УДК 656.7

АНАЛИЗ НЕШТАТНЫХ СИТУАЦИЙ И КРИТИЧНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ В ПРОЕКТЕ МЕЖДУНАРОДНОЙ КОСМИЧЕСКОЙ СТАНЦИИ

Е.А. Микрин*, В.П. Пелихов**

*Ракетно-космическая корпорация «Энергия», г. Королев

**Институт проблем управления им. В.А. Трапезникова, г. Москва

Дана классификация основных типов нештатных ситуаций, возникающих при функционировании долговременной орбитальной станции. Описаны основные характеристики критических функций, выполняемых автоматикой и программным обеспечением станции. Приведена классификация программного обеспечения по категориям опасности.

ВВЕДЕНИЕ

Безопасность космического полета долговременной орбитальной станции (ДОС) обеспечивается организацией работ по следующим направлениям:

- достижение при создании модулей ДОС и поддержание в процессе их эксплуатации требуемого уровня надежности функционирования бортовых систем;
- сведение риска возникновения возможных опасностей к приемлемому уровню мероприятиями по их предупреждению, парированию и локализации;
- анализ расчетных нештатных ситуаций (НШС) модулей и ДОС в целом, а также выбор способов выхода из них.

В основу решения проблемы обеспечения приемлемого уровня риска возникновения возможных опасностей положен принцип анализа функциональных возможностей и конструкции в целом на устойчивость к проявлению возможных опасностей, связанных с угрозой здоровью и жизни экипажа, с угрозой утраты одного из модулей ДОС, транспортного корабля или всей станции в целом. Перечень таких опасностей определяется в результате исследования программы функционирования от момента запуска до завершения существования станции на орбите.

ОПРЕДЕЛЕНИЕ И КЛАССИФИКАЦИЯ НЕШТАТНЫХ СИТУАЦИЙ

Нештатная ситуация – это состояние космического комплекса, его составных частей и привлекаемых средств, а также условий полета, непредусмотренное программой штатного функционирования, или отклонение состояния здоровья космонавтов от нормального. В качестве причин возникновения НШС могут рассматриваться отказы в бортовых системах и агрегатах, изменение условий эксплуатации и ошибки экипажа или наземного персонала управления, которые приводят к невыполнению функций бортовыми системами или к изменениям характеристик их функционирования, выходящими за допустимые пределы.

Рассмотренные НШС (см. рисунок) – это нештатные ситуации в космическом полете, которые были выявлены и рассмотрены в процессе создания космического комплекса и предполетного анализа и внесены в конструкторскую документацию.

Нерассмотренные НШС – это нештатные ситуации, анализ которых не мог быть проведен в предполетный период и которые не содержатся в конструкторской документации.

Расчетные НШС – это нештатные ситуации в космическом полете, способы и средства выхода из которых предусмотрены и внесены в конструкторскую документацию.

Нерасчетные НШС – это нештатные ситуации, причиной возникновения которых являются отказы, приводящие к нерасчетным или неопределенным условиям эксплуатации. Выходы из таких

Классификация нештатных ситуаций

НШС не гарантируются с помощью разработанных способов и средств, но для них могут быть предусмотрены мероприятия, снижающие риск и повышающие вероятность выполнения задач полета.

Аварийные ситуации (АС) – это нештатные ситуации, приводящие к полному или частичному разрушению, выходу из строя хотя бы одной из составных частей космического комплекса, а также к угрозе жизни или ухудшению здоровья хотя бы одного из членов экипажа.

ОСНОВНЫЕ ПОЛОЖЕНИЯ, ПРИНЯТЫЕ ПРИ РАЗРАБОТКЕ ПЕРЕЧНЯ НШС

По каждой опасности оформляется отчет по форме NASA, который представляется в Комиссию NASA по безопасности полета для защиты на соответствие установленным требованиям. В состав отчета включаются мероприятия по предупреждению опасностей, их парированию и локализации, а также данные по верификации этих мероприятий. Работы по анализу нештатных ситуаций выполняются в соответствии с нормативной документацией и государственными стандартами Российской Федерации.

Анализ НШС осуществляется для различных уровней структуры ДОС (отдельный агрегат, бортовая система, блок). Для этого используются возможности различных алгоритмов управления функционированием и полетом ДОС: от конкретных циклограмм, формализующих порядок функционирования отдельных агрегатов и систем, до алгоритмов верхнего уровня управления – алгоритмов программы полета ДОС.

Анализ возможных отказов и нештатных ситуаций осуществляется в рамках кооперации смежников по принадлежности. Результаты такого анализа и мероприятия, связанные с предупреждением, парированием и локализацией возможных отказов, НШС и их последствий, отражаются в соответствующей документации.

Возможные отказы и НШС, последствия которых не выходят за пределы отдельной бортовой системы, анализируются разработчиком данной системы. Результаты такого анализа отражаются соответствующими смежниками в их конструкторской документации на систему. Парирование возможных отказов и НШС рассматриваемого уровня осуществляется для всех этапов полета внутри циклограмм и алгоритмов функционирования агрегатов и систем с помощью встроенной автоматики или конечных исполнителей программно-математического обеспечения бортовых вычислительных средств.

ОСНОВНЫЕ ПОЛОЖЕНИЯ МЕТОДИКИ АНАЛИЗА НШС

Нештатные ситуации выявляются по результатам построения моделей их развития и анализа возможных опасностей, отказов, потерь функций бортовых систем и ошибок операторов. Цель анализа НШС состоит в определении возможных последствий, методов идентификации и мероприятий по выходу из таких ситуаций.

Выходы из НШС могут осуществляться либо автоматически, либо по управляющим воздействиям наземного комплекса управления (НКУ), либо экипажем посредством ручных органов управления бортовыми системами, а также при выполнении ремонта бортовых систем и конструкций.

Анализ НШС и их отбор для рассмотрения производятся по следующим критериям:

- влияние на выполнение программы полета;
- влияние на работоспособность модулей ДОС;
- необходимость ремонтных работ, выполняемых космонавтами.

Нештатные ситуации рассматриваются для всех типов полета. В ряде случаев НШС анализируются для фиксированного момента, когда возможность их проявления связана с работой системы или агрегата в этот момент.

Результаты анализа расчетных и нерасчетных НШС, а также АС представляются в форме таблиц, содержащих следующие сведения:

- наименование НШС, которое должно содержать физический смысл ситуации с привязкой к потере или угрозе потери функции;
- причина возникновения НШС и модель ее развития;
- участок, на котором рассматривается возникновение НШС;
- средства идентификации НШС (автоматика, бортовой комплекс управления, НКУ); приоритетное средство идентификации указывается первым;
- последствия НШС, в качестве которых указываются возможные состояния бортовых систем ДОС при неприятии мер по выходу из НШС;
- мероприятия по выходу из НШС, включающие в себя действия бортовой автоматики, НКУ и экипажа;
- примечания, в которых дается дополнительная информация.

Обобщенный перечень НШС включает в себя перечни расчетных и нерасчетных НШС, а также АС для различных участков полета.

АНАЛИЗ КРИТИЧНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Причины и обстоятельства, приводящие к появлению НШС, порождают множество критических функций, связанных с программным обеспечением (ПО) [1, 2].

Анализ критичности ПО бортовой вычислительной системы (БВС) должен проводиться с учетом предварительной оценки архитектуры ПО и размещения его по вычислительным средствам

Классификация программного обеспечения по категориям опасности

Категория ПО	Определение
A	• Программное обеспечение, повреждение которого может привести к катастрофическим последствиям, когда никакие адекватные средства вмешательства, имеющиеся в системе, и никакое время недостаточны, чтобы эффективно вмешаться для предотвращения последствий события
B	• Программное обеспечение, повреждение которого может привести к катастрофическим последствиям, но в системе есть адекватные средства вмешательства и имеется достаточно времени для эффективного вмешательства. • Программное обеспечение, повреждение которого может привести к критическим последствиям, когда никакие адекватные средства вмешательства, имеющиеся в системе, и никакое время недостаточны, чтобы эффективно вмешаться для предотвращения последствий события
C	• Другое бортовое ПО, повреждение которого может привести к: – критическим последствиям, и в системе имеются адекватные средства вмешательства для предотвращения последствий события; – потере системы, и в системе имеются адекватные средства вмешательства для предотвращения последствий события; – невыполнению задания полета. • Все другое наземное ПО, которое функционирует вместе с бортовым ПО, летной материальной частью или которое используется для генерации бортового ПО
D	• Все другое наземное ПО

БВС в соответствии с техническими спецификациями на ПО.

На основании технических спецификаций на интегрированное ПО и анализа реализуемости маневра ДОС осуществляется декомпозиция интегрированных функций и их размещение по компьютерам БВС.

Далее на основании предварительной оценки архитектуры программного обеспечения БВС осуществляется декомпозиция элементов конфигурации ПО на программные компоненты, реализующие те или иные критические функции во времени. Составляются соответствующие матрицы участия каждого программного компонента в реализации критических функций. В результате такого анализа выявляются программные компоненты, участвующие в реализации критических функций.

Выделяют следующие категории опасности.

Катастрофическая:

– гибель людей, угроза их жизни, ранения, приводящие к инвалидности, или временная профессиональная болезнь;

– потенциальная потеря модуля ДОС;

– потеря государственной или частной собственности.

Критическая:

– временный ущерб, не угрожающий жизни, или временная профессиональная болезнь;

– значительное повреждение модуля ДОС;

– потеря или значительное повреждение государственной или частной собственности;

– длительное, вредное влияние на окружающую среду.

В соответствии с техническими требованиями Европейского космического агентства принята классификация ПО по категориям опасности (см. выше).

Результаты проведенного анализа, с учетом принципа максимальной критичности, показывают, что программные компоненты, размещаемые на компьютерах БВС, должны иметь достаточно высокие категории – классов B и C. Проектирование интегрированного программного обеспечения БВС должно отвечать соответствующим требованиям обеспечения качества программного продукта. Данным требованиям должны отвечать все аспекты проектирования ПО на всех его стадиях, от разработки технических спецификаций до его валидации (проверке правильности) и верификации.

Отработочные, интеграционные и верификационные испытания на наземном комплексе отработки должны включать в себя моделирование как номинального полета, так и НШС в односторонних и совместных испытаниях, а также проверку правильности взаимодействия с реальными данными на односторонних и совместных тестах. Особое внимание следует обратить на отработку взаимодействия ПО и системных функций в НШС, моделирующих отказы тех или иных программных компонентов.

В заключение отметим, что применение формализованных методов анализа НШС представляется перспективным направлением исследований процессов возникновения и распространения НШС и способов их предупреждения.

ЛИТЕРАТУРА

1. *Микрин Е.А., Пелихов В.П.* Оценивание риска элементов программного обеспечения как фактор управления безопасностью функционирования долговременных орбитальных станций // Междунар. конф. по пробл. упр. (29 июня–2 июля 1999 г.) / Ин-т пробл. упр.: Тез. докл. М., 1999.
2. *Микрин Е.А.* Управление производством программно-математического обеспечения при реализации проекта МКС «Альфа» // Междунар. научн.-практ. конф. «Теория активных систем» (15–17 ноября 1999 г.) / Ин-т пробл. упр.: Тез. докл. М., 1999.

☎ *(095) 334-90-09*

E-mail: kulba@ipu.rssi.ru

❑