**Вопросы по лекции №13.**

**Низкоуровневые средства обнаружения ошибочного функционирования ПО и низкоуровневые методы защиты при конструировании безопасного ПО.**

Бригада СанУ11: Ковалев К.А., Терентьев Е.А., Щекочихин Д.А., Оганисян Т.С., Шабакаев А.Р.

Выполнил: Оганисян Т.С.

Группа 6411

**1. В чем заключается стратегия безопасности – стратегия аварийной защиты при разработке ПО СТС**

Стратегия «аварийной защиты» предусматривает априорный при проектировании ПО анализ возможных отказов и ошибок, определение опасности (ущерба) той или иной ошибки в системе или ПО, применения соответствующих мер и средств по скорейшему определения наличия ошибочной ситуации, определению мер, препятствующих развитию ошибочной ситуации и её парированию с целью минимизации ущерба от неё.

**2. Диапазон подходов к решению проблемы безопасности и аварийной защиты**

Диапазон подходов к решению проблемы безопасности и аварий-ной защиты очень велик, начиная от придания системе и ПО свойств отказоустойчивости до организованного прекращения функционирования системы путем «мягкого её останова» с организованным переводом её в запасное устойчивое состояние системы, если его можно найти, либо в исходное состояние «финального останова» с минимизацией ущерба для окружающей среды. если такого запасного устойчивого состояния найти не удается.

Где-то в промежутке между ними находятся подходы с продолжением функционирования системы и ПО с ухудшением его качества в той или иной мере (это и есть тот ущерб, который несет система вследствие проявившейся ошибки).

**3. Что такое отказоустойчивые системы? При каких условиях может быть решена задача достижения отказоустойчивости.**

Отказоустойчивая система — это система, которая при отказе продолжает функционировать без ухудшения качества процессов управления, т.е. отказ части системы или ПО как бы остается без последствий – «не видим» системой либо маскируется ею.

Отказоустойчивость сложных технических систем реализуется при наличии в системе следующих свойств:

1) избыточности аппаратуры и ПО – наличия резерва аппаратных средств и ПО

2) наличие средств встроенного контроля и диагностики в системе и ПО для обнаружения и диагностики отказов, сбоев и ошибок

3) наличия или сохранения «правильной» информации процессов управления для загрузки её в подключаемые резервные элементы при парировании отказов аппаратуры системы

**4. Перечень нештатных ситуаций и его структура**

При проектировании ПО определяется перечень возможных нештатных ситуаций в системе. После чего на каждую возможную нештатную ситуацию системы и ПО из перечня определяется метод её обнаружения и распознавания низкоуровневой защитой путем обработки имеющейся в ЦВМ информации о функционировании системы, либо введением в систему дополнительных датчиков аварийных ситуаций и состояний. В итоге контрольные фрагменты ПО низкоуровневой защиты, обнаруживающие, распознающие и локализующие ошибочные состояния - нештатные ситуации распределены по различным частям запрограммированного ПО. Обнаружив ошибочные состояния эти структурные части ПО либо используют свои методы восстановления работоспособности, если им хватает на это компетенции, либо передают управление на системный уровень аварийной защиты. На каждую ситуацию из перечня на каждую такую передачу управления в программе аварийной защиты системного уровня определяется один из рассмотренных трех сценариев реакции, направленной на минимизацию ущерба и восстановления работоспособности, реализуемый в самом ПО.

После этого в специально выделенном системном модуле ( программе) ПО, предназначенном для управления в нештатных ситуациях СТС, программируется «таблица» с перечнем предусмотренных при проектировании и рас-познаваемых ПО нештатных ситуаций и управленческих сценариев реакций на каждую из них. Входы в эту таблицу инициируются при возникновении и обнаружении встроенным контролем соответствующих нештатных ситуаций.

При возникновении непредусмотренных при проектировании или не распознаваемых нештатных ситуаций необходимо обеспечивать реакцию по самому радикальному сценарию - полного прекращения функционирования ПО и системы сорганизованным переходом их в исходное состояние (сценарию «мягкого останова»).

**5. Аварийная защита как элемент политики безопасности СТС**

Метод аварийной защиты ПО, базирующейся на «мягком» останове работ ПО позволяет корректно завершить работу ПО, выключить аппаратуру, привести систему и ПО в исходное состояние и дать сообщения об ошибке в систему более высокого уровня иерархии или эксплуатирующему персоналу.

**6. Три обобщенных сценария управления работой ПО, реализуемых в системной программе аварийной защиты**

1.Продолжение исполнения с ухудшением качества функционирования

2.Снятие ряда задач и исполнение только дежурных задач безопасности

3.Полное прекращение выполнения задач с мягким остановом

**7. В чем состоит проблема отмены Выданной из ПО управляющей информации (команды)?**

Проблема заключается в том, что выданные ошибочные команды часто являются не обратимыми. Выданная команда на включение ракетного двигателя приведёт к изменению скорости ракеты. Такую команду, выданную ошибочно, или несвоевременно можно отменить – выключить двигатель, но ракета уже летит и изменила скорость.

Во всех подобных случаях надо решить, а что будет с системой, кто её вернет в исходное состояние вместе с ПО, если командные воздействия на систему уже прошли и их не вернуть да и время уже ушло и его тоже не вернуть?

**8. Как отменить ошибочную или несвоевременную выдачу управляющей информации из ПО?**

Отмену ошибочных действий ПО надо сопровождать и возвращением системы в исходное состояние на момент проведения неправильных действий над ПО. Поэтому развитие неправильной ситуации необходимо прекращать не только отменой неправильной команды, но и приведением системы в исходное состояние. Это удобнее всего сделать через механизм аварийной защиты в варианте полного прекращения работы ПО и системы с «мягким остановом», который по определению и приводит систему в исходное состояние. При этом работа ПО, начинается с «чистого листа»

Выполнил: Терентьев Е.А.

Группа 6411

**1. В чем заключается стратегия безопасности – стратегия аварийной защиты при разработке ПО СТС**

Стратегия безопасности ПО – стратегия «аварийной защиты» предусматривает априорный при проектировании ПО анализ возможных отказов и ошибок, определение опасности (ущерба) той или иной ошибки в системе или ПО, применения соответствующих мер и средств по скорейшему определению наличия ошибочной ситуации, определению мер, препятствующих развитию ошибочной ситуации и её парированию с целью минимизации ущерба от неё. При этом оценки величины ущерба, нанесенного отказом, должны быть сопоставлены с величиной затрат на средства его предотвращения либо обнаружения.

**2. Диапазон подходов к решению проблемы безопасности и аварийной защиты**

Диапазон подходов к решению проблемы безопасности и аварийной защиты очень велик, начиная от придания системе и ПО свойств отказоустойчивости до организованного прекращения функционирования системы путем «мягкого её останова» с организованным переводом её в запасное устойчивое состояние системы, если его можно найти, либо в исходное состояние «финального останова» с минимизацией ущерба для окружающей среды, если такого запасного устойчивого состояния найти не удается.

**3. Что такое отказоустойчивые системы? При каких условиях может быть решена задача достижения отказоустойчивости.**

Отказоустойчивая система это такая система, которая продолжает функционировать без ухудшения качества процессов управления т.е. отказ части системы или ПО как бы остается без последствий.

Отказоустойчивость сложных технических систем реализуется при наличии в системе следующих свойств:

1) избыточности аппаратуры и ПО – наличия резерва аппаратных средств и ПО

2) наличие средств встроенного контроля и диагностики в системе и ПО для обнаружения и диагностики отказов, сбоев и ошибок

3) наличия или сохранения «правильной» информации процессов управления для загрузки её в подключаемые резервные элементы при парировании отказов аппаратуры системы

**4. Перечень нештатных ситуаций и его структура**

При проектировании ПО определяется перечень возможных нештатных ситуаций в системе. После чего на каждую возможную нештатную ситуацию системы и ПО из перечня определяется метод её обнаружения и распознавания низкоуровневой защитой путем обработки, имеющейся в ЦВМ информации о функционировании системы, либо введением в систему дополнительных датчиков аварийных ситуаций. Контрольные фрагменты ПО низкоуровневой защиты, обнаружив ошибочные состояния либо используют свои методы восстановления работоспособности, если им хватает на это компетенции, либо передают управление на системный уровень аварийной защиты. На каждую ситуацию из перечня в программе аварийной защиты системного уровня определяется сценарий реакции, направленной на минимизацию ущерба и восстановления работоспособности:

После этого в специально выделенном системном модуле (программе) ПО, предназначенном для управления ПО в нештатных ситуациях, программируется таблица с перечнем предусмотренных при проектировании и распознаваемых ПО нештатных ситуаций и сценариев реакций на каждую из них. Входы в эту таблицу инициируются при возникновении и обнаружении встроенным контролем соответствующих нештатных ситуаций. При возникновении непредусмотренных при проектировании или не распознаваемых нештатных ситуаций необходимо обеспечивать прекращение функционирования ПО и системы с организованным переходом их в исходное состояние (сценарию «мягкого останова»).

**5. Аварийная защита как элемент политики безопасности СТС**

Метод аварийной защиты ПО, базирующейся на «мягком» останове работы ПО позволяет корректно завершить работу ПО, выключить аппаратуру, привести систему и ПО в исходное состояние и дать сообщения об ошибке в систему более высокого уровня иерархии или эксплуатирующему персоналу.

**6. Три обобщенных сценария управления работой ПО, реализуемых в системной программе аварийной защиты**

1. Продолжение исполнения с ухудшением качества функционирования

2. Снятие ряда задач и исполнение только дежурных задач безопасности

3. Полное прекращение выполнения задач с «мягким остановом»

**7. В чем состоит проблема отмены Выданной из ПО управляющей информации (команды)?**

Выданные ошибочные команды часто являются не обратимыми. В подобных случаях надо решить, что будет с системой, кто её вернет в исходное состояние вместе с ПО, если командные воздействия на систему уже прошли и их не вернуть.

**8. Как отменить ошибочную или несвоевременную выдачу управляющей информации из ПО?**

Отмену ошибочных действий ПО надо сопровождать возвращением системы в исходное состояние на момент проведения неправильных действий над ПО. Это удобнее всего сделать через механизм аварийной защиты в варианте полного прекращения работы ПО и системы с «мягким остановом», который по определению и приводит систему в исходное состояние

Выполнил: Шабакаев А.Р.

Группа 6411

**1. В чем заключается стратегия безопасности – стратегия аварийной защиты при разработке ПО СТС**

Стратегия безопасности ПО заключается:

- анализе возможных отказов и ошибок при проектировании ПО;

- определении опасности ущерба ошибки в системе или ПО;

- применении соответствующих мер и средств по скорейшему по скорейшему определению наличия ошибочной ситуации;

- определению мер, препятствующих развитию ошибочной ситуации и её парированию с целью минимизации ущерба от неё.

Замечание: стоимость защитных мероприятий не должны превышать величин ущерба.

**2. Диапазон подходов к решению проблемы безопасности и аварийной защиты**

Диапазон подходов к решению проблемы безопасности и аварийной защиты достаточно большой, от придания системе и ПО свойств отказоустойчивости до организованного прекращения функционирования системы путем «мягкого останова» с организованны переводом ее в запасное устойчивое состояние системы, если возможно найти, или в исходное состояние «финального останова» с минимизацией ущерба для окружающей среды, если такого запасного устойчивого состояния найти не получается.

**3. Что такое отказоустойчивые системы? При каких условиях может быть решена задача достижения отказоустойчивости.**

Отказоустойчивая система – система, которая продолжает функционировать без ухудшения качества процессов управления. Отказ ПО или части системы «остается бе последствий» - «невидим» системой либо маскируется ею.

Условия решения задачи достижения отказоустойчивости СТС:

1) избыточности аппаратуры и в определённой мере ПО – наличия резерва аппаратных средств и ПО, подключаемого при отказе основных средств и ПО

2) наличие средств встроенного контроля и диагностики в системе и ПО для обнаружения и диагностики отказов, сбоев и ошибок, а точнее нарушения целостности и доступности информации.

3) наличия или сохранения «правильной» информации процессов управления для загрузки её в подключаемые резервные элементы при парировании отказов аппаратуры системы.

**4. Перечень нештатных ситуаций и его структура**

При проектировании ПО с целью обеспечения безопасности определяется перечень возможных нештатных ситуаций в системе и ПО. После чего на каждую нештатную ситуацию определяется метод её обнаружения и распознавания низкоуровневой защитой. Осуществляется это путем обработки имеющейся в ЦВМ информации о функционировании системы, либо введением в систему дополнительных датчиков аварийных ситуаций и состояний.

Таким образом, контрольные фрагменты ПО низкоуровневой защиты, обнаруживающие, распознающие и локализующие нештатные ситуации, распределены в различных частях разработанного ПО. При обнаружении используют методы восстановления работоспособности, если хватает им на это компетенции, либо передают управление на системный уровень аварийной защиты.

На каждую ситуацию из перечня на каждую такую передачу управления в программе аварийной защиты системного уровня определяется один из рассмотренных трех сценариев реакции, направленной на минимизацию ущерба и восстановления работоспособности, реализуемый в самом ПО.

**5. Аварийная защита как элемент политики безопасности СТС**

Один из методов защиты ПО заключается в «мягком» останове работ ПО, а именно:

- прекращение работы ПО в корректной форме (простой и универсальное решение);

- выключение аппаратуры, приведение ПО в исходное состояние;

- передача сообщения об ошибке в систему более высокого уровня иерархии или эксплуатирующему персоналу

Однако не все системы терпят прекращение работы ПО и крайне желательно продолжить их функционирование, допустимо снижение качества функционирования ПО. Допустимы приемы

защитного программирования для обнаружения некорректных входных данных либо ошибочных результатов.

Также обратим внимание на приложения, связанных с управлением объектов, где происходит частое повторение алгоритмов управления с выбранным периодом. Здесь можно продолжить функционирование, так как один неверный такт не приведет к резкому ухудшению результата, и имеется шанс получить в следующем такте получить новые неискаженные входные данные.

В общем случае, когда программа, в которой хотим реализовать методы устойчивости к некорректным данным, не может решить, как неточные результаты ее работы скажутся на ПО или СТС, приходиться обратиться на второй системный уровень защиты от ошибок к специальной программе аварийной защиты, которая знает, что делать в нештатной ситуации.

**6. Три обобщенных сценария управления работой ПО, реализуемых в системной программе аварийной защиты**

1) Продолжение исполнения с ухудшением качества функционирования

2) Снятие ряда задач и исполнение только дежурных задач безопасности

3) Полное прекращение выполнения задач с «мягким» остановом

**7. В чем состоит проблема отмены Выданной из ПО управляющей информации (команды)?**

Проблема отмены выданной из ПО управляющей команды заключается в том, что часто такие команды являются необратимыми. К примеру, ошибочная команда запуска торпеды в подводной лодке невозможно обратить – торпеда уже запущена и набрала скорость.

**8. Как отменить ошибочную или несвоевременную выдачу управляющей информации из ПО?**

Необходимо осуществить: прекращение развития неправильной ситуации отменой неправильной команды, а также приведением системы в исходное состояние на момент выполнения неправильного действия ПО.

Через механизм аварийной защиты осуществляется полное прекращение работы ПО и системы с «мягким остановом», который приводит систему в исходное состояние, и работа ПО начинается с «чистого листа».

Выполнил: Щекочихин Д.А  
группа 6411

**1. В чем заключается стратегия безопасности – стратегия аварийной защиты при разработке ПО СТС.**

Стратегия безопасности ПО – стратегия «аварийной защиты» предусматривает априорный при проектировании ПО анализ возможных отказов и ошибок, определение опасности (ущерба) той или иной ошибки в системе или ПО, применения соответствующих мер и средств по скорейшие определения наличия ошибочной ситуации, определению мер, препятствующих развитию ошибочной ситуации и её парированию с целью минимизации ущерба от неё.

**2. Диапазон подходов к решению проблемы безопасности и аварийной защиты.**

Диапазон подходов к решению проблемы безопасности и аварийной защиты:

1. Придания системе и ПО свойств отказоустойчивости

2. Прекращения функционирования системы путем «мягкого её останова» с организованным переводом её в запасное устойчивое состояние системы, если его можно найти, либо в исходное состояние «финального останова» с минимизацией ущерба для окружающей среды, если такого запасного устойчивого состояния найти не удается.

Где-то в промежутке между ними находятся подходы с продолжением функционирования системы и ПО с ухудшением его качества в той или иной.

**3. Что такое отказоустойчивые системы? При каких условиях может быть решена задача достижения отказоустойчивости.**

Отказоустойчивая система - это система, которая продолжает функционировать без ухудшения качества процессов управления т.е. отказ части системы или ПО как бы остается без последствий – «не видим» системой либо маскируется ею.

Условия, при которых может быть решена задача достижения отказоустойчивости:

1) избыточности аппаратуры и в определённой мере ПО – наличия резерва аппаратных средств и ПО, подключаемого при отказе основных средств и ПО.

2) наличие средств встроенного контроля и диагностики в системе и ПО для обнаружения и диагностики отказов, сбоев и ошибок, а точнее нарушения целостности и доступности информации.

3) наличия или сохранения «правильной» информации процессов управления для загрузки её в подключаемые резервные элементы при парировании отказов аппаратуры системы.

**4. Перечень нештатных ситуаций и его структура.**

Структура:

1. При проектировании ПО определяется перечень возможных нештатных ситуаций в системе.

2. Определяется метод её обнаружения и распознавания низкоуровневой защитой путем обработки, имеющейся в ЦВМ информации о функционировании системы, либо введением в систему дополнительных датчиков аварийных ситуаций и состояний.

3. Определяется один из трех сценариев реакции, направленной на минимизацию ущерба и восстановления работоспособности, реализуемый в самом ПО.

4. Программируется «таблица» с перечнем предусмотренных при проектировании и распознаваемых ПО нештатных ситуаций и управленческих сценариев реакций на каждую из них.

**5. Аварийная защита как элемент политики безопасности СТС.**

Метод аварийной защиты ПО, базируется на «мягком» останове работ ПО и позволяет корректно завершить работу ПО, выключить аппаратуру, привести систему и ПО в исходное состояние и дать сообщения об ошибке в систему более высокого уровня иерархии или эксплуатирующему персоналу.

**6. Три обобщенных сценария управления работой ПО, реализуемых в системной программе аварийной защиты.**

1. Снятия с исполнения только той задачи, в которой проявилась ошибка, и продолжение функционирования ПО (возможно с некоторым ухудшением качества) без ограничений.

2. Сокращения объема выполняемых ПО задач до определенного минимума задач, предназначенных для поддержания только само сохраняемого состояния системы без исполнения в полной мере её целевых задач. Этому сценарию соответствуют более серьёзные нарушения работоспособности ПО и системы и алгоритм контроля должен быть способен различать такие ситуации.

3. Полного прекращения функционирования СТС с «мягким остановом» системы с приведением аппаратуры и ПО в исходное состояние.

**7. В чем состоит проблема отмены Выданной из ПО управляющей информации (команды)?**

Проблема может состоять в том, что при отмене ошибочно или несвоевременно выданной команды последствия могут быть не обратимыми.

Например, если поступила команда выключить двигатель, но она была несвоевременной то это может привести к ситуации, что ракета уже летит и изменила скорость

**8. Как отменить ошибочную или несвоевременную выдачу управляющей информации из ПО?**

Отмену ошибочных действий ПО надо сопровождать возвращением системы в исходное состояние на момент проведения неправильных действий над ПО. Это удобнее всего сделать через механизм аварийной защиты в варианте полного прекращения работы ПО и системы с «мягким остановом», который по определению и приводит систему в исходное состояние. При этом работа ПО, начинается с «чистого листа».

Выполнил: Ковалев К.А  
группа 6411

**1. В чем заключается стратегия безопасности – стратегия аварийной защиты при разработке ПО СТС.**

Стратегия безопасности ПО – стратегия «аварийной защиты» предусматривает априорный при проектировании ПО анализ возможных отказов и ошибок, определение опасности (ущерба) той или иной ошибки в системе или ПО, применения соответствующих мер и средств по скорейшему определению наличия ошибочной ситуации, определению мер, препятствующих развитию ошибочной ситуации и её парированию с целью минимизации ущерба от неё. При этом оценки величины ущерба, нанесенного отказом, должны быть сопоставлены с величиной затрат на средства его предотвращения либо обнаружения.

**2. Диапазон подходов к решению проблемы безопасности и аварийной защиты.**

Диапазон подходов к решению проблемы безопасности и аварийной защиты достаточно большой, от придания системе и ПО свойств отказоустойчивости до организованного прекращения функционирования системы путем «мягкого останова» с организованны переводом ее в запасное устойчивое состояние системы, если возможно найти, или в исходное состояние «финального останова» с минимизацией ущерба для окружающей среды, если такого запасного устойчивого состояния найти не получается.

**3. Что такое отказоустойчивые системы? При каких условиях может быть решена задача достижения отказоустойчивости.**

Отказоустойчивая система - это система, которая продолжает функционировать без ухудшения качества процессов управления т.е. отказ части системы или ПО как бы остается без последствий – «не видим» системой либо маскируется ею.

Условия:

1. Избыточности аппаратуры и в определённой мере ПО – наличия резерва аппаратных средств и ПО, подключаемого при отказе основных средств и ПО.

2. Наличие средств встроенного контроля и диагностики в системе и ПО для обнаружения и диагностики отказов, сбоев и ошибок, а точнее нарушения целостности и доступности информации.

3. Наличия или сохранения «правильной» информации процессов управления для загрузки её в подключаемые резервные элементы при парировании отказов аппаратуры системы.

**4. Перечень нештатных ситуаций и его структура.**

При проектировании ПО определяется перечень возможных нештатных ситуаций в системе. После чего на каждую возможную нештатную ситуацию системы и ПО из перечня определяется метод её обнаружения и распознавания низкоуровневой защитой путем обработки, имеющейся в ЦВМ информации о функционировании системы, либо введением в систему дополнительных датчиков аварийных ситуаций. Контрольные фрагменты ПО низкоуровневой защиты, обнаружив ошибочные состояния либо используют свои методы восстановления работоспособности, если им хватает на это компетенции, либо передают управление на системный уровень аварийной защиты. На каждую ситуацию из перечня в программе аварийной защиты системного уровня определяется сценарий реакции, направленной на минимизацию ущерба и восстановления работоспособности:

После этого в специально выделенном системном модуле (программе) ПО, предназначенном для управления ПО в нештатных ситуациях, программируется таблица с перечнем предусмотренных при проектировании и распознаваемых ПО нештатных ситуаций и сценариев реакций на каждую из них. Входы в эту таблицу инициируются при возникновении и обнаружении встроенным контролем соответствующих нештатных ситуаций. При возникновении непредусмотренных при проектировании или не распознаваемых нештатных ситуаций необходимо обеспечивать прекращение функционирования ПО и системы с организованным переходом их в исходное состояние (сценарию «мягкого останова»).

**5. Аварийная защита как элемент политики безопасности СТС.**

Метод аварийной защиты ПО, базируется на «мягком» останове работ ПО и позволяет корректно завершить работу ПО, выключить аппаратуру, привести систему и ПО в исходное состояние и дать сообщения об ошибке в систему более высокого уровня иерархии или эксплуатирующему персоналу.

**6. Три обобщенных сценария управления работой ПО, реализуемых в системной программе аварийной защиты.**

1. Снятия с исполнения только той задачи, в которой проявилась ошибка, и продолжение функционирования ПО (возможно с некоторым ухудшением качества) без ограничений.

2. Сокращения объема выполняемых ПО задач до определенного минимума задач, предназначенных для поддержания только само сохраняемого состояния системы без исполнения в полной мере её целевых задач. Этому сценарию соответствуют более серьёзные нарушения работоспособности ПО и системы и алгоритм контроля должен быть способен различать такие ситуации.

3. Полного прекращения функционирования СТС с «мягким остановом» системы с приведением аппаратуры и ПО в исходное состояние.

**7. В чем состоит проблема отмены Выданной из ПО управляющей информации (команды)?**

Выданные ошибочные команды часто являются не обратимыми, ошибочными или несвоевременно выданными. В подобных случаях надо решить, что будет с системой, кто её вернет в исходное состояние вместе с ПО, если командные воздействия на систему уже прошли и их не вернуть.

**8. Как отменить ошибочную или несвоевременную выдачу управляющей информации из ПО?**

Отмену ошибочных действий ПО надо сопровождать возвращением системы в исходное состояние на момент проведения неправильных действий над ПО. Это удобнее всего сделать через механизм аварийной защиты в варианте полного прекращения работы ПО и системы с «мягким остановом», который по определению и приводит систему в исходное состояние. При этом работа ПО, начинается с «чистого листа».