Операционная система встраиваемого модуля безопасности "ОС РуСим МБ"

Инструкция по установке, жизненный цикл

ТРБП.10003-02

Листов 12

АННОТАЦИЯ

Настоящий документ является описанием процедуры установки программного комплекса (далее – ПК) "Операционная система РуСим встраиваемого модуля безопасности" ТРБП.10003-02 ("ОС РуСим встраиваемого модуля безопасности", далее по тексту – "ОС РуСим МБ" или "программа").

В документе приведены общие сведения о процессе установки:

- общее описание процедуры установки;
- частные случаи установки.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

Операционная система РуСим встраиваемого модуля безопасности ("ОС РуСим МБ") представляет из себя низкоуровневое программное обеспечение, устанавливаемая непосредственно в память ИС. При этом на каждой из поддерживаемых платформ, обеспечивается уровень совместимости с аппаратным обеспечением, и активация механизмов обеспечения безопасности и целостности загружаемого ПО:

- Использование криптографической защиты, загружаемого ПО.
- Аутентификация процесса загрузки

  Производители ИС предоставляют каждому потребителю уникальные ключи доступа к процедуре загрузки. В случае отсутствия данных механизмов — реализуются за счёт внешнего доверенного загрузчика.

  После первоначальной загрузке ПО — запись на дальнейшие изменения блокируется.

2. ИНСТАЛЛЯЦИЯ ПРОГРАММЫ

1.1. Инсталляция программы производится путем загрузки образа (маски) "ОС РуСим МБ" встраиваемого модуля безопасности на интегральную схему в процессе ее изготовления (этап 5 жизненного цикла продукта – см. Приложение 2).

3. НАСТРОЙКА ПРОГРАММЫ

1. Порядок настройки программы описан в блок-схеме, представленной на ***Рисунке 1***.

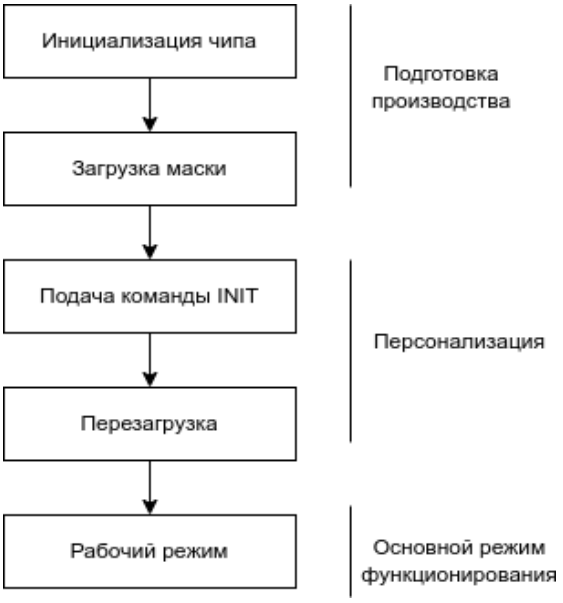

Рисунок 1

4. ПРОВЕРКА ПРОГРАММЫ

1. Для проверки работоспособности программы нам необходимо убедиться в том, что команда GENERATE RANDOM выполняется успешно.
2. Программа считается работоспособной, если команда GENERATE RANDOM выполняется успешно.

5. НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

1. Программа начинает функционировать при подаче напряжения питания и старте работы МК модуля безопасности под управлением "ОС РуСим МБ", дополнительных действий для вызова программы не требуется.

6. ВЫПОЛНЕНИЕ ПРОГРАММЫ

1. Общие сведения о работе с программой

11.1.1 Запуск программы

Программа начинает функционировать при подаче напряжения питания и старте работы МК модуля безопасности под управлением "ОС РуСим МБ", дополнительных действий для вызова программы не требуется.

11.1.2 Завершение работы с программой

Завершение работы программы происходит при прерывании питания МК модуля безопасности.

УСТАНОВКА НА СТАДИИ ПРОИЗВОДСТВА

Для оптимизации времени подготовки продуктов, с использованием "ОС РуСим МБ", загрузка ПО производится на стадии производства ИС — прямой загрузки во flash-память, а в случаях ее отсутствия — формирования маски ROM-памяти.

Дальнейшие операции с памятью блокируются. Дополнительное профилирование операционной системы осуществляется в рамках заложенных в ней функций.

УСТАНОВКА ЕДИНИЧНЫХ ИЗДЕЛИЙ

Для установки операционной системы, при единичном изготовлении требует:

- Наличие ключей доступа к загрузчику, от производителя ИС
- Программы загрузчика образа операционной системы, с поддержкой механизмов аутентификации в ИС
- Считывателя смарт-карт

Общая схема загрузки операционной системы, представлена на ***Рисунке 1***.

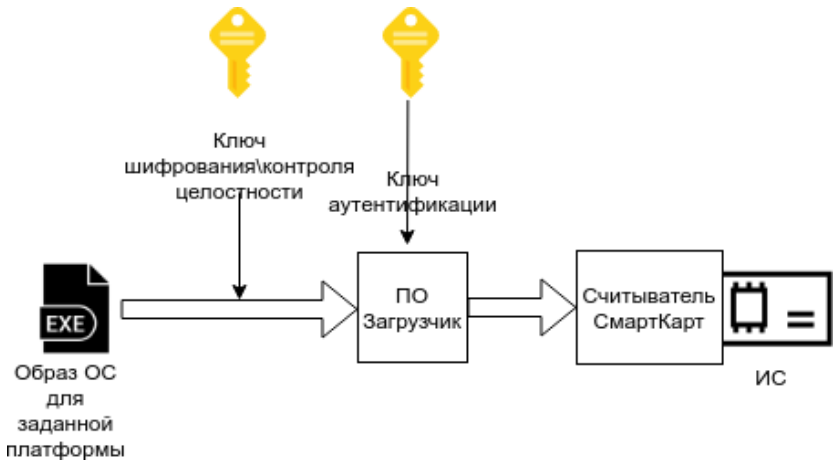

Рисунок 1. Схема загрузки

Основные шаги:

1. Получить образ ОС для заданной платформы
2. Криптографическими методами обеспечить целостность образа (зашифровать)
3. Установить в смарт-карт ридер чистую ИС
4. В программу загрузчика (от производителя ИС) предоставить ключ аутентификации (доступа) к загрузчику.
5. Загрузить образ в ИС

Приложение 2. Жизненный цикл "ОС РуСим МБ"

Жизненный цикл "ОС РуСим МБ" является частью жизненного цикла продукта, т. е., модуля безопасности – от стадии разработки до использования абонентом (Таблица П1).

Инсталляция "ОС РуСим МБ" осуществляется на стадии (этап 5, таблица П1) при производстве модуля безопасности, при этом результат на этой стадии – инициализированный модуль безопасности.

Таблица П1

№этапа ЖЦ[1]	**Интегрированный продукт модуль безопасности[2]**	**Применяемый микроконтроллер – (ИС[3])**	**Разрабатываемый ПК "ОС РуСим МБ" — встраиваемого модуля безопасности**
Этап 1	Разработка (проектирование) ВПО[4] для ИС	Разработка прошивки (ВПО) ИС	Разработка (проектирование) ОС
Этап 2		Разработка ИС (проектирование, разработка структуры, логической и (или) электрической принципиальной схемы ИС, топологии ИС)	Осуществление доставки образа разработанной ОС на производство.
Этап 3		Производство ИС (полный цикл от пластины к кристаллу)	Хранение файлов разработчика ОС на производстве, подготовка к персонализации, тестирование ОС
Этап 4		Упаковка ИС (корпусирование)	Хранение файлов разработчика ОС на

1 ЖЦ – жизненный цикл.
2 Интегрированный продукт сим-карта включает в себя ИС с установленным на нее ВПО.
3 ИС – интегральная схема.
4 ВПО – встроенное программное обеспечение (Chip firmware, OS, applets, user code).

			производстве, подготовка к персонализации, тестирование ОС
Этап 5	Инициализация модуля безопасности. Комплектация составного продукта (внедрение компонентов программного обеспечения в ИС)	Сборка ИС, ВПО, платформы	ОС – платформа инсталлируется в модуль безопасности
Этап 6	Персонализация продукта, предшествующая его использованию (внедрение данных серийного номера и инициализации)	Персонализация (Сборка ИС, ВПО, ОС – платформы, данных серийного номера и инициализации)	Персонализация ОС – платформы. В инициализированную ОС дополнительно внедряются данные серийного номера, доверенный стартовый вектор.
Этап 7	Эксплуатация	Эксплуатация ИС в составе модуля безопасности	Эксплуатация ОС – платформы в составе модуля безопасности
Этап 8	Сбор возникающих проблем у конечных пользователей и внесение информации о них в систему отслеживания проблем (bugtracker) для последующего устранения.	Сбор возникающих проблем у конечных пользователей и внесение информации о них в систему отслеживания проблем (bugtracker) для последующего устранения.	Сбор возникающих проблем у конечных пользователей и внесение информации о них в систему отслеживания проблем (bugtracker) для последующего устранения.

Процесс инициализации состоит в выполнении циклов операций, состоящих из загрузки команды внешним устройством в буфер чип-карты,

выполнении команды чип-картой и возврате чип-картой сообщения о результате выполнения команды внешнему устройству.

Перед операцией загрузки внешним устройством формируют блок команд, содержащий административную команду, в которой в качестве данных используются несколько команд, подаваемых на карту, выполняют упомянутый блок команд и возвращают сообщение о результате выполнения блока команд внешнему устройству. При этом количество команд в блоке должно быть максимально возможным для сокращения циклов обмена и определяется длиной команд, размером буфера команд, максимально допустимой длиной данных в используемом протоколе передачи.

После производства конечного продукта возможности обновить "ОС РуСим МБ" отсутствует. В случае выявления критичных ошибок и проблем – их устранение происходит только при производстве последующих партий продукта.

ПОДДЕРЖКА "ОС РУСИМ МБ"

В рамках технической поддержки "ОС РуСим МБ" обеспечивает вторую и третью линию технической поддержки и осуществляется две основные активности:

- Предварительная консультирование заказчиков по вопросам совместимости, конфигурирования и возможности персонализации "ОС РуСим МБ".

- Сопровождение выпущенных продуктов на базе "ОС РуСим МБ", в области их переконфигурирования в процессе работы.

Первая линия технической поддержки осуществляется заводами производителями конечных продуктов.

ЦИКЛ РАЗРАБОТКИ "ОС РУСИМ МБ"

В основу цикла разработки "ОС РуСим МБ" положен итеративный подход – нацеленный на получение стабильного релиза продукта, с заданными характеристиками в определенное время.

Ключевыми точками формирования релиза является:

- Портирование на новую аппаратную архитектуру
- Реализация специфичных требований заказчика.

В рамках каждой итерации формируется отдельная ветвь (branch) кода, сопровождаемая задачами (issue) для реализации и ответственными.

Каждый новый внедряемый функционал сопровождается механизмами для автоматического тестирования.

Для поддержания стабильности релизов внедрена система CI/CD, включающая в себя:

- Статический анализ исходных кодов
- Сборку всех возможных конфигурация "ОС РуСим МБ"
- Автоматическое тестирование в режимах эмуляции окружения
- Автоматическое тестирование на реальном оборудование
- Информирование о возникших проблемах.

По результирующему отчёту принимается решение о достижение поставленных целей, отсутствию критичных замечаний и возможности фиксации стабильного релиза.

Перечень сокращений

МК – микроконтроллер

ОС – операционная система

ПЗУ – постоянное запоминающее устройство

ПК – программный комплекс

ПО – программное обеспечение

ППЗУ – перезаписываемое постоянное запоминающее устройство

ПРТС – подвижная радиотелефонная связь