УДК 681.5

Отказобезопасная вычислительная система для комплексных систем управления полётом летательных аппаратов

В.А Сапогов, К.С Анисимов, А.В Новожилов.

Аннотация

В данной статье рассмотрен один из подходов построения функциональной архитектуры и архитектуры информационного обмена бортовой распределённой вычислительной системы (БРВС) комплексной системы управления (КСУ) для реализации требования отказобезопасности бортовых систем управления полётом. Разработан технический облик в целом отказобезопасной БРВС для типовой КСУ магистрального пассажирского самолёта. Сформированы новые принципы разработки отказобезопасного программного обеспечения и реконфигурации режимов его функционирования при отказах в интересах обеспечения требуемой надёжности КСУ и заданного уровня безопасности полётов.

Ключевые слова

комплексная система управления; электродистанционные системы управления; бортовая вычислительная система; отказобезопасная вычислительная система.

1. Введение

В настоящее время интенсивно развивается новое направление авиационного приборостроения, в рамках которого взамен механической проводки управления от рычагов управления летательным аппаратом к аэродинамическим рулевым поверхностям разрабатываются цифровые электродистанционные системы управления (СДУ), которые в совокупности с системами автоматического управления (САУ) и другими системами автоматизации полёта образуют комплексные системы управления. В связи с прямым влиянием на безопасность полётов КСУ приобрели статус систем с полной ответственностью за безопасность полётов. Основу таких систем управления составляют бортовые распределённые вычислительные системы реального времени (РВ). В силу прямого влияния на безопасность полётов разработка отказобезопасных БРВС РВ, являющихся ядром КСУ,

приобрела в авиации ключевое значение. Технологии разработки БРВС для систем управления полётом в ведущих странах мира, разрабатывающих и производящих пассажирские самолёты, считаются национальными критическими технологиями. Целью работы является разработка технического облика отказобезопасной БРВС для типовой КСУ магистрального пассажирского самолёта.

В России и за рубежом интенсивно развивается новое направление авиационного приборостроения, в рамках которого взамен механической проводки управления от рычагов управления летательным аппаратом (самолётом или вертолётом) к аэродинамическим рулевым поверхностям (элеронам, интерцепторам, рулю высоты, рулю направления и др.) разрабатываются цифровые электродистанционные системы (СДУ), которые в совокупности с системами автоматического управления (САУ) и другими системами автоматизации полёта образуют КСУ. КСУ позволяют уменьшить массу системы управления, резко повысить уровень автоматизации управления полётом, снизить требования к квалификации пилотов. В связи с прямым влиянием на безопасность полётов КСУ приобрели статус систем с полной ответственностью за безопасность полётов. Основу таких систем управления составляют БРВС реального времени (РВ). В силу прямого влияния на безопасность полётов разработка отказобезопасных БРВС РВ, являющихся ядром КСУ, приобрела в авиации ключевое значение. Технологии разработки БРВС для систем управления полётом во многих странах считаются национальными критическими технологиями. Особенно это касается самолётов и вертолётов гражданской авиации, к которым в плане обеспечения безопасности полётов предъявляются повышенные требования. КСУ всех новейших зарубежных самолётов строятся на основе резервированных БРВС. В ОАО МНПК «Авионика» создан научно-технический задел и накоплен определённый опыт применительно к разработке БРВС для КСУ, который требуется развить и обобщить в приложении к КСУ ЛА гражданского назначения, имеющих существенную специфику в части требований к обеспечению безопасности полётов. Проблематика работы является весьма актуальной с учётом необходимости создания импортозамещающих технологий разработки отказобезопасных БРВС для систем управления полётом.

2. Состав и структура КСУ

На современных летательных аппаратах (ЛА) применяется большое разнообразие средств автоматизации управления полётом. Анализ взаимосвязей этих средств показал целесообразность их объединения в единую комплексную систему управления ЛА [1, 2]. Состав и структура КСУ определяются назначением ЛА. Наиболее развитые средства автоматического и автоматизированного управления полётом имеют магистральные пассажирские самолёты, к которым предъявляются жёсткие требования по уровню обеспечения безопасности полётов. КСУ таких самолётов должны удовлетворять как общим требованиям, предъявляемым к бортовой авионике с учётом ожидаемых условий эксплуатации, так и специальным требованиям, обусловленным непосредственным влиянием систем управления на безопасность полётов. Такое влияние связано с переходом от механической проводки управления к системам электродистанционного управления (СДУ), которые приобрели статус «систем с полной ответственностью».

КСУ, объединяющая СДУ, САУ и другие системы, предназначена для обеспечения:

- управления полетом и балансировки самолета посредством отклонения аэродинамических поверхностей управления по командным сигналам экипажа, обеспечения автоматического и директорного управления полетом;

- управления стабилизатором по командным сигналам экипажа и системы автоматического управления (САУ), обеспечения посадки по категории IIIB (автоматическая посадка до касания ВПП и автоматический пробег и торможение);

- управления механизацией крыла по командным сигналам экипажа;

- автоматического управления тягой двигателей по командным сигналам САУ;

- автоматического и ручного по командным сигналам экипажа управления поворотом колес передней опоры и тормозами колес шасси;

- автоматического ограничения предельных значений параметров полета;

- снижения нагрузок на крыло при маневрах, действии порывов ветра и атмосферной турбулентности. Снижения перегрузок в хвостовой части самолета при действии атмосферной турбулентности;

- функционирования в ожидаемых условиях эксплуатации и обеспечения необходимых характеристик устойчивости и управляемости, в соответствии с требованиями,

изложенными в сертификационном базисе (СБ), разрабатываемом на основании Российских норм летной годности АП-25 с дополнениями в виде «Специальных технических условий», отражающих отличия отечественных норм АП-25 и зарубежных норм FAR-25 (США) и CS25 (ЕС), как при нормальной работе, так и при расчетных отказах в КСУ и во взаимодействующих системах.

Для реализации этих требований в состав КСУ магистрального пассажирского самолёта входят: система дистанционного управления (СДУ); автоматизированная система управления механизацией крыла (АСУ МК); система управления балансировкой самолёта (СУ БС); система автоматического управления полётом (САУ); автомат управления тягой двигателей (АУТД); система управления поворотом колеса передней стойки и тормозами колёс основных стоек шасси (СУ ПКТК); система ограничительных сигналов (СОС); система предупреждения критических режимов (СПКР); система встроенного предполётного и полётного контроля (СВК); система снижения нагрузок и перегрузок (ССНП); система интеллектуальной поддержки экипажа по управлению самолётом (СИПЭ УС); система ввода-вывода информации (СВВИ). Указанные системы КСУ реализуются в виде программно-аппаратных составных частей и/или программных модулей её БРВС. Например, в состав БРВС в части СДУ должны входить:

- вычислители КСУ, реализующие весь комплекс задач управления самолетом;

- блоки управления и контроля (БУК) приводов, реализующие весь комплекс задач управления и контроля управления приводами и функции ручного управления самолетом.

3. Функциональная архитектура КСУ

При разработке КСУ в качестве преобладающего рассматривался принцип автономии относительно интегрированного комплекса бортового оборудования (ИКБО) ЛА в интересах обеспечения её надёжности и безопасности полётов[3]. Более того, в составе КСУ для резервного режима (прямого) управления вводится дополнительная внутренняя полная автономия. На этот режим “наслаиваются” все другие режимы управления, реализующие дополнительные функции.

Так же при разработке архитектуры КСУ учитывался человеческий фактор. Изначально предполагалось, что любой элемент одного типа (т.е. разрабатываемый одной группой разработчиков) может содержать, не выявленную в ходе предварительных испытаний, ошибку. Что в свою очередь может привести к катастрофе ЛА.

Для уменьшения влияния человеческой ошибки на безопасность системы было принято решение об использовании разновесионного функционального программного обеспечения и гетерогенной (разнородной по типам вычислителей) распределённой вычислительной среды, а также новых архитектур и каналов информационного обмена (таких как CAN, AFDX), позволяющих обеспечить более высокий уровень надёжности. Так, вычислители «контролируемых пар» или «контролируемых триад» основного, упрощенного и резервного режимов должны использовать элементную базу различных производителей с различной технологией, внутренней архитектурой и программным обеспечением.

При разработке функциональной архитектуры КСУ определялись взаимосвязи системы управления в структуре бортового оборудования самолёта и далее производилась её детализация с учётом задач и функций элементов системы управления, а также с учётом состава КСУ, определенного Техническими требованиями.

Полученная таким образом функциональная архитектура КСУ в укрупнённом виде представлена на Рисунке 1, на котором приняты следующие сокращения: ИПК – информационное поле кабины; СУ ОСО – система управления общесамолётным оборудованием; СУ – силовая установка; СИПЭ – система интеллектуальной поддержки экипажа по управлению самолётом; ЭССиУС– экспертная ситуационная советующая и управляющая система; ИСДСУ–интегрированная система диагностики (идентификации) ситуаций управления; ФС – функциональное состояние; Э – экипаж; КБОу – сигналы управления из КБО; КБОд – сигналы датчиков из КБО; РК – разовые команды.

Функциональная архитектура характеризует функциональный состав КСУ, позволяет распределить задачи КСУ по функциональным элементам и проанализировать их взаимосвязи, а также позволяет оценить возможности функционального резервирования.

Как видно из Рисунка 1, КСУ воспринимает управляющие сигналы и команды от экипажа, управляющие сигналы и сигналы датчиков от интегрированного комплекса бортового оборудования (ИКБО), выдаёт на информационное поле кабины информацию о текущем режиме управления полётом и сигналы приближения к предельным режимам с учётом действующих ограничений, взаимодействует с СУ ОСО и выдаёт сигналы управления на приводы.

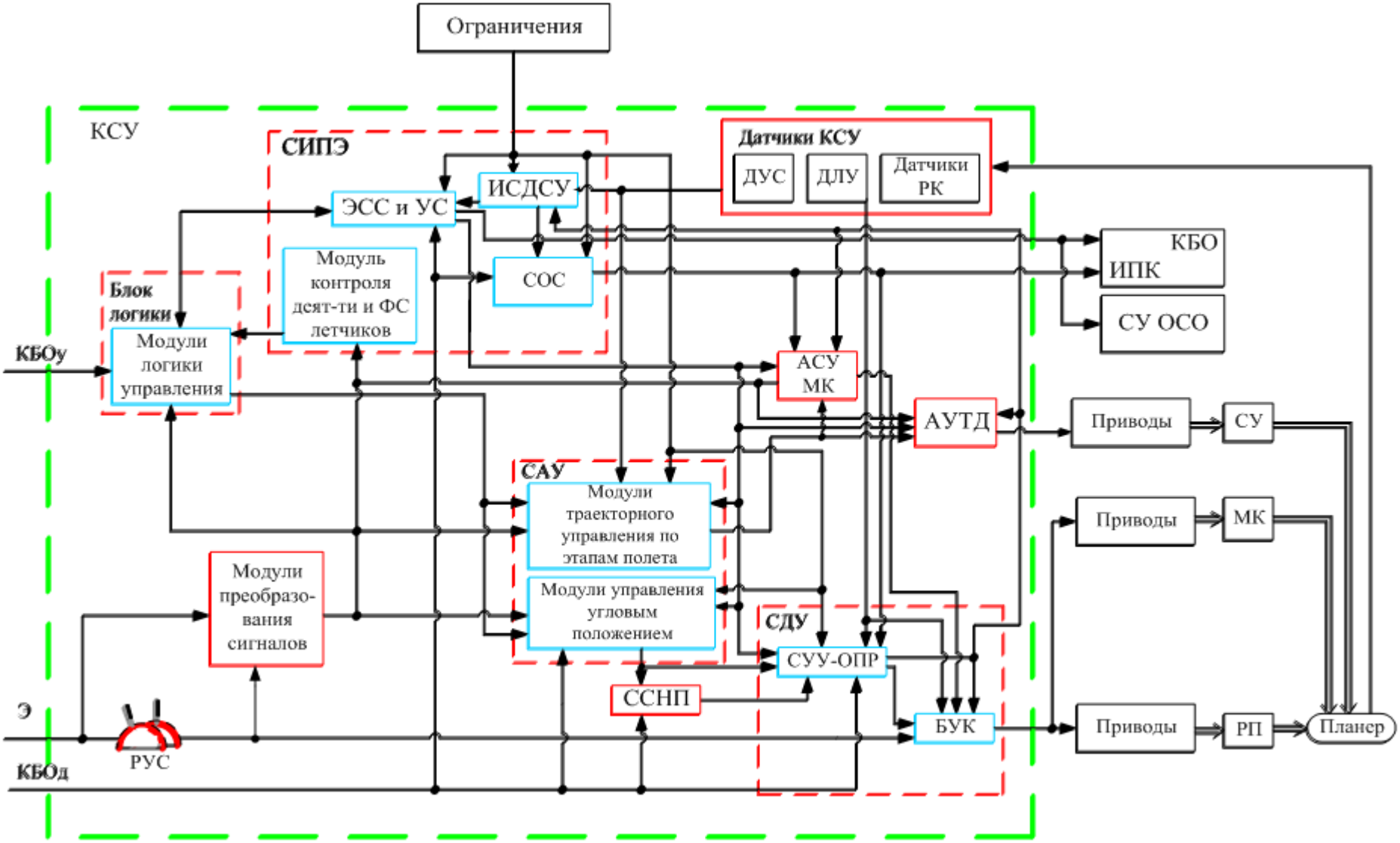

Рисунок 1 – функциональная архитектура КСУ

4. Архитектура информационного обмена в КСУ

Архитектура вычислительной системы КСУ представлена на Рисунке 2. Предусматривается создание высокоинтегрированной цифровой вычислительной среды, включающей три группы каналов цифрового информационного обмена (КИО) и вычислители (процессоры) разных уровней обработки информации.

Первая группа КИО – КИО КБО – обеспечивает обмен информацией с интегрированным КБО и другими внешними по отношению к КСУ системами. Для повышения живучести каналы разносятся по левому и правому бортам. Связь с внешними вычислительными устройствами осуществлятся по высокоскоростной цифровой линии связи ARINC-664 (AFDX). В качестве одного из вариантов информационного обмена с системами КБО рассматривается применение высоконадёжных и отработанных CAN-интерфейсов.

Вторая группа КИО (внутренние КИО КСУ в целом и СДУ в основном и упрощённом режимах управления) обеспечивает обмен информацией внутри КСУ между процессорами всех уровней управления, контроля и реконфигурации, а также обеспечивает взаимодействие КСУ с экипажем через устройства преобразования сигналов (УПС), входящие в состав вычислителей КСУ. Процессоры вычислителей КСУ решают задачи контроля входной информации (информации датчиков и управляющей информации из КБО и от экипажа) и контроля состояния собственных программно-аппаратных средств, реконфигурации вычислительных ресурсов и синтеза управляющих воздействий применительно к алгоритмическим уровням полной конфигурации САУ и СДУ.

В состав вычислителей КСУ входят четыре 2-х процессорные платы вычислителей (на каждой плате два разнородных процессора с разноверсионным ПО). Между платами организуется межмашинный обмен информацией. Количество плат выбрано с учётом того, что система управления должна нормально функционировать практически без ухудшения характеристик устойчивости и управляемости после двух одноименных отказов ее подканалов. Четырехканальная система может обеспечить необходимый уровень безотказности[4], которая составляет $P(t)=10^{-8}$ на один час полета в основном и упрощенном режимах управления.

Наиболее надежным методом проверки правильности реализации ПО является метод сравнения с моделью[5]. Сигналы управления рулевыми поверхностями, передающиеся в БУК, сравниваются с модельными и в случае расхождения более чем

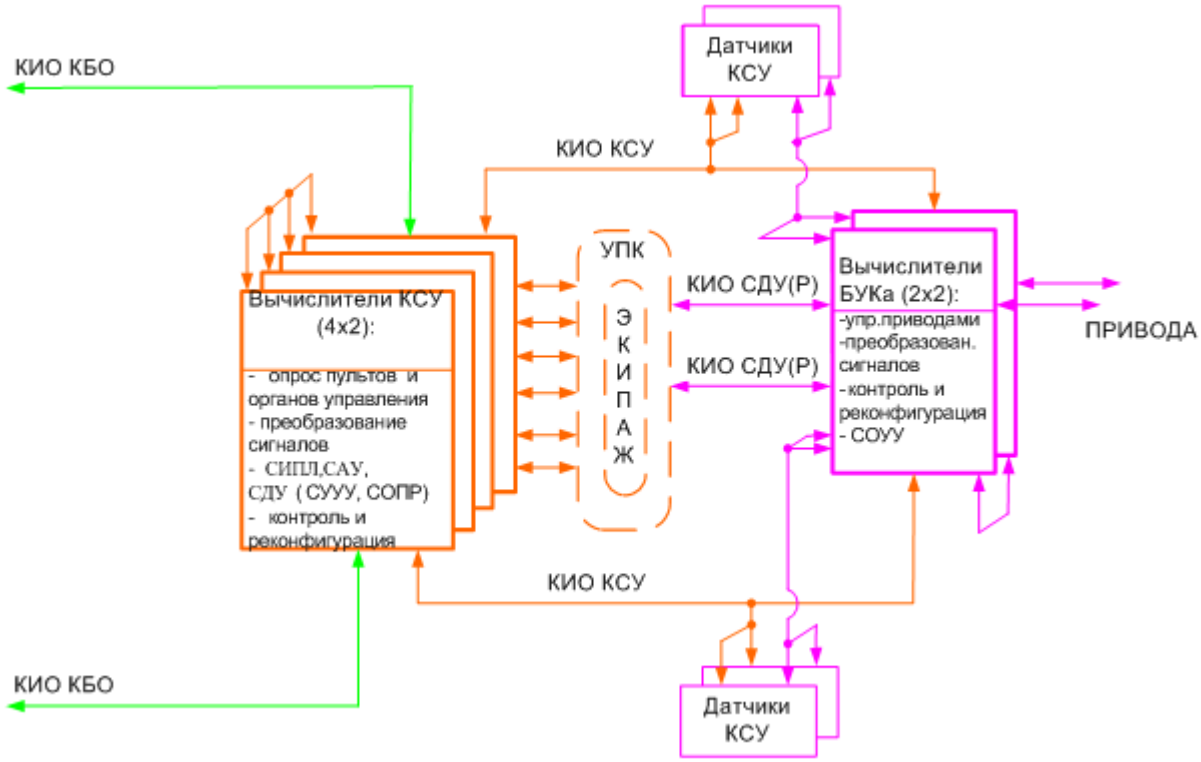

Рисунок 2 - Архитектура вычислительной системы

на пороговое значение, происходит автоматический переход на резервное управление.

При отказах вычислителей или/и КИО КСУ (реализующих функции САУ и СДУ в основном и упрощенном режимах) имеется возможность прямой передачи управляющих воздействий от рычагов управления кабины непосредственно на вычислители блоков управления и контроля (БУК) приводов с использованием КИО СДУ. В этом случае реализуется резервный режим работы КСУ. Применительно к управлению основными рулевыми поверхностями с помощью электрогидравлических приводов типа ЭГРП (на каждую рулевую поверхность работают два однотипных привода) вычислители БУКов, как показано на Рисунке 2, имеют две 2-х ядерные платы, между которыми организован межмашинный обмен информацией. Всего на два привода работают четыре разнотипных процессора с разноверсионным ПО.

Платы цифровых вычислителей БУКов конструктивно унифицированы с платами цифровых вычислителей КСУ. Рулевая поверхность остаётся управляемой до третьего отказа процессоров любого характера - аппаратного, «архитектурного», программного. Под «архитектурными» понимаются отказы процессоров, связанные с недостатками отработки архитектуры процессоров конкретного типа и их системного ПО. Наряду с вычислителями

БУКов в резервном режиме функционируют четырёхкратно резервированные собственные датчики КСУ (по два датчика на каждом борту).

Таким образом, все платы вычислителей КСУ и БУКов разнородны по типу процессорных ядер и имеют разноверсионное системное и функциональное ПО. Аппаратура в максимальной степени унифицирована в части аппаратного ядра и плат вычислителей БУКов применительно ко всем типам исполнительных устройств (приводов рулевых поверхностей, элементов механизации крыла, автоматики управления шасси и т.п.).

В общем виде архитектура информационного обмена в КСУ для основного и упрощенного управления представлена на Рисунке 3. На Рисунке 4 представлена структурная схема для резервного режима функционирования КСУ. В этом режиме обеспечивается непосредственная прямая связь между рычагами управления кабины и соответствующими группами БУКов или одиночными БУКами. В БУКах осуществляется проверка достоверности и выбор информации от РУБ и интегральных блоков датчиков (ИБД). Аппаратура в этом режиме имеет наиболее простую конфигурацию, многократно резервирована по каналам информационного обмена с экипажем и по вычислителям БУК приводов основных поверхностей управления, а, следовательно, обеспечивает и наивысшую надёжность и живучесть. Эта схема позволяет реализовать и «сквозное» аналоговое управление приводами.

При возникновении различных комбинаций отказов аппаратных средств и программного обеспечения для их своевременного обнаружения и парирования предусмотрены несколько сечений входного контроля (кворумирования и мажорирования) информации, а также межмашинный информационный обмен.

Информация, поступающая из внешних систем, контролируется на уровне вычислителей КСУ. Информация, поступающая от экипажа (с ручек управления боковых (РУБ), с датчиков положения резервированных (ДПР), с пультов и других средств управления кабины) контролируется в вычислителях КСУ и, независимо, в БУКах. В вычислителях КСУ и БУКов контролируется также информация, поступающая от датчиков ИБД. В блоках управления приводами контролируется информация, поступающая из вычислителей КСУ, а также информация, выдаваемая на привода.

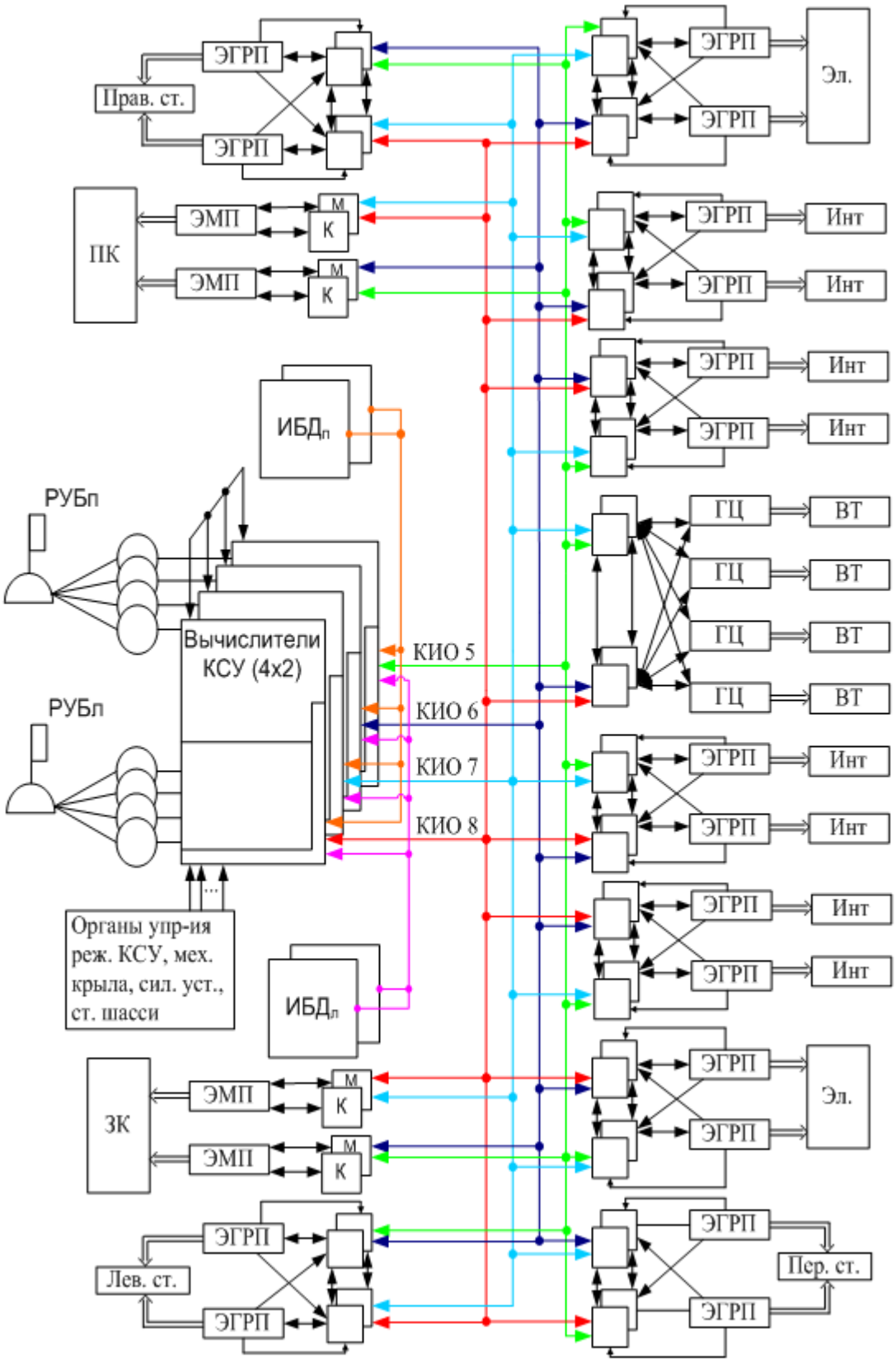

Рисунок 3- архитектура информационного обмена КСУ для основного и упрощенного управления

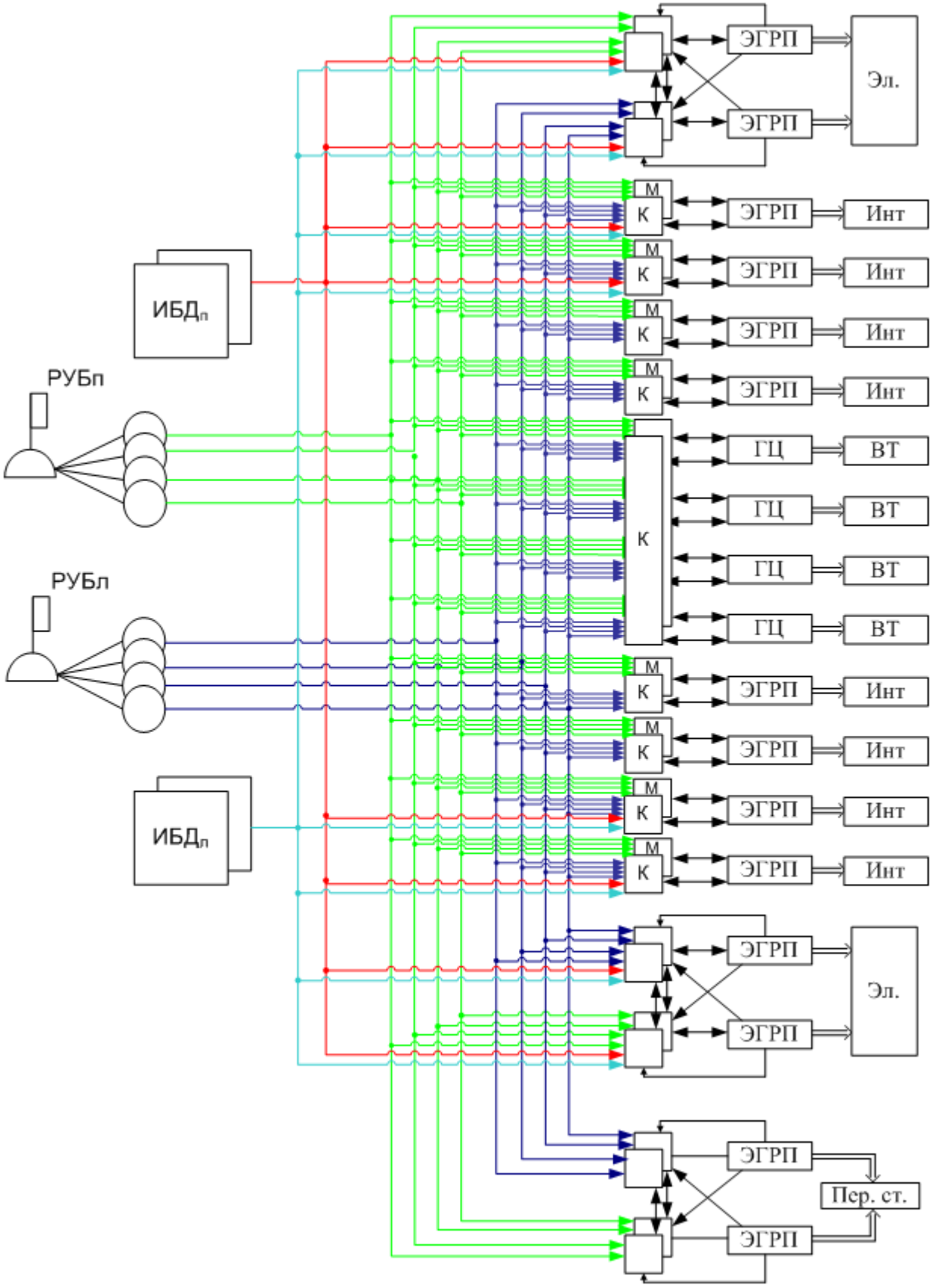

Рисунок 4 – архитектура информационного обмена КСУ для резервного управления

5. Принципы разработки отказобезопасного программного обеспечения

В настоящее время действующие у нас и за рубежом стандарты и квалификационные требования в области создания программного обеспечения для систем бортового оборудования ЛА (такие как MIL STD-498, DO-178B, КТ-178В, ГОСТ Р 51904-2002) достаточно строго формализуют все процессы, этапы и методы проектирования, направленные в первую очередь на обеспечение соответствующего уровня надежности и качества ПО на всем протяжении его жизненного цикла.

В соответствии с требованиями вышеуказанных стандартов, создание программного обеспечения аппаратуры и систем авиационной техники представляет собой совокупность взаимосвязанных процессов образующих жизненный цикл ПО. На рисунке 5 схематично показана модель жизненного цикла компонент ПО КСУ.

На основании требований этих документов основным показателем, определяющим требования к ПО и объем работ, выполнение которых необходимо для доказательства соответствия сертификационным требованиям, является Уровень ПО. Определение Уровня ПО основано на вкладе программного обеспечения в возможные отказные состояния, определяемые в процессе оценки безопасности системы и зависит от категории данного состояния. Причиной появления отказного состояния ПО может явиться не обнаруженная в нём ошибка.

Из анализа безопасности КСУ следует, что потеря ее основной функции, которой является ручное дистанционное управление рулевыми поверхностями самолета, может привести, в соответствии с классификацией АП-25 раздел А0, к катастрофической отказной ситуации. В соответствии с этим и п.2.2.3 КТ-178В для ПО КСУ, без учета особенностей ее построения, должен быть установлен самый высокий уровень – Уровень А. Однако, учитывая особенности построения системы и ее программного обеспечения можно установить различные Уровни ПО для разных его компонент. Согласно требованиям КТ-178В (п.2.3, п.12.3.3), архитектура построения системы с использованием методов обособления и разработки многоверсионного разнородного ПО позволяет снизить уровень ПО, т.к. предотвращается возникновение наиболее опасного отказного состояния по вине ненормальной работы отдельных компонент ПО. В соответствии с требованиями к КСУ и стандартами на разработку ПО, если система должна сохранять работоспособность при проявлении одной ошибки в ПО, то возникает необходимость применения указанных выше методов повышения надёжности и отказобезопасности ПО.

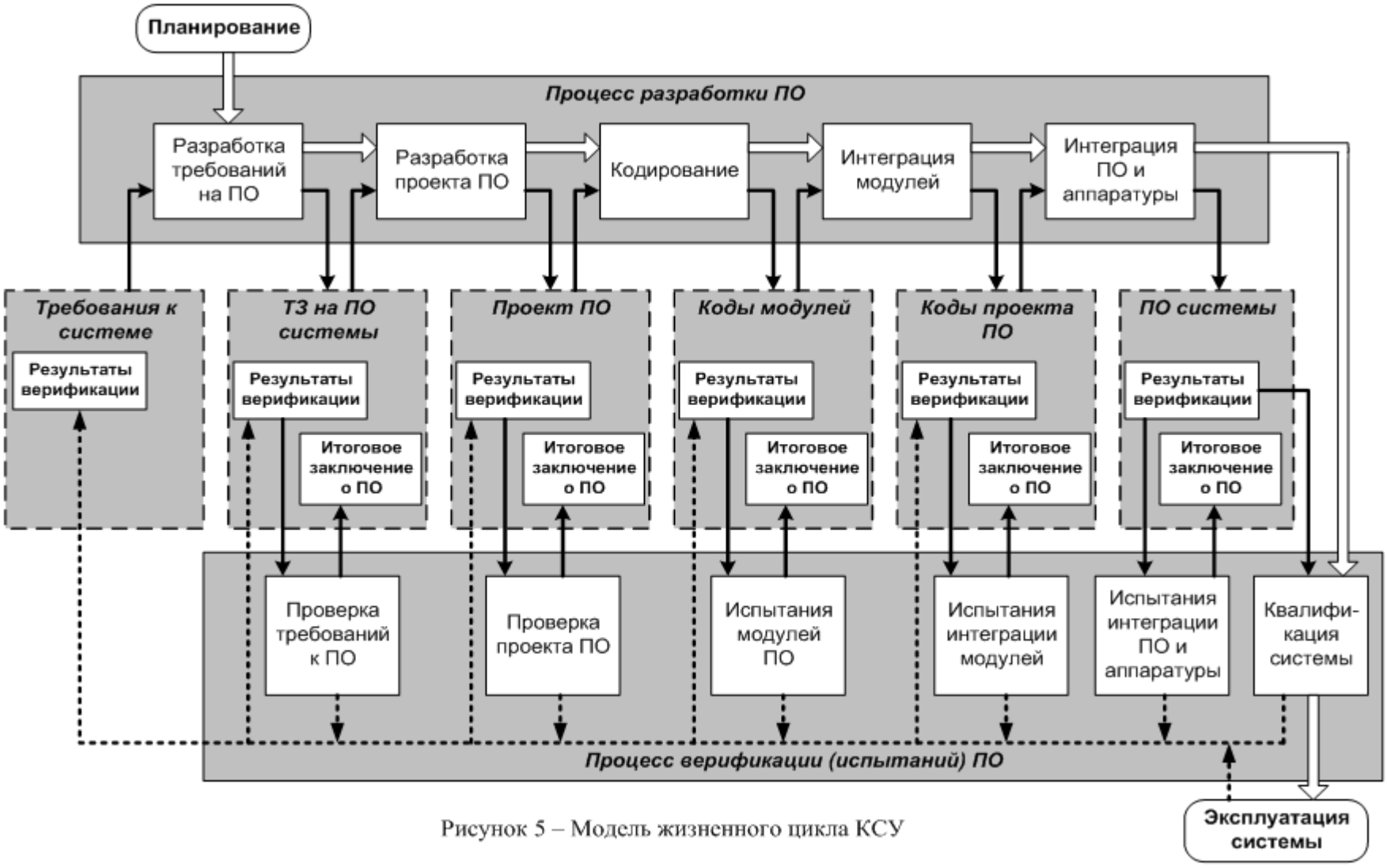

Рисунок 5 – Модель жизненного цикла КСУ

Для ПО резервного управления, обеспечивающего решение задач управления всеми приводами по минимально-допустимым законам управления, была разработана особая структура. Сложность заключается в том, что при разбежке выходных управляющих сигналов между управляющими разноверсионными каналами необходимо выбрать исправный сигнал. БУК представляет собой 4-х кратно резервированный по вычислителям модуль, и обычное кворумирование из 2-х дублированных сигналов, при возникновении ошибки в ПО, приведет к отказу кворума и потере управления. Выйти из сложившейся ситуации можно введя дополнительное модельное ПО. Но простое сравнение модельного и управляющих ПО, в случае ошибки в модельном ПО, может привезти к отказу БУКа. На рисунке 6 показан вариант структуры ПО БУКов для случая 3-х версионного ПО, исключающего указанные коллизии.

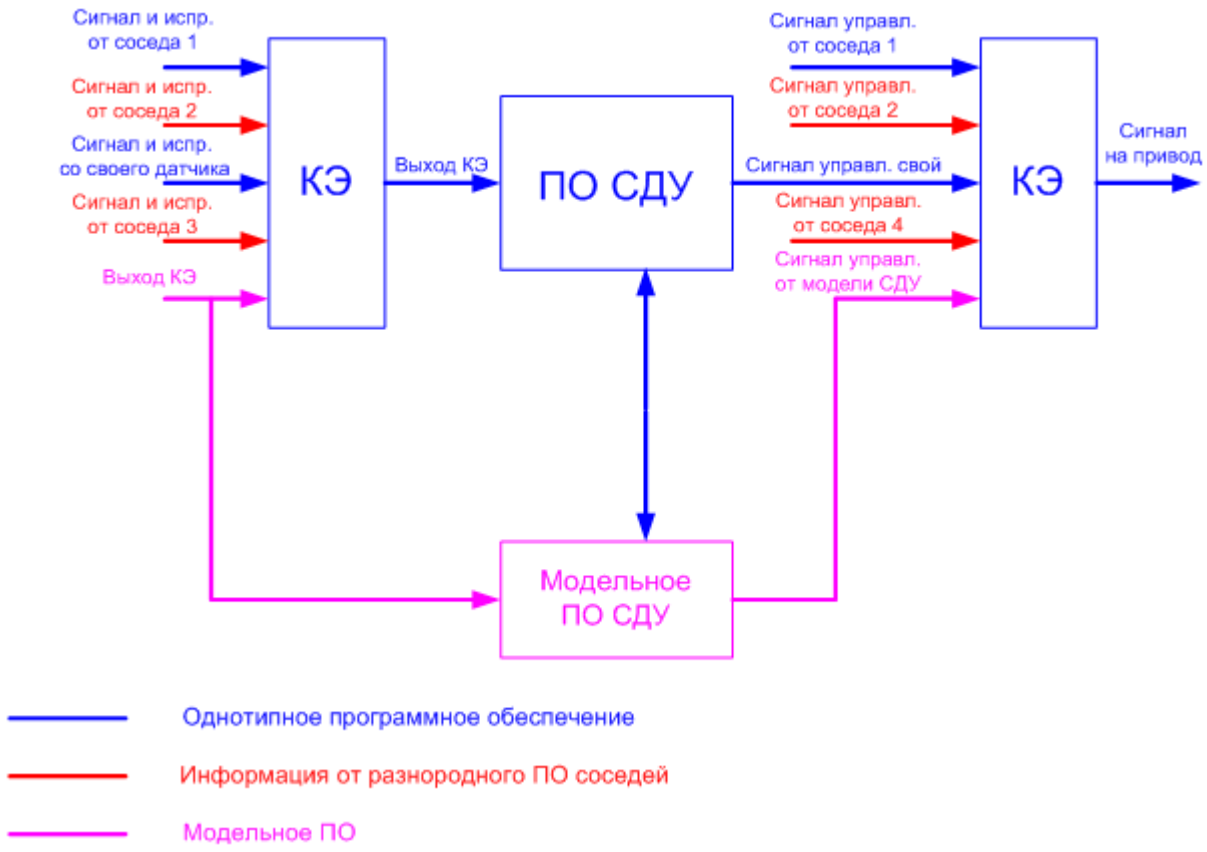

Рисунок 6 - структура ПО БУКа для резервного управления

Такое построение системы обеспечивает не только повышение надежности, но и появляется возможность разделения ПО на два. Первое ПО – резервное (аварийное), необходимое для обеспечения живучести системы, уровень критичности которого должен

соответствовать уровню А. Второе ПО – дополнительное ПО, уровень критичности которого может быть понижен до уровня В по КТ-178В, т.к. отказ его приводит не к катастрофической ситуации, а к существенной. В сумме первое и второе ПО образуют ПО КСУ.

В рамках настоящего проекта разработка программного обеспечения осуществляется с использованием комплекта средств разработки ПО SCADE Suite.

Программный комплекс «SCADE Suite» фирмы ESTEREL Technologies, включаеет в себя квалифицированный генератор программных кодов «SCADE KCG» [6]. Этот инструмент используется компанией «AIRBUS» и многими ее основными поставщиками при разработке большей части критического бортового программного обеспечения самолетов А380 и А400М, а также для вспомогательной системы управления полетом самолетов А340-500/600.

Программный комплекс разработан для обеспечения высочайшего уровня качества и безопасности. Квалифицированный по стандарту DO-178B генератор программного кода на языке С устраняет необходимость в тестировании нижнего уровня, исключает возможность внесения ошибок при написании программного кода.

Применение комплекса позволяет существенно сократить сроки разработки и повысить качество бортового программного обеспечения. Использование программного комплекса SCADE позволяет сэкономить более 35% общих расходов по разработке проекта. При разработке собственно прикладного программного обеспечения SCADE может сэкономить более 50% расходов.

6. Выводы

В рамках работы сформированы функциональная архитектура и архитектура информационного обмена бортовых распределённых вычислительных систем комплексных систем управления полётом, обеспечивающие реализацию требования их отказобезопасности. Разработан технический облик отказобезопасной бортовой распределённой вычислительной системы для типовой комплексной системы управления магистрального пассажирского самолёта. Сформированы новые принципы разработки отказобезопасного программного обеспечения и реконфигурации режимов его функционирования при отказах в интересах обеспечения требуемой надёжности комплексных систем управления полётом и заданного уровня безопасности полётов.

Библиографический список

1. Воробьёв А.В. Концепция проектирования современных комплексных систем управления полётом и технология разработки их программного обеспечения // “Передовые технологии в авиаприборостроении. Материалы V Всероссийской научно-технической конференции национальной ассоциации авиаприборостроителей (НААП). – СПб.: Изд-во Политехн. ун-та, 2009. – 111с.

2. Воробьёв А.В., Кулабухов В.С. Принципы телеоцентрического системного проектирования интеллектуальных систем управления летательных аппаратов// Материалы Третьей Всероссийской научно-практической конференции «Перспективные системы и задачи управления».- Таганрог: Изд-во ТТИ ЮФУ, 2008.
3. Воробьёв А.В., Винокуров В.В., Кулабухов В.С., Залесский С.Е., Абдулин Р.Р. и др. Техническое предложение по комплексной системе управления для семейства самолётов МС-21 (КСУ-МС-21). Пояснительная записка. ОАО МНПК «Авионика», г. Москва, 2009г.
4. Оболенский Ю.Г. «Управление полетом маневренных самолетов».-М. Филиал Воениздат, 2007г
5. Маиерс.Г «Надежность программного обеспечения». М.:Мир,1980
6. Efficient Development of Safe Avionics Software with DO-178B Objectives Using SCADE Suite. Methodological Handbook. Esterel Technologies 2005.

Исследования выполнены в рамках Государственного контракта № 02.740.11.0483 от 20.11.2009 г.

Сведения об авторах

Сапогов Василий Александрович, ведущий инженер Московского научно-производственного комплекса «Авионика», аспирант Московского авиационного института (государственного технического университета). ул. Образцова, д. 7, Москва, 127055; тел.:684-20-42; e-mail: VasiliySapogov@rambler.ru

Анисимов Кирилл Сергеевич, инженер Московского научно-производственного комплекса «Авионика».ул. Образцова, д. 7, Москва, 127055;тел.:684-21-78; e-mail: james-b7@yandex.ru

Новожилов Артем Вадимович, инженер Московского научно-производственного комплекса «Авионика».ул. Образцова, д. 7, Москва, 127055; тел.:684-21-78; e-mail: fboleros@yandex.ru