УДК 004.056

НЕКОТОРЫЕ ВОПРОСЫ ТЕХНОЛОГИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ УСТОЙЧИВОСТИ СЛОЖНЫХ СИСТЕМ

© 2004 Г. П. Аншаков, Ю. Г. Антонов, Я. А. Мостовой, А. В. Соллогуб

Государственный научно-производственный ракетно-космический центр «ЦСКБ-Прогресс»

Рассматриваются вопросы технологической защиты информации и программного обеспечения сложных технических систем.

Излагаются методы и механизмы сохранения работоспособности сложной системы при отказах и технология реализации ее работоспособности.

Введение. Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений. Тогда защита информации – комплекс мер, направленных на обеспечение информационной безопасности.

При этом термин «информационная безопасность» подразумевает наличие моделей угроз вычислительной системе, ее программному обеспечению (ПО) и данным и соответствующих моделей защиты.

Безопасность вычислительной системы, ПО и данных не может обеспечиваться повсеместно и в любых условиях, то есть «среда безопасности» определяет ограничения на область безопасности в рамках принятых моделей угроз и защиты от них.

Защита информации не сводится исключительно к защите от несанкционированного доступа к информации. Субъекты информационных отношений могут нести ущерб и от прекращения функционирования соответствующих систем в результате отказов и ошибок, что в лучшем случае будет приводить к перерывам в работе.

Необходимо рассматривать пять составляющих среды безопасности:

1. Физическая безопасность, связанная с моделями физических воздействий на систему: пожары, отключение питания, электромагнитные воздействия и т. п.

2. Безопасность персонала, связанная с моделями воздействия на персонал и персонала на систему.

3. Безопасность от информационных вторжений.

4. Правовая безопасность.

5. Безопасность функционирования системы, связанная с надежностью и живучестью оборудования системы и ПО, с моделями ошибок, «готовностью» оборудования и ПО и т. п.

Защита от физических воздействий – сооружения, охрана, электронные и механические замки, источники бесперебойного питания и т. п.

Защита от персонала – подбор качеств сотрудников, разграничение участков работы, доступа и осведомленности; технологическая защита.

Защита от информационных вторжений – технологическая защита, антивирусная защита, ограничение доступа и т. п.

Обеспечение надежности и живучести оборудования системы и ПО связаны с резервированием и избыточностью, с алгоритмическим резервированием, с тщательно проведенной отладкой ПО, с «аварийной защитой» системы и ПО, сетевыми фильтрами и т.п.

В настоящей статье рассмотрены вопросы технологической защиты информации и ПО сложных технических систем в процессе их разработки, а также задачи защиты информации при обеспечении отказо- и сбоеустойчивости систем – задачи информационной устойчивости и «аварийной защиты» сложных технических систем в процессе эксплуатации.

Данные задачи решались при разработке программного обеспечения систем управ-

ления космическими аппаратами (КА). Однако аналогичные задачи и рассмотренные методы их решения возникают при разработке сложных систем более общего вида.

1. Технологическая защита ПО. Задачи технологической защиты возникают при работе в средах разработки ПО, а затем при передаче информации по цепочке технологического цикла разработки ПО. Компоненты комплекса ПО в процессе коллективной разработки находятся в инструментальных средствах и принципиально должны быть доступны для внесения изменений разработчиками. Однако это делает возможным внесение в ПО и данные несанкционированных изменений (ошибочных или злоумышленных). Особенность ситуации технологической защиты заключается в том, что эти несанкционированные изменения могут проводиться со стороны легальных пользователей.

Поток несанкционированных изменений очень быстро приводит в неработоспособное состояние даже исходно работающий программный комплекс.

Технологическая защита должна обеспечить:

1. Сохранение целостности информации – ее защиту от нарушения и несанкционированных изменений.

2. Сохранение конфиденциальности информации – ее защиту от несанкционированного ознакомления.

3. Доступность информации – возможность для быстрого и санкционированного ее изменения в оговоренное технологическое время.

4. Предотвращение несанкционированного использования (кражи) ресурсов системы и ресурсов технологических средств разработки.

Методы и механизмы обеспечения сохранения целостности и конфиденциальности информации должны обеспечить защиту от следующих непреднамеренных и преднамеренных угроз в процессе разработки ПО:

1. Ошибок адресации при записи и передачи информации в комплексе инструментальных средств разработки.

2. Ошибок в информации при ее передаче и записи в комплексе инструментальных средств разработки.

3. «Вандализма» – разрушения системы ПО или данных вследствие информационных атак или ошибок.

4. «Утечек» информации – несанкционированного прочтения и копирования информации лицами, не имеющими на это разрешение и права, в том числе путем «подслушивания».

5. «Подмены» информации – несанкционированного изменения информации методами:

- «маскарада» – попыткой выдать себя за другого с целью обхода защиты и получения несанкционированного доступа к ПО и данным;

- «манипуляции» – несанкционированного изменения, вставки, удаления или переупорядочивания ПО и данных;

- «дезорганизации» – несанкционированного изменения адресной части информации в сообщениях;

- «передачи ложных сообщений» в сети инструментальных средств;

- «воспроизведения» несанкционированного перехвата сообщения, запоминания его и воспроизведения, как правило, несколько раз без изменений и проникновения в его смысл, что будет заставлять получателя в сети инструментальных средств многократно получать правильные данные или команды, что увеличивает трафик и может препятствовать нормальной работе сети.

Следует отметить, что «утечки» информации приводят к нарушению конфиденциальности и прибыли; «подмены» информации опасны целенаправленным искажением данных, например, в банковских счетах; «манипуляция» приводит к утрате достоверности и целостности ПО и данных; кража ресурсов приводит к несанкционированному использованию каналов связи и времени процессора.

Наиболее опасным субъектом угроз при разработке ПО является все-таки легальный пользователь, допущенный к ресурсам системы. В этом случае концентрация усилий защиты на предотвращение проникновения в систему (ограничений доступа) не приводит к ожидаемому эффекту.

Технологическая защита ПО от легального пользователя должна строиться по принципам:

1. Минимизация права доступа к информации и ПО с учетом целей этого доступа только в рамках выделенных ресурсов.

2. Контроль действий пользователя на предмет превышения им своих полномочий с обеспечением невозможности отказа пользователя от произведенных действий.

3. Отчуждение подлинника ПО на этапе интегрирования ПО – сборки его в программный комплекс.

При этом, если от угроз «утечек», «подмены» можно защититься методами ограничения доступа, технологической защитой, введением «запросов» разрешительной информации по паролям, шифрованием и т. п., то от ошибок адресации в сети инструментальных средств можно защищаться путем составления ограничительных (разрешительных) каталогов справочной информации, на соответствие с которым должна проверяться любая попытка записи информации.

Угрозы «утечки» и «подмены» информации (ПО и данных) имеют место не только при разработке сложных систем, но и при их эксплуатации.

Технологической защитой от угрозы «подмены» методом «воспроизведения» может быть организация временного стробирования передачи сообщений, счетчиков сообщений с одинаковыми атрибутами, контролем трафика и сравнением его с ожидаемым.

Одним из основных методов технологической защиты ПО и данных от несанкционированных изменений в процессе разработки ПО является принцип «отчуждения подлинника» от разработчика ПО.

В этом случае вводится служба «архива подлинников», в которой документы ПО, объявленные подлинниками, открыто доступны только для чтения. Запись в документы ПО, находящиеся в архиве подлинников ПО, возможна только с санкции руководителя проекта ПО. Эта санкция оформляется документально, например, в виде «Решения на доработку ПО», где указывается объем и сроки проведения коррекции ПО, необходимость коррекции смежных программ ПО и документации на систему, объем и сроки необходимой отладки.

По завершении проведения изменений в соответствии с «Решением на доработку» измененное ПО внедряется в систему.

Операция «отчуждение подлинника» проводится после завершения автономной отладки фрагментов ПО и передачи ПО на комплексную отладку.

До сдачи ПО в эксплуатацию возможна иерархия архивов подлинников с различным уровнем санкции на изменение ПО.

После сдачи ПО в эксплуатацию уровень санкции на изменение ПО должен быть максимально высоким.

2. Защита информации в системе при сбоях и отказах аппаратуры. Информационная устойчивость. Эксплуатация сложных систем показывает необходимость защиты информации системы от отказов и сбоев ее структурных элементов, причем таким образом, чтобы система сохраняла свои функциональные возможности. Обычно это обеспечивается наличием избыточности в аппаратуре ЦВМ и ПО. Эта избыточность может быть использована двумя принципиально различными способами:

1. Деградацией системы и ее характеристик в пространстве работоспособных состояний при отказах и сбоях ее структурных элементов.

2. Восстановлением работоспособности отказавших структурных элементов путем использования взамен их резервных элементов.

С данными способами обычно связывается свойство отказосбоеустойчивости сложных систем.

Так как алгоритмы встроенного контроля и диагностика реализуются и информация в системах концентрируется во встроенных ЦВМ, то вопросы отказоустойчивости сложных систем целесообразно рассматривать применительно к отказам (неисправностям) встроенных ЦВМ как к критическому в смысле достижения отказоустойчивости звену.

Отказоустойчивость реализуется при наличии в системе следующих свойств (таблица 1) [3]:

1. Избыточность аппаратуры и в определенной мере ПО.

2. Наличие средств встроенного контроля и диагностики для обнаружения и диагностики отказов и сбоев.

Таблица 1

Отказоустойчивость	
Свойства	*Методы*
Избыточность	1. Аппаратное резервирование. 2. Структурная перестройка (реконфигурация). 3. Деградация характеристик. 4. Избыточное отказоустойчивое кодирование.
Встроенный контроль и диагностика для обнаружения момента перехода на резерв	5. Обнаружение отказов общесистемными средствами. 6. Сравнение нескольких однородных реализаций: - аппаратное на каждой машинной операции; - программное. 7. Самопроверки и взаимные проверки: - аппаратные; - тестовые. 8. Моделирование и предсказание процессов управления по текущим состояниям. 9. Разделение отказов от сбоев.
Сохранение правильной информации процессов управления для продолжения работы	10. Запоминание правильной информации в КТ. «Откат» к КТ - загрузка запомненной правильной информации в резервные устройства. 11. Загрузка информации из системы более высокого уровня иерархии. 12. Исправление информации в сбившихся устройствах. 13. «Пропуск» - загрузка текущей информации в точке устранения неисправности (сбоя).

3. Сохранение «правильной» информации процессов управления во время отказа или сбоя и в процессе его парирования для загрузки ее в подключаемые резервные элементы.

При этом практическая реализация свойств 2 и 3 всегда сопровождается возмущениями, которые прикладываются к системе в момент возобновления функционирования. После восстановления работоспособности эти возмущения, связанные со старением информации в системе из-за отсутствия управления в течение некоторого времени, не должны приводить к потере устойчивости системы.

Таким образом, наличие только резерва аппаратуры не обеспечивает отказоустойчивости системы, также как вероятность безотказной работы (ВБР) характеризует ее не в полной мере.

Наряду с ВБР мерой отказоустойчивости должна быть вероятность сохранения устойчивости работы системы, которая является функцией вероятности обнаружения и диагностики отказа за заданное время, вероятности сохранения и загрузки «правильной» информации в резервные устройства, вероятности появления определенного уровня возмущений на систему в момент восстановления управления.

Различные методы сохранения правильной информации при обеспечении отказоустойчивости из таблицы 1 обеспечивают соответственно различную вероятность сохранения устойчивости системы (различную вероятную величину кратковременных возмущений на фазовых координатах системы) в момент восстановления управления.

Обнаружение отказов или сбоев, приводящих к искажению информации, может базироваться на обнаружении их последствий системными средствами - они проявятся через какой-то интервал времени в виде отклонений за допустимую область фазовых координат системы. В результате команда на подключение резерва или реконфигурацию будет получена с большой задержкой, когда продолжать работу нельзя и надо думать об аварийной защите системы, если она еще возможна.

Поэтому обычно обнаружение отказов или сбоев, а точнее искажений информации, базируется на сравнении на аппаратном или программном уровне двух или более однородных результатов, полученных в управляющей вычислительной системе по одним и тем же исходным данным, по одному и тому же либо по различным алгоритмам, на аппаратном либо тестовом самоконтроле устройств системы или на их взаимном контроле путем

обмена контрольной информацией. Последние методы обладают существенно меньшим запаздыванием, чем первый, то есть обнаружение отказов может произойти до того, как они или их последствия стали различимы в поведении системы.

При решении вопроса защиты информации процессов управления от последствий сбоя или отказа (для продолжения работы системы после парирования отказа) возможен вариант с «откатом» - возвратом процесса к точке, где исправное состояние системы и информации было обеспечено. Для возможности «отката» нужно запоминать и хранить некоторые состояния процесса в потенциальных точках возврата - контрольных точках (КТ).

Также возможен вариант с «пропуском» - продолжением процессов управления после восстановления работоспособности по текущей информации в точке устранения неисправности или сбоя.

Кроме того, возможен вариант «исправления» путем замены неверной информации в устройствах системы на правильную из заведомо работоспособных устройств. Например, такое исправление происходит в системах с мажорированием информации, аппаратном или программном, для «выпадающего» канала аппаратуры.

Методы аппаратного мажорирования (голосования) при исполнении каждой машинной операции в ЦВМ системы, а также избыточного отказоустойчивого кодирования при хранении и передаче информации обеспечивают использование избыточности, обнаружение ошибки, восстановление правильной информации в течение одной машинной операции на аппаратном уровне и не требуют ни «отката», ни «пропуска».

При других методах обеспечения отказо- и сбоеустойчивости (таблица 1) в сложном мультипрограммном ПО на интервале времени от момента возникновения отказа (сбоя) до момента его обнаружения процедурой диагностики может быть выдан ряд команд управления, принята или выдана информация, выработаны и сохранены глобальные переменные в ПО, инициирован ряд программ ПО. Проблема заключается в том, что все эти действия уже могут содержать ошибку, но в момент их исполнения она еще не обнаружена.

В связи с этим тактика исполнения процедуры диагностики отказа (сбоя) должна учитывать последовательность выдачи и приема команд и информации во встроенной ЦВМ, обращений ее к базе данных.

Без учета этого исполнение «отката» или «пропуска» не обеспечивает правильного функционирования системы в дальнейшем.

3. Аварийная защита. В общем случае «откат» с целью получения правильной информации для дальнейшей работы системы после сбоя или «отката» можно осуществлять в другое устойчивое состояние системы. Эта возможность приводит к методу обеспечения работоспособности систем при отказах, который назовем «аварийной защитой».

Этот метод связан с организацией дополнительного устойчивого состояния системы, при нахождении в котором отказ может быть устранен и ее работоспособность восстановлена. Дополнительные устойчивые состояния системы, возможные хотя бы для части наиболее значимых ее фазовых координат, и методы перевода в них должны быть определены при проектировании системы. Например, для КА дополнительному устойчивому состоянию соответствует движение по орбите без угловой ориентации его связанных осей.

Рассматриваемая далее «аварийная защита» базируется на «мягком останове» системы при возникновении отказов и переводе ее в дополнительное устойчивое состояние «первоначального запуска».

«Мягкий останов» должен обеспечивать как можно более организованное и приближенное к штатному выключение аппаратуры системы, что препятствует развитию аварийной ситуации и обеспечивает отсутствие необратимых последствий от отказа для системы, окружающей среды и информации. Этим самым «мягкий останов» создает условия для восстановления работоспособности системы и дальнейшего ее устойчивого функционирования после проведения соответствующих ремонтных мероприятий.

Диагностика отказов в сложной технической системе может занимать определенное время. Еще большее время может занимать восстановление работоспособности и рестарт системы, например, путем внесения изменений в программное обеспечение. Использование аварийной защиты «с мягким остановом» позволяет сочетать быструю реакцию системы на отказ с подключением эксплуатирующего персонала или системы более высокого уровня иерархии к диагностике и восстановлению работоспособности системы.

Заключение. Поскольку возможность сохранения работоспособности сложной системы при отказах и технология реализации ее работоспособности связана с сохранением и восстановлением информации, то можно говорить об информационной устойчивости сложной системы, которая дополняет оценку ее динамической устойчивости.

В процессе разработки сложных систем возникает необходимость защиты ПО и данных в инструментальных средствах разработки ПО, встроенных в систему ЦВМ. Методы технологической защиты этой информации обеспечивают доступность по внесению изменений и защищают от несанкционированных воздействий на данные и ПО.

Список литературы

1. Козлов Д. И., Аншаков Г. П., Мостовой Я. А., Соллогуб А. В. Управление космическими аппаратами зондирования Земли: Компьютерные технологии. – М.: Машиностроение, 1998.

2. Ю. Г. Антонов, Я. А. Мостовой, Ю. В. Чайкин. Принципы определения моментов проведения информационного согласования результатов работы каналов резервированной БВС КА / Тезисы докладов третьей международной научно-технической конференции «Микроэлектроника и информатика». – Москва, Зеленоград, 1997.

3. G. P. Anshakov, Y. G. Antonov, Y. A. Mostovoy. Fault-tolerance and Disaster Protection of the Complex Technical Systems / International Symposium on Impact of Space Technology Innovation on Economic Development, Shanghai, China, April 17-20 2001 г .

4. Иуду К. А. Надежность, контроль и диагностика вычислительных машин и систем. – М.: Высшая школа, 1989.

SOME ISSUES OF TECHNOLOGICAL INFORMATION PROTECTION AND INFORMATION STABILITY OF COMPLEX SYSTEMS

© 2004 G. P. Anshakov, Yu. G. Antonov, Ya. A. Mostovoy, A. V. Sollogub

State Research and Production Space Rocket Centre “TsSKB-Progress”

Issues of technological protection of information and software of complex technical systems.

Methods and mechanisms of maintaining the efficiency of a complex system in case of failures are proposed. The technology of ensuring its efficiency is also proposed.