

Эффективная технология управления циклом жизни бортового программного обеспечения спутников связи и навигации

А.А. Колташев, ФГУП «НПО прикладной механики им. акад. М.Ф. Решетнева»

В НПО ПМ создана и развивается для применения на третьей вычислительной платформе эффективная технология создания бортового программного обеспечения (ПО) спутников связи и навигации. Технология обеспечивает создание высоконадежного, технологичного при разработке, удобного при эксплуатации и переносимого на различные вычислительные платформы бортового ПО (БПО), в сжатые сроки и с гарантированным уровнем качества. Она охватывает весь цикл жизни ПО, предоставляя эффективные методы и средства как для разработки ПО, так и для его долговременного сопровождения.

The effective control technology of the on-board software life cycle of the communication and navigation satellites. A.A. Koltashev

The effective technology of creation of the communication and navigation satellites onboard software has been created at the enterprise and is developed now for application at the third computing platform. This technology provides creation of highly reliable onboard software, technological when developing, convenient when operating and portable for various computing platforms, during short time and with the guaranteed degree of quality. The technology covers the all software life cycle, giving effective methods and means, both for development of the software, and for its long-term maintenance.

Развитие современных систем космической связи и навигации, предусмотренных Федеральной космической программой, требует широкомаштабного создания спутниковых группировок долговременного функционирования. В свою очередь долговременность функционирования спутников на требуемом уровне качества, оперативность их создания, восстановления и восполнения во многом обеспечиваются качеством БПО, технологиями его создания и сопровождения, возможностями инструментальных средств разработки и сопровождения.

К этому следует добавить, что в последние годы в индустрии создания спутников связи сложилась парадоксальная ситуация: несмотря на то, что функциональные задачи, решаемые БПО, остаются от изделия к изделию в основном прежними, из экономических, технических (вес, герметичность исполнения и т.п.) и политических (ограничения стран-производителей на применение) интересов появилась необходимость использовать на функционально одинаковых изделиях разные вычислительные платформы, что делает актуальной задачу создания переносимого БПО. Таким образом, создание эффективной технологии управления циклом жизни БПО спутников связи и навигации, т.е. методов и средств эффективной разработки и долговременного сопровождения переносимого БПО с гарантированным уровнем качества, является актуальной научно-технической, технологической и экономической проблемой, решение которой вносит значительный

вклад в развитие экономики страны и повышение ее обороноспособности.

Вариантом решений этой проблемы служит технология создания БПО спутников связи и навигации, используемая в НПО ПМ. Созданная технология является результатом многолетнего сотрудничества НПО ПМ им. акад. М.Ф. Решетнева и ИСИ СО РАН им. акад. А.П. Ершова, современной реализации и развития принципов и подходов, изложенных в работе [1]. Далее приводится обзор достижений, на которых эта технология базируется.

1. Эффективная архитектурная декомпозиция БПО и типовой набор интерфейсов

Базисом технологии служат используемые принципы структурной декомпозиции и архитектурного расчленения БПО и набор канонических интерфейсов, обеспечивающих эффективный перенос БПО на новые платформы и изделия и возможность программирования команд управления и интегральных режимов логики функционирования подсистем и изделия в целом на проблемно-ориентированных языках сверхвысокого уровня [2]. Архитектура БПО спутников связи и навигации показана на рис. 1.

Среда программного функционирования предоставляет средства для организации вычислительного процесса, а среда программного управления — для командного управления подсистемами спутника в реальном времени. В составе этой среды содержится бортовой интерпретатор команд

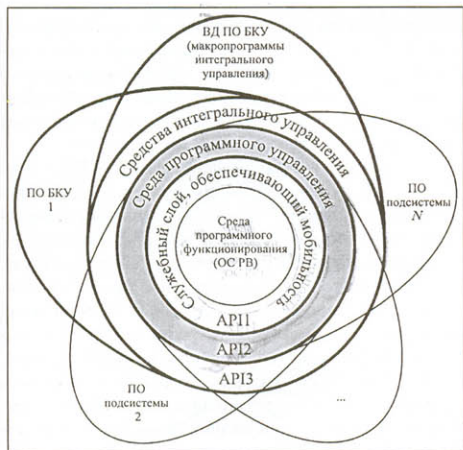


Рис. 1. Архитектура БПО спутника связи с N подсистем спутника

управления, набор команд которого программируется проектантами подсистем на проблемно-ориентированном языке, не зависящем от вычислительной платформы. ПО подсистем реализуется на языке программирования Модуля-2 на базе средств, предоставляемых этими средами, и при постоянстве интерфейсов этих сред становится также независимым от применяемой платформы.

Средства интегрального управления предназначены для решения задач автономного управления спутником в целом и служат бортовым интерпретатором макропрограмм интегрального управления, для написания которых используется проблемно-ориентированный язык программирования, позволяющий реализовать логику функционирования спутника в целом непосредственно ее проектантам. Такая архитектура не только существенно упрощает процесс проектирования и разработки БПО, но и делает его в значительной мере переносимым.

2. Эффективная модель цикла жизни БПО

БПО разрабатывается как встроенное ПО подсистем спутника, объединяемых средствами ПО БКУ и макропрограммами интегрального управления, что подтверждается в рамках подсистем спутника и спутника в целом. Привязка частей БПО к подсистемам спутника позволяет четко определить требования к ПО подсистем и БПО в целом, ответственность за архитектурное проектирование, системное тестирование и подтверждение БПО.

Такая созданная модель цикла жизни БПО определяет принципы структурной организации проекта БПО и уровни распределения ответственности, реализует эффективные модели управления проектом, конфигурацией и верификацией БПО

и гарантирует качество разработки и сопровождения БПО. В основе этой модели лежат “три кита” технологии: разработки компонент БПО, управления конфигурацией БПО и верификации БПО, рассматриваемые далее [3, 4].

3. Эффективная технология разработки компонент БПО

Технология разработки компонент БПО определяет принципы построения унифицированных компонент, требования к типовому проекту компоненты и сценарий разработки и сопровождения компоненты, гарантирующий ее качество. Составляющие технологии перечислены ниже.

1. *Стандартное архитектурное расслоение БПО и набор стандартных интерфейсов.* Реализация канонических интерфейсов слоев на проблемно-ориентированном уровне с использованием абстрактных типов данных и строгой типизации языка Модуля-2 и методические указания по применению конструкций языка программирования обеспечивают построение переносимого ПО.

2. *Типовой сценарий детального проектирования и разработки компоненты* происходит в рамках стандартного документа описания программы параллельно с проектированием набора тестов и кодированием программы. Сценарий предусматривает четыре вехи по уточнению требований к компоненте в процессе ее разработки – “анализ архитектурного проекта завершен”, “проектирование завершенно”, “программирование завершенно”, “разработка и автономное тестирование завершенны”, обеспечивающих согласование позиций проектанта ПО подсистемы и разработчика компоненты. При детальном проектировании компоненты используется разработанный метод нисходящей декомпозиции потока управления в чертежах, неформальных обозначениях с применением графического представления.

3. *Высоконадёжный сильно структурированный язык программирования с абстрактными типами данных и со строгой типизацией данных – Модуля-2* не только переносит выявление большинства ошибок программиста на стадию трансляции, но и благодаря использованию созданных стандартных библиотек типов обеспечивает переносимость компонент на различные вычислительные платформы, снижая требования к квалификации программистов и увеличивая ясность, понимаемость и потенциальную модифицируемость программ для обеспечения их долговременного сопровождения [2, 5]. Для реализации таких программ создана эффективная кросс-система программирования для базовой вычислительной платформы, допускающая ее адаптацию для новых вычислительных платформ с сохранением всех пользовательских и программных интерфейсов (см. раздел 6).

4. Измерение проектных и эксплуатационных характеристик программ связано с методами и средствами измерения статических и динамических характеристик программ, автоматически оценивающими не только достигнутые эксплуатационные характеристики программы (объем памяти, время выполнения, размер стека и т.п.), но и «добротность» программы (оценки выполнения проектных соглашений, уровня сложности программы, комментариев и т.п.).

5. Повторное тестирование и автоматическое определение значений критериев полноты тестирования входят в применяемую технологию пакетного тестирования компонент БПО с использованием платформоно независимого языка тестирования, что позволяет реализовать в терминах языка программирования набор тестовых процедур, гарантирующий достижение критериев полноты тестирования С1 и С2, автоматизация повторного тестирования и сохраняющий актуальность для новых вычислительных платформ.

6. Программирование команд управления и логико-функционального изделий на проблемно-ориентированных языках осуществляется с применением проблемно-ориентированных командных языков и систем программирования (см. раздел 6). Проблемно-ориентированный интерфейс этих систем позволяет создавать и тестировать прикладное ПО непосредственно проектантами систем без участия программистов, т.е. без «шума» (неодинакового понимания), возникающего в процессе создания ПО в интерфейсе «проектант системы – программист ПО системы». Влияние этого шума особенно существенно для класса встроенных компьютерных систем, к которому относятся бортовые комплексы управления спутников связи, и при обычном подходе устраняется методами п. 2 и верификацией.

7. Создание компонент БПО как унифицированных компонент и на унифицированных средствах производится в рамках не только изделия, но и объекта, унифицированного по проектным соглашениям, интерфейсам, языку программирования, библиотекам типов данных, поэтому компонента пригодна благодаря этому свойству к заимствованию и переиспользованию на других изделиях. При этом компоненты разрабатываются на средствах, рассмотренных в разделе 6.

4. Технология управления конфигурацией БПО

Для управления конфигурацией БПО разработаны методы и средства идентификации и управления объектами, работами и проблемами ПО, разработаны процедуры и средства, автоматизирующие процессы управления конфигурацией, формы и процедуры электронного документооборота, созданы необходимые архивы сопровождения. Технология управления

конфигурацией базируется на трех составляющих: специальных методах идентификации и представления компонент; системе автоматизированного управления объектами, работами и проблемами БПО; системе автоматизированного управления архивами компонент и изделий.

Каждая конфигурационная единица БПО – программа, сборка, выпуск представляется в виде программного проекта – электронной папки специальной структуры, содержащей всю информацию, необходимую для ее разработки и сопровождения. Управление конфигурационными единицами обеспечивается через три электронных подконтрольных архива: сопровождения работ и проблем, проектов унифицированных программ, БПО изделий.

Каждый объект разработки возникает как компонента, специфицированная архитектурным проектом, в рамках конкретного изделия. После утверждения первой редакции архитектурного проекта информация о всех компонентах вместе с графиком их разработки заносится в Архив сопровождения работ и проблем этого изделия. В итоге разработка компоненты заканчивается передачей всей документации сопровождения, оформленной как проект программы, в Архив проектов унифицированных программ, а сама компонента, настроенная на конкретное применение, передается в Архив БПО изделия. В рамках этого архива осуществляются интеграция БПО и его изготовление.

После попадания в архив ошибки в компоненте исправляются на основании отчетов о проблеме в ПО, а изменение в связи с уточнением требований осуществляется по запросам-отчетам, уточняющим требования архитектурного проекта и определяющим полный цикл работ, требующих повторения. Вся информация об отчетах о проблемах и запросах-отчетах хранится в Архиве сопровождения работ и проблем. Предложенные методы и средства не только отражают историю изменения объектов БПО, но и автоматизированно управляют конфигурацией БПО – документируют возникшие проблемы, инициируют работы по их устранению, контролируют завершенность проблем, целостность сборок БПО, санкционированность и завершенность всех его изменений.

5. Технология верификации и подтверждения БПО

В технологии выделены девять стандартных этапов верификации и подтверждения БПО, в рамках которых применены новые методы и средства: верификация требований, архитектурного проекта, средств разработки и тестирования БПО, детального проекта, кода; автономное тестирование компонент, интеграционное и системное тестирование ПО подсистем и БПО в целом на наземных отделочных комплексах (НОК) (рис. 2); подтверждение



Рис. 2. Архитектура НОК БПО с обозначениями: БЦВК – бортовой цифровой вычислительный комплекс; ИКБК – интерпретатор команд бортового компьютера; БД КУ – база данных команд управления; ТМИ – телеметрическая информация; ЦГ – циклограммы испытаний; АСУ ИТО – АСУ испытаний и телеметрической обработки; GUI1 – штатный интерфейс; GUI2 – отладочный интерфейс; GUI3 – технологический интерфейс

ПО подсистем и БПО в целом в составе подсистем на инженерных моделях и летном изделии. Часть используемых методов рассмотрена выше в рамках гарантирования качества компонент.

Главными достижениями для обеспечения верификации и подтверждения ПО подсистем и БПО в целом являются:

1. Применение в составе средств тестирования верифицированных программных моделей бортового процессора, моделей устройств бортового комплекса управления, моделей поведения подсистем спутника, позволяющих в полном объеме провести автономное и системное тестирование БПО без использования реальной аппаратуры. Побочным положительным эффектом этого подхода является “вынужденное” доскональное изучение логики функционирования аппаратуры и ее интерфейсов проектантами и программистами БПО.

2. Высокий уровень пользовательского интерфейса средств тестирования, позволяющий проводить системное тестирование непосредственно проектантам логики функционирования подсистем изделия и изделия в целом.

3. Полное сохранение пользовательских интерфейсов средств тестирования при использовании моделей разных вычислительных платформ.

4. Применение не только диалоговых средств тестирования и отладки, но и языков и средств пакетного тестирования и отладки, позволяющих проектировать и программировать тесты по той же технологии,

что и тестируемые программы БПО. При этом использование пакетов тестов автоматизирует регрессивное тестирование и постоянно улучшает набор тестов, а переносимость компонент БПО и постоянство интерфейсов средств тестирования сохраняют актуальность архивов тестов для новых изделий.

5. Организация системного тестирования в соответствии с архитектурной декомпозицией БПО. Такой подход обеспечивает эффективное распределение ответственности за последовательность и уровни системного тестирования. В действующей технологии системное тестирование осуществляется последовательно на пяти уровнях: среды программного функционирования (на уровне операционной системы), среды программного управления, ПО подсистемы в режимах системы, ПО подсистемы в режимах КА и на уровне БПО в целом (на уровне макропрограмм интегрального управления).

6. Обзор средств разработки и сопровождения БПО

Средства разработки, реализующие и поддерживающие перечисленные выше методы, представлены Технологическим комплексом производства программ (ТКПП) БПО (рис. 3). В его составе реализованы:

1. Мобильная КСП на языке Модуля-2, которая может быть адаптирована для различных целевых платформ, сохраняя все пользовательские интерфейсы. В дополнение к стандартным средствам данная система предоставляет пакетный отладчик, позволяющий организовать регрессивное тестирование, средства измерения полноты автономного тестирования (по критериям С1 и С) и средства измерения эксплуатационных характеристик компонент, гарантирующие требуемый уровень качества компонент БПО. Созданная в сотрудничестве с ИСИ СО РАН и ООО “Эксельсиор” КСП соответствует мировому уровню средств разработки надежного ПО для встроенного применения, превосходя его по отдельным показателям.

2. Мобильная система программирования команд управления конкретным изделием – ИСПОЛКОМ, позволяющая программировать набор команд управления подсистемами спутника непосредственно их проектантам.

3. Мобильная система программирования логики функционирования систем изделия – РЕАЛ, создающая макропрограммы интегрального управления непосредственно проектантами логики функционирования спутника.

4. Независимые от вычислительной платформы базовые средства разработки БПО, решающие задачи хранения и сопровождения компонент БПО и БПО в целом и задачи управления их конфигурацией. Все

Задачи, обеспечиваемые ТКПП БПО:

1. Архитектурное проектирование ПО систем и БПО в целом
2. Детальное проектирование и программирование программ и данных
3. Автономное тестирование программ
4. Сборка и изготовление БПО
5. Системное тестирование ПО подсистем и БПО в целом
6. Сопровождение архивов и баз данных БПО
7. Управление работами, конфигурацией и качеством

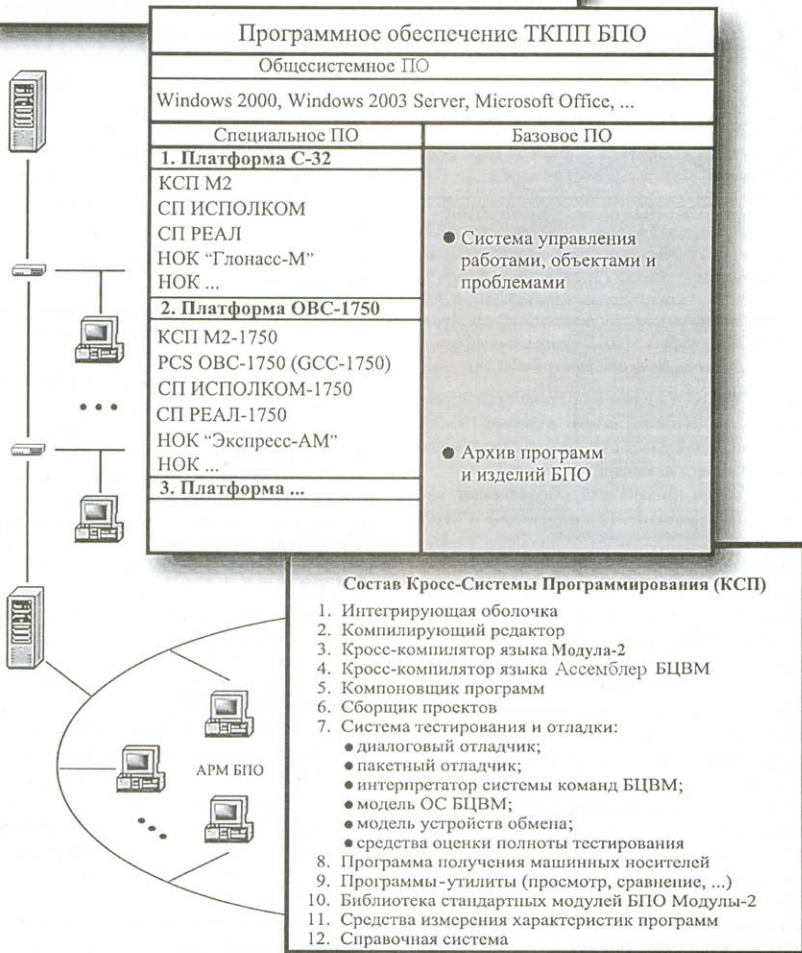


Рис. 3. Технологический комплекс производства программ БПО

средства эффективно функционируют на любой ПЭВМ на платформе Intel Pentium IV в среде ОС Windows 2000 или 2003.

5. НОК БПО, обеспечивающие интеграционное и системное тестирование БПО, изготовление и сопровождение БПО конкретных изделий (рис. 2). НОК содержит БПО конкретного изделия, программную модель целевого БЦВК и аппаратуры БКУ, модели поведения систем изделия, средства организации модельного вычислительного процесса и средства отладки.

НОК предоставляет проблемно-ориентированный пользовательский интерфейс, позволяющий проводить системное тестирование ПО систем и БПО в целом, непосредственно проектантам подсистем спутника и логики функционирования спутника в целом. Интерфейс НОК унифицирован с интерфейсами средств заводских испытаний и управления при эксплуатации. Если это предусмотрено контрактом, на основе НОК создается имитатор КА, предназначенный для тренировки персонала Центров управления и сопровождения спутника в режиме эксплуатации.

Заключение

Ряд составляющих технологии внедрен и отработан еще в рамках первого поколения спутников с БЦВМ – в проектах “Луч”, “Галс”, “Экспресс”, “Экспресс-А”, “Сесат”. Для этой вычислительной платформы программирование производилось на языке Ассемблер БЦВМ. А в полном объеме с использованием языка Модула-2 технология применена для двух различных вычислительных платформ в рамках проектов “Глонасс-М” (4 действующих спутника на текущий момент) и “Экспресс-АМ” (5 спутников) и не только успешно решила задачи по созданию эффективного и надежного БПО, удобного при эксплуатации и сопровождении (проект “Глонасс-М”), но и продемонстрировала возможность реального переноса значительного объема БПО и переиспользования информации сопровождения (исходных текстов, документации, тестов и т.п.) на существенно отличную вычислительную платформу (проект “Экспресс-АМ”). Переносимое

БПО изначально разрабатывалось для 32-разрядной CISC-архитектуры с прямой эндианностью, а переносилось на 16-разрядную БЦВМ с обратной эндианностью, причем в среду другой операционной системы [6].

В настоящее время данная технология развивается для применения на третьей вычислительной платформе с RISC-архитектурой, а также в направлении внедрения электронного документооборота и интеграции на его основе средств разработки в единую среду разработки и сопровождения БПО. Технология зафиксирована в стандарте предприятия [7], который гармонизирован со стандартами Европейского Космического Агентства.

E-mail: kaa216@nppom.ru

СПИСОК ЛИТЕРАТУРЫ

1. *Колташев А.А.* Среда программирования для встроженных ЭВМ: система требований и тенденции ее развития / Сб. “Среда программирования: методы и инструменты”. – Новосибирск: ИСИ СО РАН, 1992.
2. *Князькин Ю.М., Колташев А.А.* Гарантии качества программного обеспечения встроженных ЭВМ / Материалы Межд. научно-техн. конф. “Проблемы обеспечения качества изделий в машиностроении”. – Красноярск: КГТУ, 1994.
3. *Колташев А.А.* Технология разработки и сопровождения мобильного программного обеспечения спутников связи // Изв. вузов. Приборостроение, 2004, № 4.
4. *Колташев А.А.* Технологические аспекты создания бортового программного обеспечения спутников связи / Вестник СибГАУ им. акад. М.Ф. Решетнева. Вып. 6. – Красноярск: СибГАУ, 2005.
5. *Koltashev Andrey.* A Practical Approach to Software Portability Based on Strong Typing and Architectural Stratification / Joint Modular Languages Conference, JMLC 2003, Klagenfurt, Austria, 2003. Proceedings Lecture Notes in Computer Science (LNCS 2789) Springer-Verlag, Berlin Heidelberg, New York, 2003.
6. *Колташев А.А.* Технология переноса бортового программного обеспечения // Открытые системы, 2004, № 4.
7. *СТП 154-123-2005.* Обеспечение бортовое программное. Управление проектированием, изготовлением и сопровождением. – Железногорск: НПО ПМ, 2005.

