

**Операционная система встраиваемого модуля безопасности "ОС РуСим МБ"**  
**Инструкция по установке**  
**ТРБП.10003-02**

*Листов 7*

## АННОТАЦИЯ

Настоящий документ является описанием процедуры установки и эксплуатации 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").

Настоящий программный комплекс (ПК) не содержит лицензионных продуктов – программное обеспечение (ПО) базируется на собственном разработанном исходном коде.

В документе приведены общие сведения о процессе установки, эксплуатации:

- общее описание процедуры установки;
- частные случаи установки;
- эксплуатация (поддержка).

## СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ.....	4
2. ИНСТАЛЛЯЦИЯ ПРОГРАММЫ.....	5
3. НАСТРОЙКА ПРОГРАММЫ.....	5
4. ПРОВЕРКА ПРОГРАММЫ.....	5
5. НАЧАЛО РАБОТЫ С ПРОГРАММОЙ.....	6
6. ВЫПОЛНЕНИЕ ПРОГРАММЫ.....	6
УСТАНОВКА НА СТАДИИ ПРОИЗВОДСТВА.....	6
УСТАНОВКА ЕДИНИЧНЫХ ИЗДЕЛИЙ.....	7

## 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.

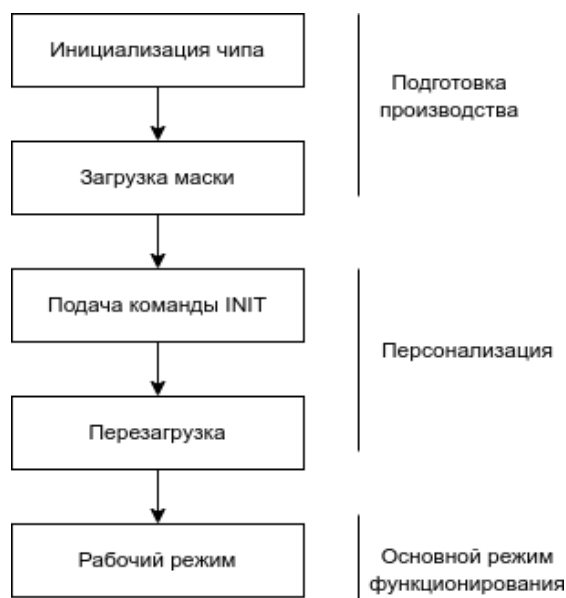
После первоначальной загрузке ПО — запись на дальнейшие изменения блокируется.

## 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.

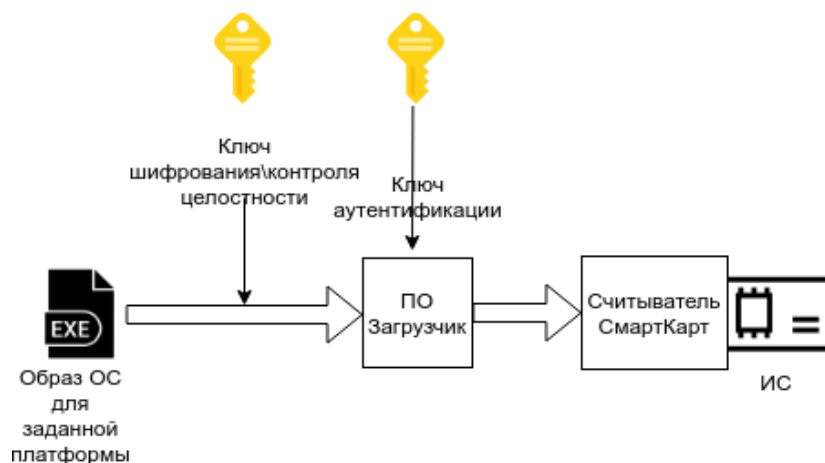
Дальнейшие операции с памятью блокируются. Дополнительное профилирование операционной системы осуществляется в рамках заложенных в ней функций.

## 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-карты ридер чистую ИС
4. В программу загрузчика (от производителя ИС) предоставить ключ аутентификации (доступа) к загрузчику.
5. Загрузить образ в ИС.