

# РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Операционная система смарт-карты (UICC/SIM/USIM/ISIM)

## «Операционная система N\_Sim 2.0»

### 1. Общие сведения

Настоящее руководство пользователя предназначено для описания порядка получения, установки (загрузки) и использования программного обеспечения «Операционная система N\_Sim 2.0» (далее - ПО, ОС смарт-карты, COS).

Документ подготовлен в составе комплекта материалов для регистрации ПО в реестре российского программного обеспечения (Минцифры России).

#### 1.1. Назначение документа

Руководство описывает типовые сценарии работы с ОС смарт-карты на этапах производства, персонализации и эксплуатации UICC/SIM/USIM/ISIM.

#### 1.3. Термины и сокращения

Термины и сокращения, используемые в документе (пример; откорректировать под вашу реализацию):

Термин	Определение
APDU	команда/ответ по ISO/IEC 7816-4.
COS	Card Operating System, операционная система смарт-карты.
UICC	универсальная интегральная карта (SIM/USIM/ISIM).
EF/DF/MF	элементарный/директория/мастер-файл файловой системы UICC.
SCP	Secure Channel Protocol (защищенный канал администрирования по GlobalPlatform).
OTA	over-the-air управление приложениями/параметрами по сети оператора (при наличии).
PIN/ADM	коды доступа пользователя/администратора (если используется модель PIN/ADM).

## 2. Описание ПО

ПО «Операционная система N\_Sim 2.0» предназначено для выполнения функций операционной системы смарт-карты (UICC) и обеспечивает выполнение команд APDU, хранение и обработку данных в защищенной области памяти карты, а также применение политик безопасности.

Ниже приведен пример перечня функций. Оставьте только те, которые фактически реализованы и входят в состав поставки:

- поддержка протокола обмена и командного интерфейса ISO/IEC 7816-4;
- поддержка файловой системы UICC (MF/DF/EF), включая операции выбора, чтения и обновления записей/байтов;
- механизмы контроля доступа (PIN/PUK/ADM/ключи домена) и разграничение прав;
- криптографические сервисы (при наличии): симметричное шифрование, MAC, хэширование, генерация случайных чисел;
- поддержка приложений (при наличии): Java Card и управление их жизненным циклом;
- администрирование через защищенный канал (при наличии): GlobalPlatform SCP02/SCP03 или иной протокол;
- поддержка профилей SIM/USIM/ISIM и процедур аутентификации в сети (при наличии и в рамках применимых спецификаций).

## 4. Требования к рабочему месту и инфраструктуре

### 4.1. Аппаратные требования

Минимальные требования:

- ПК (x86) с USB 2.0/3.0;
- ридер смарт-карт с поддержкой PC/SC (контактный) либо соответствующий программатор/персонализационное оборудование;

### 4.2. Программные требования

Минимальные требования:

- драйверы PC/SC для ридера;
- инструмент отправки APDU (например, собственная утилита правообладателя или сторонние средства персонализации);

## 5. Получение проверочного экземпляра

Предоставляется комплект ПО для загрузки ОС:

- Программа загрузчик;
- Скрипт(последовательность команд) с загружаемой ОС;
- Руководство по загрузке ОС

## 6. Типовые сценарии использования

### 6.1. Инициализация и персонализация (пример)

Сценарий применяется при подготовке смарт-карт к выдаче сотовому оператору (заказчику) и включает:

- загрузку ОС;
- создание файловой структуры MF/DF/EF согласно выбранному профилю UICC;
- запись персональных данных и параметров профиля (например, идентификаторов, сервисных параметров);
- установку административных ключей/кодов (PIN/PUK/ADM) и политик доступа;

Конкретный состав EF/DF и атрибуты доступа определяются техническим заданием от заказчика.

### 6.2. Администрирование через защищенный канал (при наличии)

Операции загрузки приложений и изменения критичных параметров выполняются только после установления защищенного канала (SCP, OTA).

Типовой порядок действий:

1. установление защищенного канала (обмен вызов-ответ, генерация сессионных ключей, включение шифрования и/или MAC);
2. выполнение административных команд (загрузка/установка/удаление приложений, смена ключей и т.д.);

### 6.3. Управление приложениями

Типовые операции включают:

- загрузку пакета приложения;
- установку экземпляра приложения и инициализацию параметров;
- управление жизненным циклом (активация/деактивация/удаление);
- контроль прав доступа приложений к данным/файлам.

### 6.4. Поддержка аутентификации в сети

При использовании смарт-карты в сети оператора ОС может обеспечивать выполнение алгоритмов аутентификации и производных криптографических функций в соответствии с профилем SIM/USIM/ISIM.

Возможные варианты (пример; оставить применимые):

- Milenage (3G/4G AKA) с соответствующими параметрами (K, OP/OPc и т.д.);
- национальные алгоритмы (например, S3G);
- генерация и хранение ключевых материалов в защищенной памяти карты;

- защита персонализационных параметров и ограничение доступа к ним.

## 7. Требования информационной безопасности

- выполнение административных операций только через защищенный канал;
- политики управления PIN/ADM (число попыток, блокировка, разблокировка).

## 8. Диагностика и устранение неисправностей

При возникновении ошибок рекомендуется фиксировать:

- полный протокол обмена APDU (команды и ответы);
- имя продукта и идентификатор карты;
- условия воспроизведения (ридер, ОС ПК, версия утилиты);

### 8.1. Типовые статусы ISO/IEC 7816-4

Ниже приведены часто встречающиеся коды статуса (не являются исчерпывающим перечнем):

SW1 SW2	Смысл
9000	Успех.
6A82	Файл/объект не найден.
6982	Условия безопасности не выполнены (недостаточно прав/не пройдена проверка).
6700	Неверная длина/формат команды.
6D00	Команда не поддерживается.
6E00	Неверный CLA (класс команды).

## Приложение А. Перечень применимых стандартов и документов

- ISO/IEC 7816;
- ETSI/3GPP спецификации UICC/SIM/USIM/ISIM;
- GlobalPlatform Card Specification и Secure Channel Protocol;