

Описание функциональных характеристик

Программное обеспечение «Операционная система N_Sim 2.0»

1. Назначение ПО и решаемые задачи

Программное обеспечение (ПО) «Операционная система N_Sim 2.0» представляет собой операционную систему, предназначенную для обеспечения функционирования идентификационных модулей абонента (UICC) в сетях мобильной связи (2G, 3G, 4G/LTE, 5G), а также в устройствах промышленного интернета вещей (M2M/IoT).

Основные задачи, решаемые ПО:

- **Идентификация и аутентификация:** обеспечение защищенного доступа абонента к услугам сетей связи оператора в соответствии с международными протоколами (3GPP TS 33.102 и др.).
- **Обеспечение безопасности данных:** защита критически важной информации чувствительной информации от несанкционированного доступа, клонирования и физических атак на микроконтроллер.
- **Управление жизненным циклом приложения:** поддержка управления (установка/удаление) приложениями (Java-приложения) для предоставления дополнительных сервисов.
- **Дистанционное управление (ОТА):** обеспечение возможности удаленного обновления содержимого сим-карты без физической замены носителя.
- **Интеграция с устройствами:** обеспечение протокольного взаимодействия между смарт-картой и терминальным устройством (смартфоном, модемом, IoT-датчиком).

2. Функциональные характеристики ПО

Операционная система «N_Sim 2.0» обладает следующей функциональностью:

2.1. Управление файловой системой:

- Поддержка иерархической структуры файлов в соответствии со стандартом ISO/IEC 7816-4 (MF, DF, EF).
- Разграничение прав доступа к файлам на основе гибких политик безопасности (PIN-коды, административные ключи).

2.2. Криптографическая защита:

- Реализация алгоритмов симметричного и асимметричного шифрования (AES, DES/3DES, RSA).
- Поддержка специализированных алгоритмов аутентификации абонентов (Milenage, Туак и др.).
- Генерация аппаратных случайных чисел (TRNG) для формирования сессионных ключей.

2.3. Среда исполнения приложений (Runtime Environment):

- Поддержка платформы Java Card, позволяющая исполнять загружаемые апплеты и обеспечивать их изоляцию на карте за счёт механизма Java Card firewall и контролируемого межапплетного взаимодействия.
- Поддержка набора команд USAT (USIM Application Toolkit) для инициации действий со стороны карты (вывод сообщений на экран, отправка SMS, управление вызовами).

2.4. Коммуникационные интерфейсы и протоколы:

- Поддержка протоколов передачи данных T=0 и T=1.
- Совместимость с контактными (ISO/IEC 7816) и бесконтактными (ISO/IEC 14443) интерфейсами.
- Поддержка защищенных каналов передачи данных (SCP02/SCP03) по стандартам GlobalPlatform.

3. Затрачиваемые ресурсы, входные и выходные данные

3.1. Технические требования к аппаратным ресурсам:

ПО предназначено для работы на микроконтроллерах смарт-карт (Secure Elements), обладающих следующими минимальными характеристиками:

- **Энергонезависимая память (NVM/Flash/EEPROM):** от 64 Кб (для хранения ОС, файловой системы и апплетов).
- **Оперативная память (RAM):** от 2 Кб (для работы стека протоколов и выполнения криптографических вычислений).
- **Процессор:** 8/16/32-битное ядро с поддержкой аппаратного ускорения криптографии.

3.2. Входные данные:

- Команды в формате APDU (Application Protocol Data Unit) по стандарту ISO/IEC 7816-4.

- Входящие бинарные SMS-сообщения (в рамках OTA-управления).

3.3. Выходные данные:

- Ответы на APDU-команды (статусные слова и данные).
- Результаты вычисления алгоритмов аутентификации (SRES, RES, Kc, CK, IK) и иные данные.
- Команды управления терминалом (Proactive Commands) в рамках USAT-сервисов.

4. Особенности реализации и преимущества

- **Гибкость настройки:** возможность тонкой настройки конечных продуктов под требования заказчиков (операторов связи).
- **Безопасное обновление в защищенных криптографией режимах :**
 - обновлять можем содержимое файлов
 - создавать/удалять файлы
 - устанавливать/удалять приложения
- **Надежность:** реализованы механизмы атомарности операций (защита от разрыва питания во время записи данных) и контроля износа ячеек памяти (Wear Leveling).