ОС РуСим

Описание программы.

ТРБП.10002-01

Листов 26

АННОТАЦИЯ

Настоящий документ является описанием программного комплекса (далее – ПК) «Операционная система РуСим» ТРБП.10002-01 («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 7
4. Используемые технические средства 11
5. Вызов и загрузка 12
6. Входные и выходные данные 13
7. Инсталляция программы 14
8. Настройка программы 15
9. Проверка программы 16
10. Начало работы с программой 17
11. Выполнение программы 18
Приложение 1. Определения 19
Приложение 2. Жизненный цикл ОС РуСИМ 23
Перечень сокращений 26

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование и обозначение программы.

Наименование программы: Программный комплекс «Операционная система РуСим».

Обозначение программы: ТРБП.10002-01.

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.

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 инсталлироваться («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. 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 инсталлируются в SIM-карты при ее изготовлении.

2.5.2. 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 системы USIM-карты (далее – ОС USIM).

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 USIM

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

Таблица 1

№ п/п	**Наименование спецификации**
1.	**ETSI**
1.1.	TS 101.220 (v6.6.0, Rel-6): Application Identifiers for telecommunications
1.2.	TS 102.127 (v6.3.0, Rel-6): Transport Protocol for CAT applications; Stage 2
1.3.	TS 102.221 (v6.8.0, Rel-6): UICC-Terminal interface; Physical and logical characteristics
1.4.	TS 102.222 (v6.8.0, Rel-6): Administrative Commands for telecommunications applications
1.5.	TS 102.225 (v6.6.0, Rel-6): Secured packet structure for UICC applications
1.6.	TS 102.226 (v6.12.0, Rel-6): Remote APDU Structure for UICC based Applications
1.7.	TS 102.241 (v6.7.0, Rel-6): UICC Application Programming Interface (UICC API); UICC API for Java Card™
1.8.	TS 143.019 (v6.0.0, Rel-6): Digital cellular telecommunications system

№ п/п	Наименование спецификации
	(Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API) for Java Card; Stage 2 (3GPP TS 43.019)
2.	**3GPP**
2.1.	TS 23.040 (v6.5.0, Rel-6): Technical realization of the Short Message Service (SMS)
2.2.	TS 23.041 (v6.2.0, Rel-6): Technical realization of Cell Broadcast Service (CBS)
2.3.	TS 23.048 (v5.8.0, Rel-5): Security Mechanisms for the (U)SIM application toolkit; Stage 2
2.4.	TS 31.101 (v6.4.1, Rel-6): UICC-Terminal interface; Physical and Logical Characteristics
2.5.	TS 31.102 (v6.8.0, Rel-6): Characteristics of the USIM Application
2.6.	TS 31.103 (v6.6.0, Rel-6): Characteristics of the ISIM Application
2.7.	TS 31.111 (v6.4.0, Rel-6): USIM Application Toolkit (USAT)
2.8.	TS 31.115 (v6.2.0, Rel-6): Secured packet structure for (U)SIM Toolkit applications
2.9.	TS 31.116 (v6.3.0, Rel-6): Remote APDU Structure for (U)SIM Toolkit applications
2.10.	TS 31.130 (v6.4.1, Rel-6): (U)SIM Application Programming Interface; (U)SIM API for Java™ Card
2.11.	TR 31.900 (v6.0.0, Rel-6): SIM/USIM Internal and External Inter-working Aspects
2.12.	TS 33.102 (v6.3.0, Rel-6): 3G Security; Security architecture
2.13.	TS 35.205 (v6.0.0, Rel-6): Specification of the MILENAGE Algorithm Set
2.14.	TS 43.019 (v6.0.0, Rel-6): Subscriber Identity Module Application Programming Interface; (SIM API) for Java Card™; Stage 2
2.15.	TS 51.011 (v4.13.0, Rel-4): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface

№ п/п	Наименование спецификации
2.16.	TS 51.014 (v4.5.0, Rel-4): Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
3.	**OPEN GLOBAL PLATFORM**
3.1.	Global Platform Card Specification 2.1.1 (with support of Multi Security Domains and Applications Extradition)

3.2.2. ОС USIM 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 надстройка 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 USIM состоит из следующих типов файлов:

MF – главный файл (Master File);

DF – выделенный файл (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;

– KMXSCE производства KM211;

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

5. ВЫЗОВ И ЗАГРУЗКА

5.1. Программа начинает функционировать при подаче напряжения питания и старте работы МК USIM-карты под управлением ОС USIM, 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.

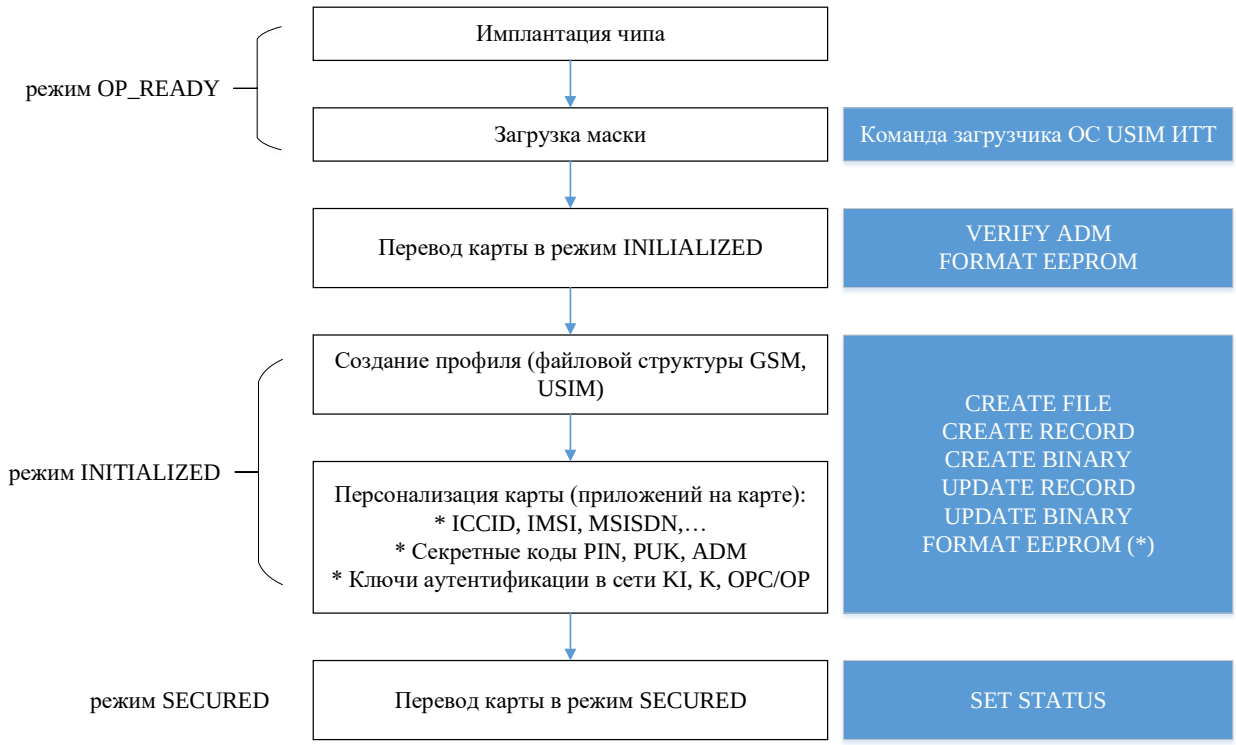
6.2. Выходными данными программы являются ответы команд и возвращаемые ими данные ОС USIM.

7. ИНСТАЛЛЯЦИЯ ПРОГРАММЫ

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

8. НАСТРОЙКА ПРОГРАММЫ

8.1. Порядок настройки программы описан в блок-схеме, представленной на рисунке 1.



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

Рисунок 1

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 USIM, дополнительных действий для вызова программы не требуется.

11.ВЫПОЛНЕНИЕ ПРОГРАММЫ

11.1.Общие сведения о работе с программой

11.1.1Запуск программы

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

11.1.2 Завершение работы с программой

Завершение работы программы происходит при прерывании питания карты USIM 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	Значение целостности блока данных файла загрузки.

File Data Block Hash)	
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.
Многосессионная 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 могу 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 (Selectable application)	Приложение, которое может быть выбрано по AID посредством интерфейса ME-UICC в соответствии с процессами, описанными в ISO/IEC 7816-4.
Сессия выбираемого	Связь между приложением и внешним миром во

приложения (Selectable application session)	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 сим- карта.

Таблица П1

№этапа ЖЦ[1]	**Интегрированный продукт сим-карта[2]**	**Применяемый микроконтроллер – (ИС[3])**	**Разрабатываемый ПК ОС РуСим - (U)SIM - платформа[4]**
Этап 1	Разработка (проектирование) ВПО[5] 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 (U) SIM платформы на производство.
Этап 3		Производство ИС (полный цикл от пластины к кристаллу)	Хранение файлов разработчика (U) SIM – платформы на производстве, подготовка к персонализации, тестирование (U)SIM - платформы
Этап 4		Упаковка ИС (корпусирование)	Хранение файлов разработчика (U) SIM – платформы на производстве, подготовка к персонализации,

1 ЖЦ – жизненный цикл.

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

3 ИС - интегральная схема.

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

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

			тестирование (U)SIM - платформы
Этап 5	Инициализация сим-карты. Комплектация составного продукта (внедрение компонентов программного обеспечения в ИС)	Сборка ИС, ВПО, (U)SIM - платформы	(U)SIM – платформа инсталлируется в сим-карту
Этап 6	Персонализация продукта, предшествующая его использованию (внедрение данных эмитента или оператора)	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.
Этап 7	Эксплуатация	Эксплуатация ИС в составе сим-карты	Эксплуатация (U)SIM – платформы в составе сим-карты
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.

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