УДК 004.415:681.3

В.В.СКЛЯР[1], В.Б.ОСТРОУМОВ[2], Н.Ф.СИДОРЕНКО[2], В.С. ХАРЧЕНКО[1]

[1] *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2] *Научно-техническое специальное конструкторское бюро «Полисвит», Украина*

ТРЕБОВАНИЯ К РАЗРАБОТКЕ, ВЕРИФИКАЦИИ, СЕРТИФИКАЦИИ И СОПРОВОЖДЕНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ БОРТОВОЙ АВИАЦИОННОЙ ТЕХНИКИ: ОПЫТ СОЗДАНИЯ И ИСПОЛЬЗОВАНИЯ СТАНДАРТА ПРЕДПРИЯТИЯ

Изложен опыт разработки и использования стандарта предприятия СТП 522-120-2004, содержащего требования к разработке, верификации, сертификации и сопровождению программного обеспечения бортовой авиационной техники. Проведен обзор структуры и содержания данного стандарта. Сделан вывод о целесообразности выпуска на основе СТП 522-120-2004 отраслевого авиационного стандарта.

верификация, сертификация, программное обеспечение, бортовая авиационная техника

Введение

В научно-техническом специальном конструкторском бюро (НТ СКБ) «Полисвит» был разработан и используется стандарт предприятия СТП 522-120-2004 «Система программной документации. Порядок разработки, верификации, сертификации и сопровождения программного обеспечения бортовой техники». Этот стандарт создавался совместно со специалистами кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е.Жуковского «ХАИ», имеющими опыт в разработке отраслевых и государственных нормативно-технических документов и проведения экспертизы критического программного обеспечения объектов атомной энергетики и космических систем (в качестве экспертов государственных регулирующих органов).

Проблемы формирования требований к критическим компьютерным системам и программному обеспечению (ПО), а также общие вопросы стандартизации и обеспечения качества в программной инженерии исследуются в работах [1 – 11]. В них, в частности, анализируются:

– риски, связанные с использованием информационных технологий в целом и программного обеспечения, в частности, в компьютерных системах для критических приложений – атомной энергетики, аэрокосмической техники [1 – 3];

– методическое обеспечение решения задач систематизации и применения стандартов [3 – 6], профилирования и управления требованиями к ПО [7, 8];

– методы и средства оценки и обеспечения качества и надежности ПО, инструментальной поддержки верификации и экспертизы ПО [9 – 11].

Однако, в известных работах не рассмотрены вопросы, посвященные непосредственной разработке стандартов для промышленных предприятий. Кроме того, отсутствует анализ, позволяющий обобщить опыт стандартизации отдельных предприятий и распространить его для отрасли в целом.

Цель данной статьи:

– изложение опыта разработки стандарта СТП 522-120-2004, который может быть полезен специалистам в области нормативного регулирования компьютерных систем для аэрокосмических и других критических приложений;

– обзор структуры и содержания стандарта СТП 522-120-2004;

– анализ опыта использования стандарта на предприятии и целесообразности выпуска на его основе отраслевого авиационного стандарта, содержащего требования к разработке, верификации, сертификации и сопровождению ПО бортовой авиационной техники.

Анализ нормативных документов в области программной инженерии для критических приложений

Необходимость верификации для ПО критических приложений установлена в различных нормативно-технических документах [11 – 14]. В качестве примеров стандартов, регламентирующих процессы разработки и верификации критического ПО, могут быть приведены [3]:

– для АЭС – стандарты МАГАТЭ (Международного агентства атомной энергии), в частности, стандарт NS-G-1.1 (2000) «Программное обеспечение для компьютерных систем, важных для безопасности АЭС. Руководство по безопасности»;

– для ракетно-космической техники – стандарты ECSS (European Cooperation for Space Standardization – Европейской кооперации по космической стандартизации), в частности, стандарт ECSS-E-10-02A (1998) «Разработка космических систем – Верификация»;

– для авиационной техники – стандарты RTCA (Radio Technical Commission for Aeronautics – Радиотехнической комиссии по аэронавтике), в частности, стандарт DO-178 «Рассмотрение программного обеспечения при сертификации бортовых систем и оборудования».

Проведенный анализ позволил сделать следующие выводы. Указанные стандарты ориентированы на так называемый процессный подход к изложению требований, при котором требования к программному продукту декомпозируются по процессам жизненного цикла (ЖЦ). Это связано с тем, что все они в части структуры ЖЦ ПО базируются на положениях стандарта ИСО/МЭК 12207:1995 «Информационные технологии – Процессы жизненного цикла программного обеспечения», который является основополагающим в области программной инженерии (см. табл. 1). Следует отметить, что стандарт ИСО/МЭК 12207:1995 адаптирован в качестве государственного стандарта Украины ДСТУ 3918-1999. Кроме того, во всех указанных стандартах подчеркивается важность выполнения процедур верификации на всех этапах ЖЦ ПО. Под верификацией подразумевается процесс, направленный на подтверждение соответствия ПО заданным требованиям путем различного рода проверок и обеспечения объективных доказательств.

Анализ исходных данных для разработки

При разработке СТП 522-120-2004 учитывались результаты:

– проведенного исследования содержания документов национальной и международной нормативной базы в области критической программной инженерии (информационно-управляющих систем АЭС, бортовых и наземных вычислительных комплексов и др.), созданной и динамично развиваемой международными организациями ИСО (Международная организация по стандартизации), МЭК, МАГАТЭ, ECSS;

– анализа действующего в Украине и СНГ авиационного стандарта КТ-178А «Квалификационные требования. Требования к программному обеспечению бортовой аппаратуры и систем при сертификации авиационной техники», который представляет собой переведенный и адаптированный стандарт RTCA DO-178A;

– обобщения многолетнего опыта коллектива предприятия и разработчиков стандарта в области разработки и верификации систем, аппаратуры и ПО при сертификации авиационной техники, а также опыта оценки систем и программного обеспечения для критических приложений. Принятый подход к разработке СТП 522-120-2004 включал следующую последовательность действий:

– критический анализ положений стандарта КТ-178А;

– адаптация положений стандарта КТ-178А с учетом специфики НТ СКБ «Полисвит»;

– разработка положений СТП 522-120-2004, отсутствующих в стандарте КТ-178А;

– проведение независимого аудита содержания СТП 522-120-2004.

Таблица 1

Процессы жизненного цикла программного обеспечения согласно стандарту ДСТУ 3918-1999

Основные процессы жизненного цикла	**Процессы поддержки жизненного цикла**	**Организационные процессы жизненного цикла**
Процесс заказа	Процесс документирования	Процесс управления
Процесс поставки	Процесс конфигурационного управления	Процесс создания и сопровождения инфраструктуры
Процесс разработки	Процесс обеспечения качества	Процесс усовершенствования
Процесс эксплуатации	Процесс верификации	Процесс обучения
Процесс сопровождения	Процесс валидации	
	Процесс совместного обзора	
	Процесс аудита	
	Процесс решения проблем	

Последнее из действий выполнялось силами специалистов кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е.Жуковского «ХАИ».

Проведение независимого аудита позволило повысить качество СТП 522-120-2004 и учесть при его разработке опыт нормативного регулирования в других критических отраслях, таких как атомная энергетика и ракетно-космическая техника [15 – 18].

Структура и содержание стандарта СТП 522-120-2004

Для разработки СТП 522-120-2004 структура ЖЦ ПО бортовой техники была уточнена с учетом рекомендации КТ-178А. На рис. 1 изображена общая модель ЖЦ ПО бортовой техники с указанием номеров соответствующих разделов СТП 522-120-2004. Выбранная структура ЖЦ ПО является основой для структуры стандарта. В табл. 2 приведена детализированная структура жизненного цикла ПО бортовой техники, которая уточнена путем указания действий для соответствующих процессов ЖЦ и ссылок на разделы СТП, КТ-178А и ДСТУ 3918.

Табл. 2 включает содержание СТП 522-120-2004 в части процессов ЖЦ ПО. Названия процессов и действий ЖЦ ПО являются названиями разделов и подразделов СТП 522-120-2004. Кроме того, СТП 522-120-2004 включает следующие общие разделы: 1. Область применения; 2. Нормативные ссылки; 3. Перечень принятых сокращений; 4. Термины и определения; 5. Общие положения.

СТП 522-120-2004 содержит следующие приложения: Приложение А. Рекомендуемое содержание работ к графику создания ПО бортовой техники; Приложение Б. Процедуры верификации ПО; Приложение В. Формы отчетных документов по верификации ПО.

Опыт использования стандарта на предприятии

В течение 2005-2007 годов стандарт предприятия СТП 522-120-2004 проходил опытную эксплуатацию в НТ СКБ «Полисвит», после которой был введен в действие как постоянный.

Проведенный анализ показал, что, несмотря на специализированность, характерную для стандартов предприятий, СТП 522-120-2004 (см. табл. 2) превосходит исходный стандарт КТ-178А по ряду критериев, таких как структурированность, логичность, полнота, непротиворечивость, ясность. Следует подчеркнуть, что в разработанном стандарте учтен передовой опыт, аккумулированный в последних стандартах по программной инженерии.

Заключение. Направление дальнейших работ

Результаты проведенных работ и опыта применения позволили сделать вывод о целесообразности выпуска на основе СТП 522-120-2004 отраслевого стандарта.

Для этого должны быть выполнены следующие работы и учтен ряд обстоятельств:

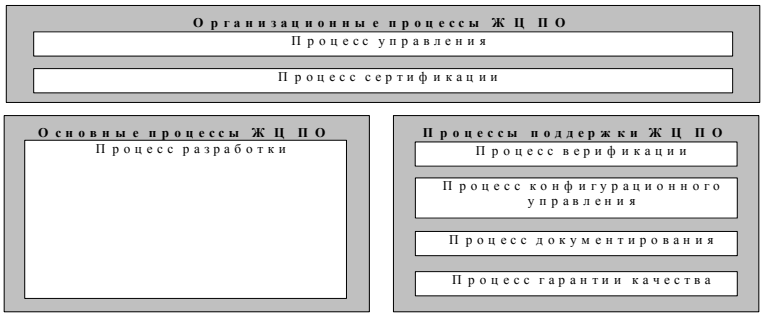

Рис. 1. Общая модель жизненного цикла программного обеспечения бортовой техники

Таблица 2

Детализированная структура жизненного цикла программного обеспечения бортовой техники

Процессы ЖЦ ПО	**Действия процессов ЖЦ ПО**	**Раздел СТП 522-120-2004**	**Раздел КТ-178А**	**Раздел ДСТУ 3918**
6. Процесс управления разработкой ПО	Общие положения	6.1	5	7.1.2
	Планирование разработки ПО	6.2	–	–
	Планирование верификации ПО	6.3	–	–
	Планирование управления конфигурацией ПО	6.4	–	–
	Планирование гарантии качества ПО	6.5	–	–
	Планирование сертификации ПО	6.6	–	–
7. Процесс разработки	Этап «Требования»	7.1	6.2.2.1	5.3.4
	Этап «Проектирование»	7.2	6.2.3.1	5.3.5, 5.3.6
	Этап «Программирования»	7.3	6.2.4.1	5.3.7
	Этап «Испытания»	7.4	6.1, 6.2.5.2.2, 6.2.5.2.3	5.3.8
	Этап «Завершение»	7.5	6.1	5.3.10
	Этап «Сопровождение»	7.6	6.4	5.5
8. Процесс верификации	Общие положения	8.1	–	6.4
	Проверка требований к ПО	8.2	6.2.2.2	6.4
	Проверка проекта ПО	8.3	6.2.3.2	6.4
	Проверка программных модулей ПО	8.4	6.2.4.2	6.4
	Определение требований к испытаниям	8.5	6.2.5.1	6.4
	Испытания программных модулей	8.6	6.2.5.2.1	5.3.7
	Испытания интегрированного ПО	8.7	6.2.5.2.2	5.3.9
	Испытания интеграции ПО и аппаратных средств	8.8	6.2.5.2.3	5.3.11
	Удостоверение эксплуатационной пригодности ПО	8.9	5.5	6.5
	Повторная верификация ПО	8.10	5.6, 6.2.7, 6.4	6.4
	Верификация инструментальных средств	8.11	6.2.8	6.4
9. Процесс управления конфигурацией ПО	Общие положения	9.1	7.1, 7.2.7	6.2
	Управление конфигурацией ПО на уровне одобренных версий	9.2	7.2.4	
	Учет состояния конфигурации ПО	9.3	–	–
	Порядок внесения изменений в одобренную версию	9.4	–	–
	Контроль носителей	9.5	7.2.5	–
	Контроль за вносимыми изменениями в рабочие версии программных документов	9.6	–	–
	Требования по обозримости связей по отношению к предыдущей базовой версии	9.7	–	–
	Контроль загрузки исполняемой программы в память	9.8	–	–

Процессы ЖЦ ПО	Действия процессов ЖЦ ПО	Раздел СТП 522-120-2004	Раздел КТ-178А	Раздел ДСТУ 3918
	Документы, регламентирующие деятельность группы управления конфигурацией ПО	9.9	7.2.1, 7.2.2	–
	Маркировка	9.10	7.2.3	–
	Аудиторские проверки конфигурации ПО	9.11	7.2.6	–
10. Процесс документирования	Общие положения	10.1	8.2	6.1
	Требования к содержанию и оформлению документов	10.2	8.1	–
	Историческая документация	10.3	–	–
11. Процесс гарантии качества	Общие положения	11.1	–	6.3
	Гарантии качества верификации	11.2	6.2.2.3, 6.2.3.3, 6.2.4.3, 6.2.5.3	6.3
	Гарантии качества управления конфигурацией ПО	11.3	7.2.6	6.3
	Инспекционные проверки (совместные обзоры)	11.4	–	6.6
	Аудит	11.5	–	6.7
	Решение проблем	11.6	–	6.8
	Обучение персонала	11.7	–	7.4
12. Процесс сертификации ПО	Общие положения	12.1	8.2	–
	Мероприятия, выполняемые для обеспечения сертификации ПО	12.2	8.2	–
	Работы по сертификации ПО КИ АТ категории Б	12.3	8.2	–
	Работы по сертификации ПО КИ АТ категории А	12.4	8.2	–

– СТП 522-120-2004 был разработан на основе стандарта КТ-178А, который представляет собой перевод устаревшей версии стандарта RTCA DO-178A. В настоящее время действующим является стандарт DO-178B (1992) "Software Considerations in Airborne Systems and Equipment Certification" ("Рассмотрение программного обеспечения при сертификации бортовых систем и оборудования"). Кроме того, в 2001 г. RTCA был выпущен документ DO-248B "Final Annual Report for Clarification of DO-178B Software Considerations in Airborne Systems and Equipment Certification"" (Отчет по разъяснению стандарта DO-178B), в котором учтен опыт применения DO-178B. Таким образом, при адаптации СТП 522-120-2004 в качестве отраслевого стандарта должны быть учтены положения нормативных документов RTCA DO-178B и DO-248B. Следовательно, целесообразно принять к сведению это обстоятельство и гармонизировать положения последних версий рассматриваемых нормативных документов для реальных условий Украины и перспектив развития ее авиационной отрасли;

– часть положений СТП 522-120-2004 отражает специфику предприятия и потому должна быть либо исключена, либо доработана;

– необходимо дополнительно проанализировать и обобщить позитивный опыт нормативного регулирования в области критического ПО в других областях, поскольку вопросы, связанные с применением информационных технологий и минимизацией рисков аварий по причинам дефектов ПО, имеют много общего как в части регулирующих требований, так и методов оценки и обеспечения их выполнения, что может быть, безусловно, полезно для авиационных приложений [11 – 13, 18].

Разработка и внедрение отраслевого стандарта для авиационных систем позволят не только продвинуть в нормативном плане современные индустриальные технологии проектирования, верификации и сертификации ПО, но и повысить, в конечном счете, надежность и безопасность авиационной техники.

Литература

1. Ястребенецкий М.А., Васильченко В.Н., Харченко В.С. Безопасность атомных станций: Информационные и управляющие системы. – К.: Техніка, 2004. – 472 с.

2. Харченко В.С., Ястребенецкий М.А., Скляр В.В. Новые информационные технологии и безопасность ИУС АЭС // Ядерная и радиационная безопасность. - 2003. – Т. 6, № 2. – С. 19-28.

3. Конорев Б.М. и др. Нормативная база программной инженерии в разработке систем с интенсивным использованием ПО. – Х.: ХАИ, 2001.– 162 с.

4. Смит Д., Симпсон К. Функциональная безопасность. Руководство по применению стандарта МЭК 61508. – М.: Издательский Дом «Технологии», 2004. – 208 с.

5. Moore J. Software Engineering Standards. A User's Map. – Los Alamos, CA, USA: IEEE Computer Society, 1998.

6. Johnson G. Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety // Proceedings of CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-based I&C Systems. – Hluboka nad Vltavou (Czech Republic). – 2001. – P. 109-115.

7. Скляр В.В. Стандарты в области критических информационных технологий и программной инженерии: Систематизация, профилирование, гармонизация требований // Радіоелектронні і комп'ютерні системи. – 2003. – Вип. 1. – С. 78-85.

8. Леффингуэлл Д., Уидриг Д. Принципы работы с требованиями к ПО. Унифицированный подход. – М.: Вильямс, 2002. – 448 с.

9. Липаев В.В. Обеспечения качества программных средств. Методы и стандарты. – М.: СИНТЕГ, 2001. – 380 с.

10. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. – Х.: ХАИ, 2004. – 159 с.

11. Конорев Б.М., Харченко В.С., Чертков Г.Н. Концепция и принципы реализации интегрированной инструментальной системы для поддержки экспертизы и независимой верификации критического программного обеспечения (SAVExpert-System). – Государственный комитет ядерного регулирования Украины, 2003. – 60 с.

12. НП 306.5.02/3.035-2000. Нормы и правила по ядерной и радиационной безопасности. Требования по ядерной и радиационной безопасности к ИУС АЭС. – К.: Государственная администрация ядерного регулирования Украины, 2000. – 80 с.

13. ГНД 306.7.02/2.041-2000. Методика соответствия информационных и управляющих систем, важных для безопасности атомных станций, требованиям по ядерной и радиационной безопасности. – К.: Министерство экологии и природных ресурсов Украины, 2000. – 46 с.

14. Харченко В.С., Тарасюк О.М., Скляр В.В. О метрическом подходе к оценке качества и надежности программного обеспечения // Системи обробки інформації. – Х.: НАНУ, ПАНМ, ХВУ, 2002. – Вип. 6 (22). – С. 342-345.

15. Laprie J.-C. Dependability Handbook. LAAS Report n 98-346. – Toulouse: Laboratory for Dependability Engineering, 1998. – 365 p.

16. Lyu M.R. Handbook of Software Reliability Engineering. – McGraw-Hill Company, 1996. – 805 p.

17. Скляр В.В. Оценка CASE-инструментов с использованием иерархической модели характеристик // Збірник наукових праць ІПМЕ ім. Г.Є. Пухова. – К.: ІПМЕ НАНУ, 2003. – Вип. 22. – С. 183-187.

18. Харченко В.С., Скляр В.В., Ястребенецкий М.А. Экспертная оценка безопасности OTS компонент информационных и управляющих систем АЭС // Інформаційні технології в енергетиці: Збірник наукових праць ІПМЕ ім. Г.Є. Пухова. – К.: ІПМЕ НАНУ, 2003. – С. 12-19.

Поступила в редакцию 31.10.2007

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.