СВД
Встраиваемые
Системы

Использование ЗОСРВ Нейтрино при разработке ПО, связанного с функциональной безопасностью

Александр Кузнецов

Преподаватель учебного центра

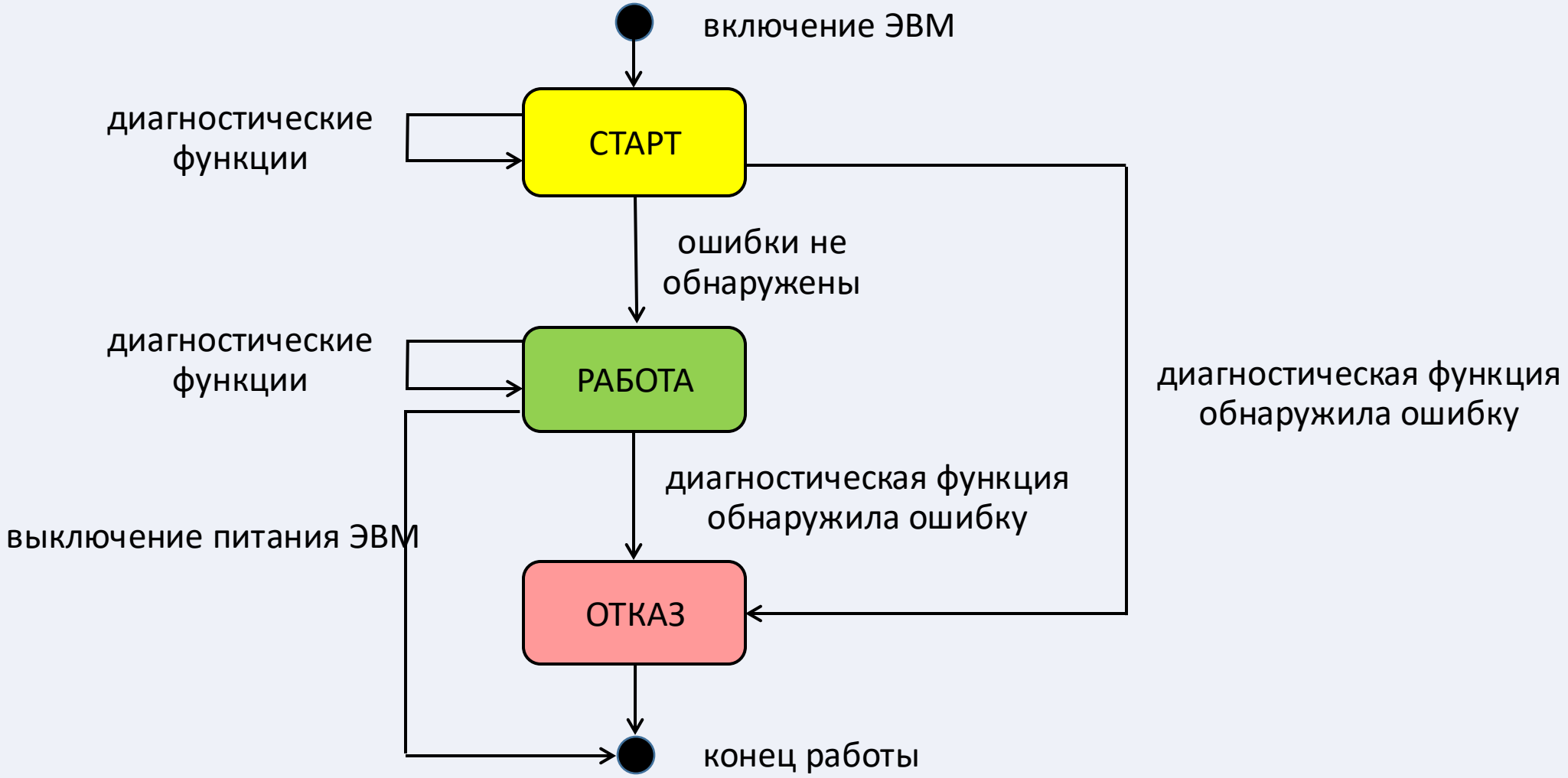
Ядро и системная библиотека ЗОСРВ «Нейтрино»

- **обеспечивают работу программ в среде исполнения «Нейтрино»**
- **соответствуют требованиям ГОСТ IEC 61508-3-2018**
  - по 3-му уровню стойкости к систематическим отказам программного обеспечения (CCO3/SC3)
  - этот уровень является максимальным для системного ПО

Функции ядра и системной библиотеки

- функции инициализации программ
- функции безопасности
- функции диагностики
- функции отладки
- функции интерфейсов к дополнительным модулям ЗОСРВ «Нейтрино»

Конечный автомат состояний ядра / системной библиотеки

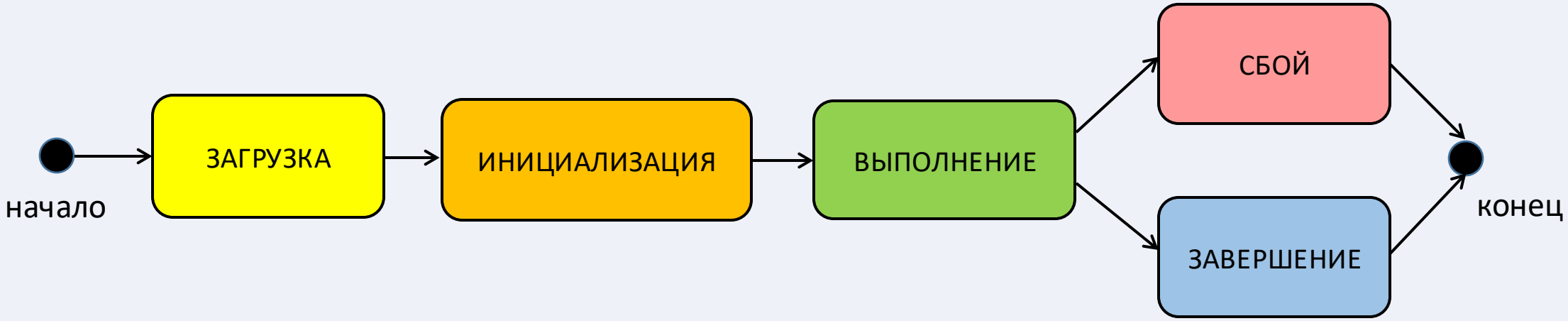


Состояния ядра / системной библиотеки

- **СТАРТ**
  - загрузка ядра и системной библиотеки на устройстве
  - загрузка и инициализация программ
- **РАБОТА**
  - предоставление программам функций безопасности, диагностики, отладки и интерфейсов к дополнительным модулям ЗОСРВ «Нейтрино»
- **ОТКАЗ**
  - вывод сообщения об отказе через диагностический интерфейс
    - обычно используется последовательная консоль через интерфейс UART
  - прекращение работы
    - переход в бесконечный цикл без программного выхода

Разработка программ

- **осуществляется с помощью программного продукта «Комплект разработчика для ЗОСРВ «Нейтрино» редакции <…> »**
- **конечный автомат состояний программы:**



Состояния программы

- **ЗАГРУЗКА**
  - размещение сегментов кода и данных программы в ОЗУ с последующим запуском:
    - модулем **procnto** из сценария загрузки
    - другой программой
- **ИНИЦИАЛИЗАЦИЯ**
  - выделение и инициализация динамических ресурсов для программы:
    - выделение различных видов памяти
    - создание каналов, соединений, файловых дескрипторов и т. д.
    - создание мьютексов и других примитивов синхронизации
    - инициализация всех видов данных, в том числе атрибутных структур ресурсов
    - создание потоков и дочерних процессов
    - загрузка динамических библиотек

Состояния программы (продолжение)

- **ВЫПОЛНЕНИЕ**
  - потоки программ используют API системной библиотеки
  - ядро планирует потоки
  - запрещено вызывать функции системной библиотеки для динамического выделения ресурсов
- **ЗАВЕРШЕНИЕ**
  - освобождение оперативной памяти и ресурсов
    - по собственной инициативе программы
    - по инициативе другой программы с необходимыми правами
    - аварийно по инициативе средств диагностики ядра
- **СБОЙ**
  - программа не работает, но занимает место в ОЗУ
  - необходимо переводить её в состояние ЗАВЕРШЕНИЕ с помощью другой программы с необходимыми правами

Разработка программ

- каждая программа, связанная с ФБ, должна проходить оценку соответствия требованиям ГОСТ IEC 61508-3 по соответствующему уровню ССО
- для изоляции процессов во времени поддерживается механизм партиционирования
- для защиты от инверсии приоритетов поддерживается механизм наследования приоритетов при использовании синхронных сообщений и мьютексов

Функции инициализации

- **создают условия для того, чтобы программы выполняли функции безопасности детерминированным образом**
- **обеспечивают выделение процессу ресурсов устройства**
  - управление дочерними процессами
  - управление динамическими библиотеками
  - управление потоками и механизмами их синхронизации
  - управление памятью процессов
    - динамическая память
    - общая память
  - управление каналами, соединениями и файловыми дескрипторами
  - управление обработкой прерываний
  - управление часами, таймерами и длительностью системного такта

Функции безопасности

позволяют создавать программы, связанные с выполнением функций безопасности

- **синхронизация**
- **передача сообщений между потоками**
- **обработка прерываний**
- **уведомления о срабатывании таймеров**
- **доступ к памяти устройства**

Функции диагностики

используются для выявления сбоев ПО

- **диагностика аппаратных средств**
  - некорректное обращение к шинам
  - некорректные ассемблерные инструкции
  - некорректное использование адресов
  - деление на ноль
  - если эти ошибки возникают в контексте процесса, ядро переводит процесс в состояние СБОЙ
  - если эти ошибки возникают в контексте ядра, ядро переходит в состояние ОТКАЗ
- **мониторинг процессов**
  - переход процесса в состояния СБОЙ и ЗАВЕРШЕНИЕ можно обрабатывать с помощью администратора высокой готовности (**ham**)

Функции диагностики (продолжение)

- **диагностические уведомления**
  - об истечении максимальной длительности блокировки потока
  - о разрыве соединения с каналом
  - о необходимости срочной разблокировки клиента сервером
  - о банкротстве партиции
  - об общесистемных событиях
  - о состоянии администратора ресурса

Функции отладки

собирают информацию о процессах для последующего анализа причин их некорректного поведения

- **трассировка ядра**
  - запись событий в журнал трассировки ядра (**procnto-*-instr-***)
    - запись о событии ядра содержит временную метку, тип и параметры события
    - для анализа трасс в КР для ЗОСРВ «Нейтрино» предусмотрен инструмент **tracekev**
- **дамп памяти**
  - сохранение содержимого памяти процесса после сбоя (с участием службы **dumper**)
- **системный журнал**
  - запись событий в системный журнал (с участием служб **slogger** и **syslogd**)

Функции интерфейсов к дополнительным модулям

Системная библиотека содержит функции доступа к дополнительным модулям ЗОСРВ «Нейтрино»:

- **файлы и файловые системы**
- **стандарные потоки ввода-вывода**
- **операции над стандартными типами данных**
- **поддержка серверов PCI (pci-*)**
- **очереди POSIX-сообщений (mqueue)**
- **POSIX-сигналы**
- **прочие вспомогательные функции**

Требования к компетентности персонала

- **высшее / среднее специальное образование в области вычислительной техники / промышленной автоматизации**
- **знание руководства по функциональной безопасности ядра и системной библиотеки ЗОСРВ «Нейтрино» и эксплуатационной документации**
- **повышение квалификации по следующим направлениям (доступно в учебном центре ООО «СВД ВС»):**
  - Разработка технических средств и программного обеспечения согласно требованиям ГОСТ IEC 61508
  - Разработка программного обеспечения для ЗОСРВ «Нейтрино»
  - Администрирование и диагностика ЗОСРВ «Нейтрино»

Заключение

- **ЗОСРВ «Нейтрино» позволяет разрабатывать программы, связанные с ФБ**
- **ядро и системная библиотека состоят из функций инициализации программ, безопасности, отладки, диагностики и интерфейсов к дополнительным модулям ЗОСРВ «Нейтрино»**
- **ООО «СВД ВС» предоставляет всю необходимую поддержку для подготовки специалистов по разработке и эксплуатации ПО, связанного с ФБ, в соответствии с ГОСТ IEC 61508**

СВД
Встраиваемые
Системы

Спасибо за внимание!

Александр Кузнецов

Преподаватель учебного центра

ул. Кузнецовская, д. 19
г. Санкт-Петербург
www.kpda.ru
+7 (812) 317-55-56