

Операционная система РуСим («ОС РуСим»)
Описание программы

Листов 29

АННОТАЦИЯ

Настоящий документ является описанием программного комплекса (далее – ПК) «Операционная система РуСим» («ОС РуСим», далее по тексту – программа).

В документе приведены общие сведения о программе:

- описание функциональных характеристик ОС РуСим являющейся составной частью модуля идентификации абонента (USIM) для использования в подвижных радиотелефонных сетях (далее – ПРТС) стандартов 2G, 3G/LTE, 5G;
- описаны логическая структура и алгоритм работы программы;
- указаны технические средства, которые используются при работе программы, способы её вызова и загрузки, входные и выходные данные.

СОДЕРЖАНИЕ

1.	ОБЩИЕ СВЕДЕНИЯ.....	4
2.	ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ.....	5
3.	ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ	6
4.	ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА.....	11
5.	ВЫЗОВ И ЗАГРУЗКА	13
6.	ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ	14
7.	ИНСТАЛЛЯЦИЯ ПРОГРАММЫ	15
8.	НАСТРОЙКА ПРОГРАММЫ	17
9.	ПРОВЕРКА ПРОГРАММЫ.....	18
10.	НАЧАЛО РАБОТЫ С ПРОГРАММОЙ.....	19
11.	ВЫПОЛНЕНИЕ ПРОГРАММЫ	20
	ПРИЛОЖЕНИЕ 1. ОПРЕДЕЛЕНИЯ	21
	ПРИЛОЖЕНИЕ 2. ЖИЗНЕННЫЙ ЦИКЛ ОС РУСИМ.....	25
	Перечень сокращений	29

1. ОБЩИЕ СВЕДЕНИЯ

- 1.1. Наименование программы: Программный комплекс «Операционная система РуСим».
- 1.2. Программа не требует для своего функционирования какого-либо специального или общесистемного программного обеспечения (далее – ПО).
- 1.3. Языки программирования

При разработке программы использованы следующие языки программирования, запросов, представления и визуального моделирования:

- язык программирования C;
- язык программирования Assembler для архитектуры ARM Cortex M, KMX32;
- среда разработки и отладки приложений Keil ARM, Eclipse, VS Code.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1. Программа предназначена для обеспечения работы USIM-карт в подвижной радиотелефонной связи (далее – ПРТС) стандартов 2G, 3G/LTE, 5G.

2.2. Программа обеспечивает решение следующих функциональных задач:
хранение идентификационной информации об учетной записи абонента;
идентификацию и аутентификацию абонента: установление подлинности USIM – карты в ПРТС стандартов 2G, 3G/LTE, 5G;
взаимодействие с мобильным терминалом (телефоном) и обмен данными с базовым оборудованием ПРТС стандартов 2G, 3G/LTE, 5G;
обеспечение конфиденциальности данных пользователя, шифрование и обеспечение целостности данных;
исполнение предоставляемых оператором приложений в соответствии со спецификацией SIM Toolkit (STK);
хранение и ведение телефонной книжки абонента;
хранение истории входящих и исходящих телефонных вызовов, а также SMS-сообщений абонента.

2.3. Программа является ПО, все компоненты которого должны устанавливаться («прошиваться») на SIM-карту при ее изготовлении.

2.4. Программа предназначена для использования в составе SIM-карты во всех областях ее применения.

2.5. Общие функциональные ограничения программы

2.5.1.1. Программа предоставляет инфраструктуру и средства для реализации прикладной функциональности на SIM-карте, в соответствии с требованиями и задачами конкретных операторов сотовой связи, которые с помощью аппаратных средств инициализации устанавливаются в SIM-карты при ее изготовлении.

2.5.1.2. Основной задачей программы, установленной на SIM-карту, является обеспечение надежного информационного обмена данными между абонентами сети и информационной системой операторов сотовой связи.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1. Структура программы

3.1.1. Программа является встраиваемой операционной системой USIM-карты (далее – ОС РуСим).

3.1.2. Программа является встраиваемой системой, выполнение функционала которой связано с правильной работой аппаратных средств SIM-карты, а именно микроконтроллера (МК). Применение программы без использования аппаратных средств SIM-карты является невозможным.

3.2. Встраиваемая ОС РуСим

3.2.1. ОС РуСим удовлетворяет требованиям спецификаций (и более новых ревизий), приведенных в таблице 1.

Таблица 1

№ п/п	Наименование спецификации
1.	ISO
1.1.	ISO 7816-3 2006
1.2.	ISO 7816-4 2013
1.3.	ISO 7816-5 2004
1.4.	ISO 7816-8 2004
1.5.	ISO 7816-9 2000
2.	ETSI
2.1.	TS 101.220 (v6.6.0, Rel-6): Application Identifiers for telecommunications
2.2.	TS 102.127 (v6.3.0, Rel-6): Transport Protocol for CAT applications; Stage 2
2.3.	TS 102.221 (v6.8.0, Rel-6): UICC-Terminal interface; Physical and logical characteristics

№ п/п	Наименование спецификации
2.4.	TS 102.222 (v6.8.0, Rel-6): Administrative Commands for telecommunications applications
2.5.	TS 102.223 (v9.6.0, Rel-9): Card Application Toolkit (CAT)
2.6.	TS 102.224 (v6.1.0, Rel-6): Security mechanisms for UICC based Applications Functional requirements
2.7.	TS 102.225 (v6.6.0, Rel-6): Secured packet structure for UICC applications
2.8.	TS 102.226 (v6.12.0, Rel-6): Remote APDU Structure for UICC based Applications
2.9.	TS 102.241 (v6.7.0, Rel-6): UICC Application Programming Interface (UICC API)
2.10.	TS 143.019 (v6.0.0, Rel-6): Digital cellular telecommunications system (Phase 2+)
3.	3GPP
3.1.	TS 23.040 (v6.5.0, Rel-6): Technical realization of the Short Message Service (SMS)
3.2.	TS 23.041 (v6.2.0, Rel-6): Technical realization of Cell Broadcast Service (CBS)
3.3.	TS 23.048 (v5.8.0, Rel-5): Security Mechanisms for the (U)SIM application toolkit; Stage 2
3.4.	TS 31.101 (v6.4.1, Rel-6): UICC-Terminal interface; Physical and Logical Characteristics
3.5.	TS 31.102 (v6.8.0, Rel-6): Characteristics of the USIM Application
3.6.	TS 31.103 (v6.6.0, Rel-6): Characteristics of the ISIM Application
3.7.	TS 31.111 (v6.4.0, Rel-6): USIM Application Toolkit (USAT)
3.8.	TS 31.115 (v6.2.0, Rel-6): Secured packet structure for (U)SIM Toolkit applications
3.9.	TS 31.116 (v6.3.0, Rel-6): Remote APDU Structure for (U)SIM Toolkit

№ п/п	Наименование спецификации
	applications
3.10.	TS 31.130 (v6.4.1, Rel-6): (U)SIM Application Programming Interface
3.11.	TR 31.900 (v6.0.0, Rel-6): SIM/USIM Internal and External Inter-working Aspects
3.12.	TS 33.102 (v6.3.0, Rel-6): 3G Security; Security architecture
3.13.	TS 35.205 (v6.0.0, Rel-6): Specification of the MILENAGE Algorithm Set
3.14.	TS 43.019 (v6.0.0, Rel-6): Subscriber Identity Module Application Programming Interface
3.15.	TS 51.011 (v4.13.0, Rel-4): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
3.16.	TS 51.014 (v4.5.0, Rel-4): Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
4.	OPEN GLOBAL PLATFORM
4.1.	Global Platform Card Specification 2.2 (with support of Multi Security Domains and Applications Extradition)
4.2.	Global Platform Card Specification v2.2 - Amendment B - Remote Application Management over HTTP
5.	JavaCard
5.1	Java Card Classic Platform Specification 3.0.4

3.2.2. ОС РуСим включает в себя следующие компоненты:

библиотека функций работы с памятью;
 функции поддержки физического уровня операций ввода-вывода;
 простейший остов для вызова событий из основного класса, реализованного байт-кодом языка высокого уровня;
 основной класс, реализованный байт-кодом языка высокого уровня;
 прочие библиотеки, использующиеся для наследования основного класса.

3.2.3. Библиотеки функций работы с памятью интегрированы с первичным программным обеспечением, предоставляемым непосредственно производителем МК. Они включены в пакет примеров, прилагаемых к спецификации и отладчику для конкретного МК.

3.2.4. Операции ввода-вывода выполнены на МК до физического уровня. Знание адресного пространства, где располагается буфер обмена, и сигнальных признаков событий получения байта реализует низкоуровневую функцию контроля ввода вывода, согласно установленному физическому протоколу. Протокол подробно описан в стандарте ISO7816-3. Это обычный последовательный полудуплексный канал с использованием переговоров о параметрах передачи вначале установления канала при подаче питания на МК.

На данном низком уровне обработка ввода-вывода необходима для проверки корректности протокола, проверки паритета и управления ожиданием. Вся обработка, начиная с канального уровня, происходит в пакетах библиотек, выполненных на байт-коде.

3.2.5. Диспетчер происходящих событий на низком уровне предназначен для передачи событий методу класса, выполненному на байт-коде. Данный компонент является надстройкой над обработчиком ввода вывода, обеспечивающую передачу входных данных и вызов методов-обработчиков событий основного класса. Чтобы обеспечить безошибочную диспетчеризацию, элемент остова имеет адресную таблицу расположения пакета основного класса и указатели на методы-обработчики событий в этом классе.

3.2.6. Архитектура МК исключает возможность использование динамической загрузки компонент в защищенную от записи область ROM (FLASH). Поэтому никакой угрозы функциональному ограничению такой подход не имеет. При подготовке ROM весь двоичный код образа уже связан адресами с вызовами внутри себя и исключает какое-либо динамическое переприсвоение.

3.2.7. Файловая структура ОС РуСим состоит из следующих типов файлов:

MF – главный файл (Master File);

DF – выделенный файл (Dedicated file);

ADF – выделенный файл приложения (Application Dedicated file);

TF – простой бинарный файл (Transparent File);

LF – линейный файл фиксированной длины (Linear Fixed File);

CF – циклический файл (Cyclic File);

LINK – ссылка на файл.

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

4.1. Условием работы программы является наличие технических (аппаратных) средств с параметрами, удовлетворяющими следующим требованиям:

микроконтроллер с ПЗУ не менее 20 кбайт и ОЗУ не менее 4096 байт;
интегральная схема карты с перезаписываемой памятью (ROM – ППЗУ)
размером не менее 132 кбайт.

4.2. Программа обеспечивает поддержку следующих аппаратных платформ в уточняемых конфигурациях:

Samsung SC000 ARM (TM) S3FW9Fx.

Samsung SC000 ARM (TM) S3D350A.

Huada CIU98288F, CIU98480H, CIU98M25.

TMC семейство THD89.

4.3. Программа не требует для своего функционирования какого-либо специального или общесистемного программного обеспечения.

4.4. Информация о технических средствах, обеспечивающих поддержание жизненного цикла.

4.4.1. Информация о технических средствах хранения исходного текста и объектного кода.

4.4.1.1. Для хранения исходного текста и объектного кода ПО «ОС РуСим» используется оборудование: ProLiant DL160 Gen9, инвентарные номера CZJ52106BY, CZJ0440CYS; ProLiant DL360 G7 инвентарный номер CZ2606008V.

4.4.1.2. Адрес нахождения технических средств хранения исходного текста и объектного кода ПО «ОС РуСим» - г. Москва, Мичуринский пр. 45.

4.4.2. Информация о технических средствах компиляции исходного текста в объектный код.

4.4.2.1. Для компиляции исходного текста в объектный код ПО «ОС РуСим» используется компилятор GCC, компилятор Clang, комплекта компилятора Keil со следующими компонентами:

– C Compiler: Armcc.exe V5.06 update 7 (build 960)

– Assembler: Armasm.exe V5.06 update 7 (build 960)

- Linker/Locator: ArmLink.exe V5.06 update 7 (build 960)
- Library Manager: ArmAr.exe V5.06 update 7 (build 960) Hex
- Converter: FromElf.exe V5.06 update 7 (build 960).

4.4.2.2. Адрес нахождения технических средств компиляции исходного текста в объектный код ПО «ОС РуСим» - г. Москва, Мичуринский пр. 45.

4.4.3. Информация о технических средствах, необходимых для активации, выпуска, распространения, управления лицензионными ключами на территории РФ.

4.4.3.1. Для активации, выпуска, распространения, управления лицензионными ключами на территории РФ ПО «ОС РуСим» используется оборудование: ProLiant DL160 Gen9, инвентарные номера CZJ52106BY, CZJ0440CYS; ProLiant DL360 G7 инвентарный номер CZ2606008V. с установленными компонентами компилятора, указанными в п.4.4.2.1.

4.4.3.2. Адрес нахождения технических средств, необходимых для активации, выпуска, распространения, управления лицензионными ключами ПО «ОС РуСим» - г. Москва, Мичуринский пр. 45.

5. ВЫЗОВ И ЗАГРУЗКА

5.1. Программа начинает функционировать при подаче напряжения питания и старте работы МК USIM-карты под управлением ОС РуСим, дополнительных действий для вызова программы не требуется.

6. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

6.1. Входными данными программы являются данные, получаемые ПК, установленным на SIM-карте, от ME по заранее определенным правилам. Данные правила должны соответствовать ГОСТ Р ИСО/МЭК 7816-3-2013 и ГОСТ Р ИСО/МЭК 7816-4-2013. Они определяются эмитентом карты.

6.2. Выходными данными программы являются ответы команд и возвращаемые ими данные ОС РуСим.

7. ИНСТАЛЛЯЦИЯ ПРОГРАММЫ

7.1. УСТАНОВКА НА СТАДИИ ПРОИЗВОДСТВА. Операционная система РуСим 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 загрузки ПО — запись на дальнейшие изменения блокируется. Установка программы производится путем загрузки образа (маски) ОС РуСим на интегральную схему в процессе изготовления (этап 5 жизненного цикла продукта – см. Приложение 2).

7.2. 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



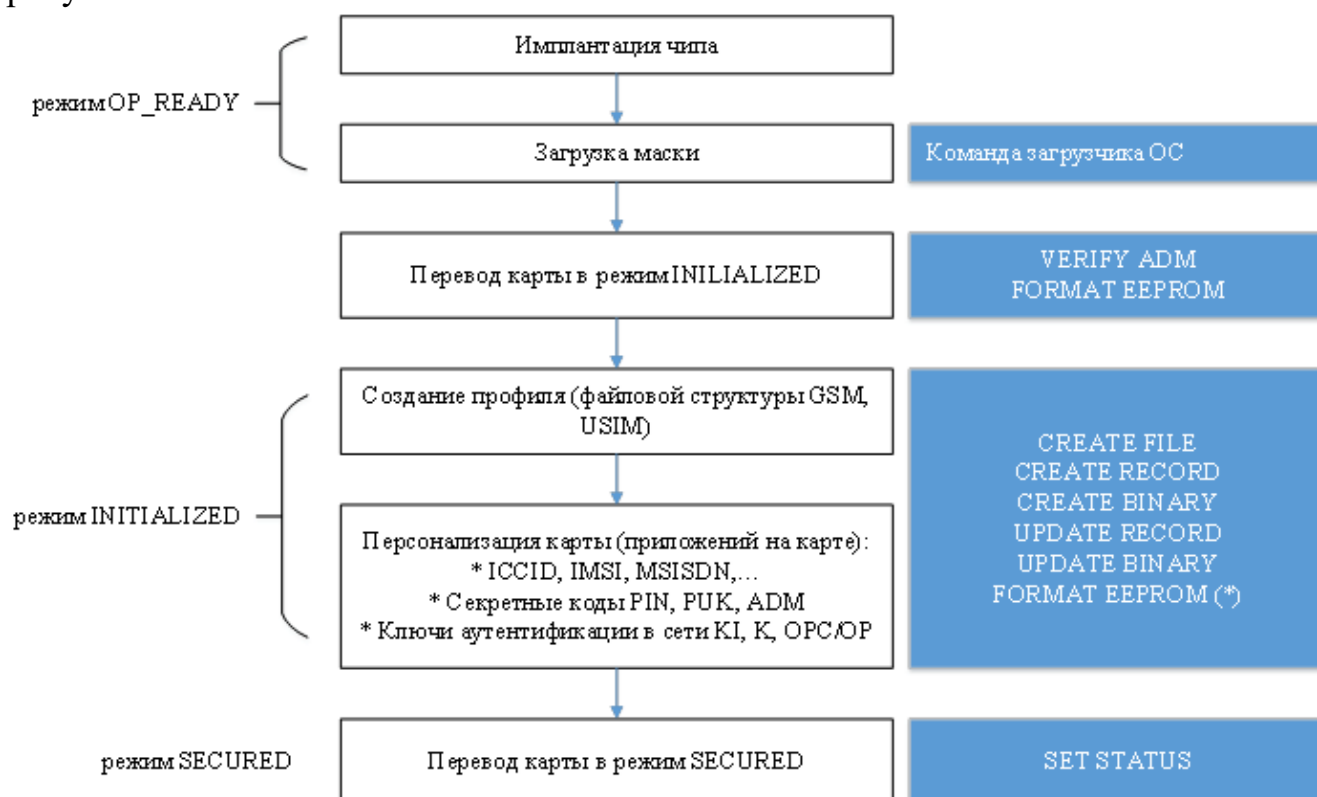
Рисунок 1. Схема загрузки

Основные шаги:

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

8. НАСТРОЙКА ПРОГРАММЫ

8.1. Порядок настройки программы описан в блок-схеме, представленной на рисунке 2.



(*) Команда позволяет начать процесс создания профиля и персонализации с начала.

Рисунок 2. Порядок настройки программы

9. ПРОВЕРКА ПРОГРАММЫ

9.1. Для проверки работоспособности программы на необходимо убедиться в том, что команда `VERIFY CODE` выполняется успешно.

9.2. Программа считается работоспособной, если команда `VERIFY CODE` выполняется успешно.

10.НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

10.1.Программа начинает функционировать при подаче напряжения питания и старте работы МК USIM-карты под управлением ОС РуСим, дополнительных действий для вызова программы не требуется.

11. ВЫПОЛНЕНИЕ ПРОГРАММЫ

11.1. Общие сведения о работе с программой

11.1.1 Запуск программы

Программа начинает функционировать при подаче напряжения питания и старте работы МК USIM-карты под управлением ОС РуСим, дополнительных действий для вызова программы не требуется.

11.1.2 Завершение работы с программой

Завершение работы программы происходит при прерывании питания карты USIM с ОС РуСим.

ПРИЛОЖЕНИЕ 1. ОПРЕДЕЛЕНИЯ

3G доступ (3G access)	Субъект доступа – приложения, базирующиеся на спецификации UICC (3G-приложения, такие как USIM, ISIM, фреймворк), или приложения, базирующиеся на API UICC.
APDU (Application Protocol Data Units)	Стандартный коммуникационный протокол обмена сообщениями между устройством считывания карт (ME) и смарт-картой (карта USIM).
Приложение (Application)	Приложение состоит из набора механизмов безопасности, файлов, данных и протоколов (за исключением протоколов передачи).
Выдача приложения (Application Extradition)	Процесс, позволяющий приложению, ассоциированному с одним доменом безопасности, ассоциироваться с другим доменом безопасности.
Провайдер приложения (Application Provider)	Владелец приложения, ответственный за его функционирование.
Асимметричное шифрование (Asymmetric Cryptography)	Метод шифрования, использующий два взаимосвязанных преобразования: публичное преобразование (определяемое компонентом публичного ключа) и закрытое преобразование (определяемое компонентом секретного ключа); эти два компонента имеют следующее свойство: невозможно вычислить закрытый ключ, даже если известен публичный ключ.
Сессия карты (Card Session)	Связь между картой и внешним миром, начинающаяся с ATR и оканчивающаяся последующей перезагрузкой или выключением карты.
Держатель карты (Cardholder)	Конечный пользователь карты.
Card Manager	Общий термин для трех органов управления картой GlobalPlatform: OPEN, Issuer Security Domain и Cardholder Verification Method Services provider.
Открытый текст (Clear Text)	Незашифрованная информация.
Криптограмма (Cryptogram)	Результат операции шифрования.
Криптографическая контрольная сумма (Cryptographic	Преобразование данных методом симметричного шифрования, обеспечивающее проверку подлинности источника данных и их целостность.

Checksum)	
Шаблон проверки подлинности данных, DAP (Data Authentication Pattern)	Используется для проверки подлинности источника и целостности данных; например, DAP может быть MAC, если используется метод симметричного шифрования, или электронной подписью, если используется метод асимметричного шифрования, или хешем для проверки целостности информации.
Объект данных (Data Object)	Информация, видимая на интерфейсе, состоящая из тега, длины и значения; объекты данных также называются объектами данных BER-TLV, COMPACT-TLV и SIMPLE-TLV.
Каталог карты (Dedicated File)	Файл, содержащий условия доступа и, опционально, элементарные (простые) файлы или другие каталоги.
Электронная подпись (Digital Signature)	Преобразование данных методом асимметричного шифрования, позволяющее получателю доказать происхождение и целостность данных; электронная подпись защищает отправителя и получателя от подделки данных третьими лицами; она также защищает от подделки отправителя получателем.
Элементарный (простой) файл (Elementary File)	Файл, содержащий условия доступа и данные, но не другой файл.
Параметры управления файлами (File Control Parameters)	Логические, структурные атрибуты а также атрибуты безопасности файла.
Файловый идентификатор (File Identifier)	Двухбайтный идентификатор файла.
Домен безопасности эмитента (Issuer Security Domain)	Объект карты, обеспечивающий выполнение требований контроля, безопасности и защиты коммуникации карты.
Файл загрузки (Load File)	Файл, переданный на карту GlobalPlatform, содержащий блок данных файла загрузки и, возможно, один или более блоков DAP.
Блок данных файла загрузки (Load File Data Block)	Часть файла загрузки, содержащая одно или более приложений, а также библиотеки или информацию по поддержке приложения(-ий) в соответствии с требованиями определенной платформы.

Хеш блока данных файла загрузки (Load File Data Block Hash)	Значение целостности блока данных файла загрузки.
Подпись блока данных файла загрузки (Load File Data Block Signature)	Значение, включающее хеш блока данных файла загрузки, и обеспечивающее целостность и подлинность блока данных файла загрузки.
Код проверки подлинности сообщения, MAC (Message Authentication Code)	Преобразование данных методом симметричного шифрования, обеспечивающее проверку подлинности источника данных и их целостность.
Корневой каталог (Master File)	Обязательный уникальный каталог карты, представляющий собой корень файловой структуры.
Многофункциональная карта (Multi-application card)	Карта, на которой может быть выбрано более одного приложения/приложения Toolkit.
Многосесссионная карта (Multi-session card)	Карта, поддерживающая более одной текущей сессии приложения во время сессии карты.
Предок (Parent File)	Каталог карты, предшествующий файлу в иерархии.
Путь (Path)	Конкатенация файловых идентификаторов.
Post-Issuance	Этап после выдачи карты держателю.
Pre-Issuance	Этап до выдачи карты держателю.
Контроль избыточности (Redundancy Check)	Преобразование данных, позволяющий получателю проверить целостность данных без использования секретного ключа.
SIM Application Toolkit	Набор приложений и связанных процедур, которые могут быть использованы в GSM-сессии.
Защищенный канал (Secure Channel)	Механизм коммуникации между объектом вне карты и картой, обеспечивающий уровень надежности для одной или обеих сторон.
Сессия защищенного канала (Secure Channel Session)	Сессия во время сессии приложения, начинающаяся с установления защищенного канала и оканчивающаяся закрытием защищенного канала или закрытием сессий приложения/карты.
Домен безопасности (Security Domain)	Объект карты, обеспечивающий выполнение требований контроля, безопасности и коммуникации провайдера приложения.
Выбираемое	Приложение, которое может быть выбрано по AID

приложение (Selectable application)	посредством интерфейса ME-UICC в соответствии с процессами, описанными в ISO/IEC 7816-4.
Сессия выбираемого приложения (Selectable application session)	Связь между приложением и внешним миром во время сессии карты, начинающаяся с выбора приложения и оканчивающаяся отменой выбора или окончанием сессии карты.
Симметричное шифрование (Symmetric Cryptography)	Метод шифрования, использующий одинаковый секретный ключ для преобразований на стороне отправителя и на стороне получателя; без знания секретного ключа затруднительно вычислить преобразования отправителя/получателя.
Временные объекты JCRE Entry Point (Temporary JCRE Entry Point Objects)	Часть объектов Java Card Runtime Environment Entry Point, защищенных от несанкционированного повторного использования (например, объект APDU, исключения JCRE). В переменных класса, переменных экземпляра или компонентах массива не могут храниться ссылки на эти объекты.
USIM Application Toolkit	Набор приложений и связанных процедур, которые могут быть использованы в USIM-сессии.
Сессия USIM (USIM Session)	USIM-сессия – сессия выбираемого приложения.

ПРИЛОЖЕНИЕ 2. ЖИЗНЕННЫЙ ЦИКЛ ОС РУСИМ

Жизненный цикл ОС РуСим является частью жизненного цикла продукта, т. е. карты (U)SIM – от стадии разработки до использования абонентом (Таблица П1).

Инсталляция ОС РуСим осуществляется на стадии (этап 5, таблица П1) при производстве SIM-карты, при этом результат на этой стадии – инициализированная SIM-карта.

Таблица П1

№этапа ЖЦ¹	Применяемый микроконтроллер – (ИС²)	Разрабатываемый ПК ОС РуСим - (U)SIM - платформа³	Интегрированный продукт сим-карта⁴
Этап 1	Разработка прошивки (ВПО) ИС	Разработка (проектирование) ОС	Разработка (проектирование) ВПО ⁵ для ИС
Этап 2	Разработка ИС (проектирование, разработка структуры, логической и (или) электрической принципиальной схемы ИС, топологии ИС)	Осуществление доставки образа разработанной (U) SIM платформы на производство.	Разработка ИС (проектирование, разработка структуры, логической и (или) электрической принципиальной схемы ИС, топологии ИС)
Этап 3	Производство ИС (полный цикл от пластины к кристаллу)	Хранение файлов разработчика (U) SIM – платформы на производстве, подготовка к персонализации,	Производство ИС (полный цикл от пластины к кристаллу)

1 ЖЦ – жизненный цикл.

2 ИС - интегральная схема.

3 (U)SIM – встроенное в сим-карту ПО, предназначенное для использования в мобильном телефоне или любом другом мобильном устройстве для предоставления сервисов конечному пользователю (абоненту).

4 Интегрированный продукт сим-карта включает в себя ИС с установленным на нее ВПО.

5 ВПО - встроенное программное обеспечение (Chip firmware, OS, applets, user code).

		тестирование (U)SIM - платформы	
Этап 4	Упаковка ИС (корпусирование)	Хранение файлов разработчика (U) SIM – платформы на производстве, подготовка к персонализации, тестирование (U)SIM - платформы	Упаковка ИС (сборка кристаллов в корпусе)
Этап 5	Сборка ИС, ВПО, (U)SIM - платформы	(U)SIM – платформа устанавливается в сим-карту	Инициализация сим-карты. Комплектация составного продукта (внедрение компонентов программного обеспечения в ИС)
Этап 6	Персонализация (Сборка ИС, ВПО, (U)SIM – платформы, данных оператора - эмитента)	Персонализация (U)SIM – платформы. В инициализированную сим-карту дополнительно внедряются данные оператора, подписка на услуги и т.п.	Персонализация продукта, предшествующая его использованию (внедрение данных эмитента или оператора)
Этап 7	Эксплуатация ИС в составе SIM-карты	Эксплуатация (U)SIM – платформы в составе сим-карты	Эксплуатация
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.

Устранение неисправностей. ОС представляет из себя ПО для встраиваемых систем с высоким уровнем защиты. В основу ее архитектуры безопасности, заложена концепция, что будучи загруженной на целевое устройство (например смарт-карту), внесение каких-либо изменений в последующем недопустимы. В этой связи, непосредственно перед применением на целевых устройствах, ОС проходит многоуровневую процедуру проверки на соответствие стандартам и требованиям.

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

Соответственно, если в процессе эксплуатации обнаружится ошибка, то внести изменения не получится, и целевое устройство придется изъять и заменить на другое, содержащее корректную версию ОС.

ПОДДЕРЖКА ОС РУСИМ

Техническая поддержка. В рамках технической поддержки ОС РуСим обеспечивает вторую и третью линию технической поддержки и осуществляется две основные активности:

- Предварительная консультация заказчиков по вопросам совместимости, конфигурирования и возможности персонализации ОС РуСим.
- Сопровождение выпущенных продуктов на базе ОС РуСим, в области их переконфигурирования в процессе работы.

Первая линия технической поддержки осуществляется заводами производителями конечных продуктов.

Модернизация ПО. Исправление замечаний, а также дополнение ОС новым функционалом осуществляется в итеративном порядке, по мере поступления таких запросов от клиентов, либо если они возникают как дополнение к существующим стандартам и требованиям. Данной работой занят весь штат разработчиков компании.

ЦИКЛ РАЗРАБОТКИ ОС РУСИМ

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

Ключевыми точками формирования релиза является:

- Портинг 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 конфигураций ОС РуСим
- Автоматическое тестирование в режимах эмуляции окружения

- Автоматическое тестирование на реальном оборудовании
- Информирование о возникших проблемах.

По результирующему отчёту принимается решение о достижении 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
МЕ (Mobile Equipment)	– мобильное устройство