ЛС бракуется канал, подключенный к данной линии связи. Также при расхождении информации для выдачи ВА одного из каналов с данными двух других каналов проводится бракование канала,

ПЗУ1											
ПЗУ1.1						ПЗУ1.2					
0	1	…	125	126	CI1	0	1	…	125	126	CI2
ПЗУ2											
ПЗУ2.1						ПЗУ2.2					
127	128	…	252	253	CI3	127	128	…	252	253	CI4

Рис. 5. Структура постоянного запоминающего устройства

Fig. 5. ROM structure

выдавшего недостоверную информацию, и его восстановление путем полной перезагрузки этого канала и последующей передачей оперативной информации из соседнего канала по межканальному интерфейсу. При этом необходимым условием для перезагрузки канала является сигнал снятия питания, выставленный с обоих «соседних каналов». После снятия питания процессор проходит инициализацию, затем квитирует соседние процессоры об успешном запуске. При отсутствии квитанции в течение определенного времени соседний процессор меняет вектор сброса для восстанавливаемого процессора и заново перезапускает его.

Возможность смены вектора сброса в канале обеспечивается соответствующей структурой ПЗУ (рис. 5). ПЗУ вычислительного канала условно разделено на два банка с возможностью переключения используемого в данный момент банка соседим или собственным каналом вычислителя. Для противодействия повреждениям памяти в обоих банках ПЗУ хранятся одинаковые программы. Каждая копия программы разбита на блоки, которые снабжены контрольными суммами. В первых блоках ПЗУ хранится программный загрузчик, управление на который передается при подаче питания на процессорный канал. После запуска загрузчик проверяет свою целостность и отправляет квитанции в соседние каналы.

При успешном перезапуске восстанавливаемый канал должен получить из соседнего канала данные для восстановления работоспособности, включая рестартный массив, который содержит ключевые параметры для восстановления ВП. Для удобства восстановления оперативной информации после перезагрузки канала используется специальная зона ОЗУ, где хранятся все необходимые для восстановления ВП данные (признаки прохождения характерных участков программы, входные/выходные массивы данных, часть глобальных переменных). Поскольку все три канала функционируют по одинаковой временной диаграмме, запоминая при прохождении определенных участков необходимые признаки, то это позволяет любому каналу после перезагрузки вернуться в актуальное состояние. Одновременно с этим также восстанавливается счет времени.

Как отмечалось выше, ПО ВС реализовано с использованием компактной ОСРВ собственной разработки НПОА. При этом, в каждом канале функционирует системный поток, несколько функциональных потоков и фоновый поток самотестирования вычислителей, содержащий в том числе и тесты ПЗУ на наличие искажений с последующим восстановлением сбойных участков независимо от штатных алгоритмов. Приоритеты потоков расставлены так, чтобы и сигналы управления выдавались вовремя, и была возможность самодиагностики внутри ВС для поддержания функционирования в автономном режиме (рис. 6).

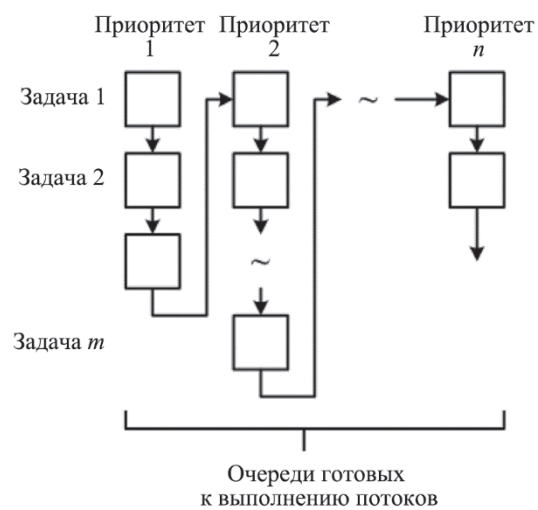

Рис. 6. Порядок подключения потоков операционной системы реального времени

Fig. 6. Flow-chart of real-time operating system flow

В случае подтверждения целостности загрузчика им осуществляется копирование основной программы из ПЗУ в ОЗУ с выборкой исправных блоков из двух банков ПЗУ вычислительного канала. При копировании параллельно считается и контрольная сумма блока. Если она не совпадает с хранящейся в ПЗУ, то блок считается испорченным и копируется по такому же принципу из другого банка. Данная операция позволяет получить в ОЗУ исправную копию программы даже при множественном повреждении ее блоков в составе ПЗУ. Размер блоков выбирают наименьшим с целью снижения вероятности искажения блоков, хранящих одну и ту же часть программы в обоих банках. При дальнейшей работе искаженные блоки ПЗУ восстанавливаются соответствующим потоком ОСРВ.

Заключение

Conclusion

Реализация трехканальной архитектуры управляющего вычислителя с типами связей «точка – точка» между каналами и дублированными связями для взаимодействия с внешними системами обеспечивает выполнение предъявленных требований к малогабаритной ВС для СУ малым подводным аппаратом с длительным сроком автономного существования. Ограничения по ГМХ обусловили минимизацию аппаратного исполнения, поэтому все вопросы по синхронизации, контролю и восстановлению ВП были решены на программном уровне.

Основной особенностью такой малогабаритной архитектуры является отказ от внутрисистемных магистралей и выделенных модулей выборки решений с возложением всех системных и диспетчирующих функций на ОСРВ трехканального вычислителя, которая также осуществляет синхронизацию каналов и восстановление системы после сбоя. Используемая блочная структура переключаемых банков памяти обеспечивает сохранность ПО и восстановление каналов в течение всего времени функционирования СУ.

Библиографический список

References

1. *Клячко Л.М., Рогожников А.В., Борисовский Д.В.* Пространственно-распределенные системы мониторинга состояния и управления АНПА и обитаемых ПА в условиях сложной помеховой обстановки естественного и искусственного происхождения в арктической зоне // Управление движением корабля и специальных аппаратов. Труды XXXX Всерос. науч.-техн. конф. ИПУ РАН. 2015. С. 82–93. [*L. Klyachko, A. Rogozhnikov, D. Borisovksiy.* Space distributed status monitoring and control system for AUVs and manned underwater vehicles in difficult natural and man-made background noise situation in the Arctic zone. Control of ships and special-purpose vehicles // Proc. of XXXX All- Russian Scientific & Engineering Conference IPU RAN. 2015. P. 82–93. (In Russian)].
2. *Русанов В.Н., Сильянов Н.В., Киселев А.Ю., Пряничников С.В.* Самодиагностируемая резервируемая бортовая вычислительная система // Аэрокосмическое приборостроение. 2014. Вып. 2. С. 16–27. [*V. Rusanov, N. Silyanov, A. Kisilev, S. Prynichnikov.* Self-diagnostic redundant on-board computer system // Aerokosmicheskoe priporostroenie. 2014; 2: 16–27. (In Russian)].
3. *Русанов В.Н., Сильянов Н.В., Киселев А.Ю.* Самодиагностируемая трехканальная бортовая вычислительная система с резервированием замещением // Аэрокосмическое приборостроение. 2015. Вып. 3. С. 23–31. [*V. Rusanov, N. Silyanov, A. Kisilev.* Self-diagnostic three-channel system with stand-by redundancy // Aerokosmicheskoe priporostroenie. 2015; 3: 23–31. (In Russian)].
4. *Антимиров В.М., Уманский А.Б., Шалимов Л.Н.* Бортовые цифровые вычислительные системы семейства «Малахит» для работы в экстремальных условиях // Вестник СГАУ. 2013. № 4(42). С. 19–27. [*V. Antimirov, A. Umanskii, L. Shalimov.* On-board digital computer system of the Malakhit family for extreme operation conditions // Vestnik SGAU. 2013; 4(42): 19–27. (In Russian)].
5. *Antimirov V.M., Vagin A.Yu., Umanskii A.B., Shalimov L.N., Yatsuk G.E.* A new generation of fail-safe controlling digital computing systems for aerospace hardware // 21st Saint-Petersburg International Conference on Integrated Navigation Systems. Saint-Petersburg, 2014. P. 178–85.
6. Command & Data Handling Systems [electronic resources] / Website RUAG. URL: http://www.ruag.com/space/products/digital-electronics-for-satellites-launchers/data-handling-systems/ (access date 25.11.14).
7. Das Project MUSE [electronic resources] / Website Fraunhofer-Institut für Offene Kommunikationssysteme. URL: http://www.fokus.fraunhofer.de/go/muse (access date 14.11.14)
8. *Longden L., Thibodeau Ch., Hillman R., Layton Ph., Dowd M.* Designing a single board computer for space using the most advanced processor and mitigation technologies // Maxwell Technologies. 2012. P. 17.
9. *Есиновский А.В., Леонтьев А.В., Уманский А.Б.* Вычислительный модуль повышенной надежности для систем

управления космическими аппаратами // Вопросы электромеханики. 2014. № 4. Т. 141. С. 27–30. [*A. Esinovskiy, A. Leontiev, A. Umanskii.* Computer module of enhanced reliability for space craft control systems // Voprosy electromeckhaniki. 2014; 4(141): 27–30. (In Russian)].

10. *Соловьева Н.В., Чебанов Е.Е., Дудин Н.В., Ханевский Д.А., Баженов А.И.* К вопросу создания собственной операционной системы реального времени // РКТ. Сер. XI. Системы управления ракетных комплексов. 2012. Вып. 1. С. 59–68. [*N. Soloviev, E. Chabanov, N. Dudin, D. Khanevskiy, A. Bazhenov.* On development of our own real-time operating system // RKT. Ser. XI. Missile control systems. 2012; 1: 59–68. (In Russian)].

Сведения об авторах

Уманский Алексей Борисович, к.т.н, начальник сектора АО «Научно-производственное объединение автоматики им. академика Н.А. Семихатова». Адрес: 620075, Россия, г. Екатеринбург, ул. Мамина-Сибиряка, д. 145. Тел.: +7 (343) 263-76-89; E-mail: pdwn1982@yandex.ru.

Яцук Георгий Евгеньевич, начальник сектора АО «Научно-производственное объединение автоматики им. академика Н.А. Семихатова». Адрес: 620075, Россия, г. Екатеринбург, ул. Мамина-Сибиряка, д. 145. Телефон: +7 (343) 263-76-89; E-mail: rx9cim@rambler.ru.

Ананьин Александр Сергеевич, инженер-конструктор АО «Научно-производственное объединение автоматики им. академика Н.А. Семихатова». Адрес: 620075, Россия, г. Екатеринбург, ул. Мамина-Сибиряка, д. 145. Телефон: +7 (343) 263-76-89; E-mail: ananyinac@yandex.ru.

About the authors

Umanskii A., Candidate of Technical Sciences, Head of sector, Scientific and Production Association of Automatics named after academician N.A. Semikhatov. Address: ul. Mamina-Seberyaka 145, Yekaterinburg, 620075, Russia. Tel.: +7 (343) 263-76-89; E-mail: pdwn1982@yandex.ru.

Yatsuk G., Head of sector, Scientific and Production Association of Automatics named after academician N.A. Semikhatov. Address: ul. Mamina-Seberyaka 145, Yekaterinburg? 620075, Russia. Tel.: +7 (343) 263-76-89; E-mail: rx9cim@rambler.ru.

Ananyin A., Design engineer, Scientific and Production Association of Automatics named after academician N.A.Semikhatov. Address: ul. Mamina-Seberyaka 145, Yekaterinburg, 620075, Russia. Tel.: +7 (343) 263-76-89; E-mail: ananyinac@yandex.ru.

Поступила / Received: 14.02.18
Принята в печать / Accepted: 18.04.18