

УДК 681.51:629.78

ББК 32.973.202

ПУТИ ПОВЫШЕНИЯ НАДЕЖНОСТИ И КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В КОСМИЧЕСКОЙ ОТРАСЛИ

Тюгашев А. А.¹

(ФГБОУ ВПО «Самарский государственный аэрокосмический университет им. академика С.П. Королева (Национальный исследовательский университет)», Самара)

Ильин И. А.²

(ЦНИИМАШ, Королев)

Ермаков И. Е.³

(НПО «Тесла», Орел)

Описывается текущая ситуация с созданием бортового программного обеспечения в аэрокосмической отрасли, описываются проблемы и намечаются пути их решения.

Ключевые слова: управляющее программное обеспечение, космический аппарат, верификация, тестирование программ.

1. Введение

В настоящее время в высокотехнологичных и наукоемких отраслях промышленности в нашей стране существует ряд серьезных проблем, среди которых – необходимость обновления основных фондов, оборудования и используемых технологий, проблема нехватки квалифицированных специалистов, особенно наиболее активного и продуктивного возраста – 30–50 лет, и т.д. Актуальной частной задачей при этом является повыше-

¹ Андрей Александрович Тюгашев, доктор технических наук, доцент (tau7@ssau.ru).

² Илья Александрович Ильин (ilyailyin@yandex.ru).

³ Илья Евгеньевич Ермаков (ilya@ertakov.net.ru).

ние надежности и качества космической техники, включая системы управления и их программное обеспечение [4].

2. Современное состояние в области создания программного обеспечения в космической отрасли

Как показывает практика, одной из главных причин аварий, потери дорогостоящих аппаратов, в которых воплощен труд многотысячных коллективов, являются сбои и ошибки функционирования систем управления. Часто к критическим последствиям приводят недостатки, ошибки и низкий уровень отказоустойчивости бортового программного обеспечения, на которое и возлагается в настоящее время, как правило, непосредственное решение задач управления. Рассматривая ситуацию через призму проблем в данной предметной области, можно отметить следующее. Еще в годы реализации программы «Аполлон» ее руководитель Дж. Ф. Ши отмечал [1]: «Хотя инженеры в любой области стремятся расценивать свои собственные разработки как наиболее ответственные, все же можно утверждать, что после создания необходимых ракетных двигателей основой надежного выполнения широких задач при длительных космических полетах являются вычислительные средства, имеющиеся на борту космического корабля». И сейчас [5] по многим оценкам, именно построение комплекса программного обеспечения – наземного и бортового, является зачастую критическим путем на сетевом графике работ по созданию современных аэрокосмических комплексов. Современному программному обеспечению свойство сложности присуще вообще, как неотъемлемая черта. Объем используемых программ достигает десятков миллионов строк исходного кода. Успешная и своевременная реализация проектов в сфере создания современного сложного программного обеспечения – весьма сложная проблема даже для опытных высококвалифицированных коллективов, вовсе не всегда успешно решаемая [6, 10, 12].

Еще более усложняется ситуация, когда речь идет об управляющих программах, функционирующих в режиме реального времени и от правильного функционирования которых напрямую зависит реализация важнейших миссий, безопасность, а иногда – человеческие жизни. К надежности подобного программного обеспечения, называемого критическим, предъявляются особо высокие требования. Именно такого рода программное обеспечение используется в аэрокосмической отрасли. К сожалению, ошибки в программах приводили и приводят к катастрофам и авариям.

Можно отметить следующие современные тенденции при создании систем управления космическими комплексами:

- реализация управления современными средствами выведения и космическими аппаратами с помощью бортовых цифровых вычислительных машин (БЦВМ) или комплекса БЦВМ – БВС (бортовой вычислительной системы);
- перенос «центра тяжести» в принятии решений с Земли на борт;
- возрастающий объем и сложность бортового программного обеспечения;
- необходимость согласованной работы большого числа приборов, устройств, функциональных программных модулей.

Наиболее широко на предприятиях отрасли применяется подход к обеспечению надежности, основанный на многоэтапной отладке и испытаниях управляющего программного обеспечения. Сначала проводится, как правило, автономная отладка, затем проверка функционирования управляющего программного обеспечения (ПО) во взаимодействии со специально созданными программными моделями бортовых систем и параметров движения летательного аппарата, и на заключительном этапе комплексной отладки – совместно с реальной БВС и бортовой аппаратурой [6, 7].

Несмотря на это, можно говорить о частном «кризисе» разработки ПО в космической отрасли. Трудоемкость, стоимость и сложность разработки ПО вносят значительный вклад в стои-

мость и сроки создания ракетно-космических комплексов в целом. Повторяющиеся ошибки в управляющем ПО приводят к потерям дорогостоящих аппаратов, утрате результатов длительного труда многотысячных коллективов, включая международные проекты. Существующие методы и технологии не позволяют гарантировать необходимый уровень надежности, отказоустойчивости и безопасности.

Говоря о причинах сложившейся ситуации, можно выделить следующие:

- зависимость от уникального опыта и квалификации конкретного разработчика;
- переход на новые вычислительные платформы (в том числе зарубежные);
- недопонимание между специалистами по бортовым системам, проектантами, программистами;
- большой объем программной документации, требующий актуализации наряду с ПО;
- противоречивость требований к управляющему ПО.

При этом следует сказать, что тестирование ПО не дает необходимых гарантий качества и надежности и не может дать их в принципе, что отмечалось еще классиками программирования [3]. Использование программных моделей бортовой аппаратуры (БА) на испытательных стендах в свою очередь требует верификации и ускорения разработки комплекса моделей. Часто одна и та же логика управления должна реализовываться на различных аппаратных и программных платформах.

Ясно, что нужна разработка и внедрение в аэрокосмической отрасли комплекса мер для преодоления сложившегося кризиса, качественного увеличения уровня надежности, безопасности и отказоустойчивости ПО, и на этой основе – отказоустойчивости и надежности ракетно-космических изделий в целом с соответствующим повышением вероятности успешного выполнения целевых задач.

3. Методы повышения надежности и качества программного обеспечения

На основании проведенного анализа, изучения отечественного и зарубежного опыта, современных достижений информатики и программирования, авторы выделяют следующие методы повышения качества и надежности ПО в отрасли:

- совершенствование процессов разработки ПО – обеспечение качества за счет использования современных методик, языков и инструментов;
- создание методик и языков для строгой, непротиворечивой и полной спецификации требований к ПО;
- автоматизация тестирования ПО с обеспечением требуемой полноты покрытия;
- автоматическая генерация фрагментов программ, заведомо соответствующих спецификации (для тех составляющих частей системы управления, где это возможно);
- формальные методы верификации со строгим доказательством свойств ПО;
- использование проверки моделей (*model checking*).

Кроме того, для решения проблемы своевременного создания комплекса бортового ПО и повышения производительности труда разработчиков целесообразна работа по следующим направлениям:

- использование современных методик, языков и инструментария;
- внедрение платформенно-независимого «промежуточного слоя» ПО;
- применение интуитивно понятных человеку визуальных представлений;
- автоматическая генерация фрагментов программ (где это возможно);
- автоматизация тестирования ПО;

- снижение зависимости от уникального опыта и квалификации конкретного разработчика за счет создания полной и качественной документации и использования проблемно-ориентированных языковых средств высокого уровня, удобных для человека.

Внедрение в жизнь перечисленных мер возможно путем разработки и внедрения на предприятиях аэрокосмической отрасли специализированных методик спецификации, проектирования, разработки, синтеза и верификации программного обеспечения, поддерживаемых специализированными инструментальными программными средствами. Набор подобных средств (индивидуально подбираемый на каждом предприятии в зависимости от специфики изготавливаемых изделий) должен создаваться со следующими главными целями:

- обеспечение необходимых показателей надежности, качества и безопасности ПО в отрасли;
- снижение сроков, стоимости и трудоемкости разработки управляющего ПО;
- снижение сроков, стоимости и трудоемкости разработки программных моделей БА, используемых при испытаниях;
- автоматизация построения актуальной, полной и точной программной документации.

Примером работ в направлении построения подобных средств автоматизации может служить программный комплекс ГРАФКОНТ/ГЕОЗ, созданный в Самарском государственном аэрокосмическом университете (национальном исследовательском университете), по заказу ГНПРКЦ «ЦСКБ-Прогресс» [5, 9]. Программный комплекс включает следующие основные модули и средства:

- транслятор с проблемно-ориентированного языка спецификаций управляющих алгоритмов реального времени;
- визуальный конструктор циклограмм управляющих алгоритмов;
- визуальный конструктор управляющей программы комплексного функционирования;

- генератор управляющей программы на языках ассемблер и Си (может параметрически настраиваться на другие языки программирования);
- генератор таблицы возможных вариантов исполнения управляющего алгоритма;
- генератор отладочных заданий для каждого варианта исполнения;
- генератор таблицы управляющих и информационных связей управляющей программы.

Среди других работ в данной области можно назвать технологию ГРАФИТ-ФЛОКС, используемую успешно в НПЦ АП им. Н.А. Пилюгина, на протяжении ряда лет, в том числе в проектах «Морской старт», РБ «Бриз-М», РБ «Фрегат» [2, 8]. Технология использует визуальный конструктор процедурной части управляющих программ ГРАФИТ и табличный процессор декларативной части ФЛОКС. Комплексную автоматизированную методику создания БПО внедряет в производственный процесс в настоящее время МОКБ «Марс».

Весьма значительных успехов в совершенствовании технологии создания управляющих программ для своих космических аппаратов достигло ОАО «ИСС», см. работы А.А. Колташева и В.В. Хартова [7, 11]. Важнейшими принципами при этом стали использование нескольких слоев программного обеспечения с выделением платформенно-независимого промежуточного слоя, использование и бортовых интеллектуальных интерпретаторов СЕАНС и ДКД, реализующих автономное управление КА. При написании бортовых программ используется язык Модуля-2 со строгой статической типизацией, жесткими нормами модульности и структурного программирования, позволяющие снизить количество ошибок в БПО.

В качестве направлений дальнейших работ в настоящее время целесообразным представляется следующее.

Первое направление связано с созданием теоретического и методологического фундамента для качественного совершенствования процессов разработки БПО за счёт внедрения и разви-

тия современных достижений науки и практики программной инженерии, таких как:

- высокоуровневые языки спецификаций, проектирования, моделирования, программирования, в том числе визуальные;
- формальные методы спецификации требований к ПО систем управления, верификации и валидации ПО, аттестации ПО на соответствие требованиям, гарантирующие качество ПО в противоположность традиционному тестированию;
- развитое технологическое ПО – инструменты автоматизации, поддерживающие ПО на всех этапах жизненного цикла.

Использование автоматизированных средств разработки ПО в отрасли даст возможность обеспечить гарантированный уровень качества ПО (его надёжности, отказоустойчивости и безопасности), снижение влияния человеческого фактора на качество ПО, автоматическую генерацию программной документации, автоматизацию генерации полного набора тестов с учетом внутренней структуры программ, технологичность и единообразие процессов создания ПО, сокращение сроков и трудозатрат.

Второе направление – это всемерное развитие и совершенствование нормативных основ в области процессов создания БПО в виде рекомендаций, требований, отраслевых стандартов. Подобного рода единый отраслевой нормативный базис призван обеспечить:

- единство основополагающей терминологии, определений и классификаций;
- использование на предприятии методологически проработанных подходов, моделей, инструментов при создании ПО;
- единую шкалу требований и критериев, определяющих качество процессов и технологий создания ПО и качество программной продукции;
- задание направлений совершенствования процессов и технологий разработки ПО в отрасли.

Примером успешно работающего аналога может служить международный стандарт DO-178 и его отечественная версия

ГОСТ Р 51904-2002 «Программное обеспечение встроенных систем. Общие требования к разработке и документированию», введенная в действие с июня 2002 года. Кстати, он поддерживается рядом инструментальных программных средств крупнейших производителей. Предусматривается сертификация процессов жизненного цикла БПО в авиации в соответствии с требованиями стандарта. Подобный же подход (несомненно, с весьма вдумчивым и постепенным его внедрением, со следованием принципу «не навреди»), как представляется, может быть применен и в космической отрасли. Можно привести еще пример «Стандарты кодированию на языке С++ при создании бортового ПО» истребителя пятого поколения F-35.

И, наконец, третьим направлением работ является создание, наполнение и развитие учебно-методической базы знаний в сфере создания БПО для обеспечения кадровой преемственности. Данная база знаний предназначена:

- для парирования кадровых проблем (естественный уход квалифицированных кадров старшего поколения и низкое качество подготовки молодых специалистов);
- для обеспечения необходимого уровня качества подготовки персонала и сокращения сроков такой подготовки;
- для аттестации персонала;
- для сохранения опыта, накопленного в отрасли за десятилетия (и предотвращения реальной угрозы его невосполнимой утраты) и пополнения этого опыта современными достижениями науки и практики;
- для обеспечения основы взаимодействия с системой высшего и специального образования.

Соответственно, можно выделить следующие виды работ по указанным направлениям:

- аналитическое – изучение отечественного и зарубежного опыта в области создания ПО в аэрокосмической отрасли, отслеживание перспективных тенденций и их оценка, изучение соответствующих процессов на предприятиях нашей страны;

- теоретическое – разработка формализованных методов и математических моделей, применимых на различных этапах жизненного цикла критического ПО;
- нормативное – разработка требований, рекомендаций и проектов стандартов, регламентирующих процессы разработки и этапы жизненного цикла БПО;
- технологическое – формулирование требований к средствам инструментального ПО их проектирование и разработка;
- информационно-методическое – создание электронной отраслевой базы знаний по теме разработки и использования ПО, планирование состава и содержания методического обеспечения подготовки специалистов соответствующего профиля для аэрокосмической отрасли.

Литература

1. *Авиастроение. Том 6.* (Итоги науки и техники, ВИНТИ АН СССР). – М., 1978.
2. БАЛТРУШАЙТИС В.В. «ГРАФИТ-ФЛОКС» – технология разработки программного обеспечения бортовых вычислительных машин // Тезисы докл. Межд. научно-техн. конф., посвященной 90-летию со дня рождения акад. Н.А. Пилюгина. – М.: НПЦ АП, 1998. – С. 79–81.
3. ДЕЙКСТРА Э.В. *Навстречу корректным программам.* – Grenoble: Mathematics Technological University, 1967.
4. ИЛЬИН И.А., ЕРМАКОВ И.Е., ТЮГАШЕВ А.А. *Создание единой отраслевой САПР ПО как основное условие предотвращения кризиса управляющего ПО в космической отрасли* // Актуальные проблемы российской космонавтики: Труды XXXVI Академических чтений по космонавтике, Москва, январь 2012 г. – С. 468.
5. КАЛЕНТЬЕВ А.А., ТЮГАШЕВ А.А. *ИП/СALS технологии в жизненном цикле комплексных программ управ-*

- ления. – Самара: Изд-во Самарского научного центра РАН, 2006.
6. КИРИЛИН А.Н., АХМЕТОВ Р.Н., СОЛЛОГУБ А.В., МАКАРОВ В.П. *Методы обеспечения живучести низкоорбитальных автоматических КА зондирования Земли: математические модели, компьютерные технологии.* – М.: Машиностроение, 2010. – 384 с.
 7. КОЛТАШЕВ А.А. *Эффективная технология управления циклом жизни бортового программного обеспечения спутников связи и навигации* // *Авиакосмическое приборостроение.* – 2006. – №12. – С. 20–25.
 8. ПАРОНДЖАНОВ В.Д. *Развитие системного обеспечения вычислительных комплексов при отработке систем управления ракет-носителей и космических аппаратов* / В кн.: XXII научные чтения по космонавтике, посвященные памяти академика С.П. Королева и других выдающихся отечественных ученых – пионеров освоения космического пространства. Тезисы докл. – М.: ИИЕТ РАН, 1998. – С.14–15.
 9. ТЮГАШЕВ А.А. *Интегрированная среда для проектирования управляющих алгоритмов реального времени* // *Известия российской академии наук: Теория и процессы управления.* – 2006. – №2. – С. 128–141.
 10. *Управление космическими аппаратами зондирования Земли: компьютерные технологии* / Д.И. Козлов, Г.П. Аншаков, Я.А. Мостовой, А.В. Соллогуб. – М.: Машиностроение, 1998. – 368 с.
 11. ХАРТОВ В. В. *Автономное управление космическими аппаратами связи, ретрансляции и навигации* // *Авиакосмическое приборостроение.* – 2006. – №6. – С. 29–33.
 12. BROOKSE F. *No Silver Bullet – Essence and Accident in Software Engineering* // *Proceedings of the IFIP 10th World*

Computing Conference, Dublin, Ireland, September 1-5,
1986. – P. 1069–1076.

WAYS TO IMPROVE QUALITY AND RELIABILITY OF SOFTWARE IN AEROSPACE INDUSTRY

Andrey Tyugashev, Samara State Aerospace University, professor
(tau7@ssau.ru).

Ilya Ilyin, TsNIIMASH (Korolyov, ilyailyin@yandex.ru).

Ilya Ermakov, NPO Tesla, Technical Director (ilya@ermakov.net.ru).

Abstract: The problem is considered of reliable control software development for Aerospace Industry. The state-of-the-art is described and possible ways to increase quality, reliability and safety of the critical software are proposed.

Keywords: control software, spacecraft, program verification, program testing.

*Статья представлена к публикации
членом редакционной коллегии М. В. Губко*