АКЦИОНЕРНОЕ ОБЩЕСТВО
«АЛАДДИН Р.Д.»

УТВЕРЖДЕН
RU.АЛДЕ.02.13.022-02 32 01- ЛУ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ «TRUSTED SECURITY MODULE» ДЛЯ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА «ДОВЕРЕННАЯ ПЛАТФОРМА» НА БАЗЕ ARM-ПРОЦЕССОРОВ

Руководство системного программиста
(Руководство по установке)

RU.АЛДЕ.02.13.022-02 32 01

Листов 12

2020

Литера_____

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

АННОТАЦИЯ

В данном руководстве приведено описание производственных процедур для генерации, установки и настройки программного изделия «Средство доверенной загрузки «Trusted Security Module» для программно-аппаратного комплекса «Доверенная платформа» на безе ARM-процессоров (далее по тексту - СДЗ «TSM»).

Ввиду сложности установки СДЗ «TSM» целевая аудитория данного руководства, сотрудники компании-производителя, отвечающие за установку СДЗ «TSM» на программно-аппаратный комплекс.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ ОБ СДЗ «TSM»

1.1. Назначение программы

СДЗ «TSM» является средством доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты и применяется в информационных системах, в которых обрабатывается информация, содержащая «совершенно секретно» сведения, а также в государственных информационных системах и в информационных системах обработки персональных данных.

СДЗ «TSM» получает монопольный контроль над процессом загрузки СВТ непосредственно после подачи питания, препятствует загрузке нештатной ОС или других нештатных средств загрузки СВТ.

СДЗ «TSM» предназначено для работы в СВТ на ARM-микропроцессорах семейства i.MX6 производства компании NXP.

1.2. Предотвращаемые угрозы

СДЗ «TSM» предназначено для защиты СВТ от следующих угроз безопасности:

1. Несанкционированный доступ к информации за счет загрузки нештатной ОС, в обход правил разграничения доступа штатной ОС и (или) других СЗИ, работающих в среде штатной ОС;
2. Несанкционированную загрузку штатной ОС и получение несанкционированного доступа к информационным ресурсам;
3. Нарушение целостности программной среды СВТ и (или) состава компонентов аппаратного обеспечения СВТ;
4. Нарушение целостности программного обеспечения СДЗ «TSM»;
5. Отключение и (или) обход нарушителями СДЗ «TSM»;
6. Несанкционированное изменение конфигурации (параметров) СДЗ «TSM»;
7. Преодоление или обход функций безопасности СДЗ «TSM»;
8. Получение остаточной информации СДЗ «TSM» из памяти СВТ после завершения работы СДЗ «TSM»;
9. Получение доступа к ресурсам СДЗ «TSM» из программной среды СВТ после завершения работы средства доверенной загрузки.

1.3. Функции программы

1) Аутентифицирует пользователя до загрузки ОС, по паролю или по паролю и токену;
2) Разграничивает доступа к СДЗ «TSM» на уровне ролей

администратор/пользователь;

3) Осуществляет доверенную загрузку ОС общего назначения и блокировку загрузки нештатной ОС;
4) Обеспечивает автоматическое реагирование на нарушения ФБ путем блокирования загрузки ОС, блокировании учетной записи пользователя, ведения журнала аудита;
5) Обеспечивает управление параметрами СДЗ и режимами функций безопасности через графический интерфейс управления;
6) Контролирует целостности файловых систем ОС и других данных пользователей;
7) Регистрирует события безопасности в журнале аудита безопасности;
8) Производит самотестирование СДЗ “TSM”;
9) Осуществляет контроль состава аппаратной платформы (привязка к микропроцессору и носителю данных).

СДЗ «TSM» доверено загружает любую ОС общего назначения, работающую на ARM-процессорах, в том числе ОС Linux (Debian, Ubuntu, Astra Linux и др.), Android, Sailfish и другие.

СДЗ «TSM» может встраиваться в уже работающие системы, наделяя их дополнительными возможностями по обеспечению информационной безопасности.

1.4. Требования к характеристикам аппаратной платформы

Программно-аппаратный комплекс (далее по тексту ПАК), на который устанавливается СДЗ “TSM” может быть в виде модуля РЭС, ячейки РЭС, блока РЭС или устройства РЭС[1] и должен удовлетворять следующим техническими характеристикам:

- один из процессоров: i.MX6 Solo, i.MX6 DualLite, i.MX6 Dual, i.MX6 Quad;
- объем ОЗУ (DDR) от 128 Мбайт до 4 Гбайт;
- объем ПЗУ от 1 до 4 Гбайт (определяется размером файловой системы применяемой пользователем ОС);
- тип ПЗУ - SD/microSD-карта или eMMC (микросхема);

[1] Термины модуль РЭС, ячейка РЭС, блок РЭС и устройство РЭС даны по ГОСТ Р 52003-2003

- интерфейс USB 2.0 (тип A/B) для подключения устройства ввода – манипулятора мышь (в случае отсутствия сенсорной панели) и токена;
- Одна из комбинаций устройства ввода-вывода:
    1) интерфейс HDMI для подключения дисплея + манипулятор мышь;
    2) LVDS либо параллельный интерфейс для подключения дисплея + i2C интерфейс для подключения сенсорного экрана.
- часы реального времени со стационарным питанием (от батарейки);
- сетевой интерфейс Ethernet и/или Wi-Fi и/или 3G/4G (для обеспечения процедур обновления и удаленного управления);
- интерфейс JTAG (опционально).

1.5. Состав дистрибутива СДЗ «TSM» и носитель данных

В таблице 1 ниже приведен состав инсталлируемых файлов СДЗ «TSM»

№	**Компонент разрабатываемого образца**	**Имя файла**	**Раздел на загрузочном носителе (EMMC микросхема)**
1	СПО «Доверенный загрузчик»;	boot.sbin	1-ый раздел - FAT16/FAT32
2	Параметры СПО «Доверенный загрузчик»	par[N].sbin	
3	СПО «Компонент СДЗ»;	sdz.sbin	
4	СПО «Доверенная среда исполнения»;	tee.sbin	

2. УСТАНОВКА И НАСТРОЙКА СДЗ «TSM»

Установка и настройка программных компонентов СДЗ “TSM” заключается в проведении корректной установки дистрибутива на ПАК с использованием специального автоматизированного рабочего места (далее по тексту АРМ-СДЗ).

2.1. Требования к АРМ установки СДЗ «TSM» на ПАК

АРМ-СДЗ должен состоять из следующих компонентов:

1. Персональный компьютер:
    - процессор x86/x64;
    - клавиатура + мышь;
    - интерфейс USB2.0/3/0;
    - ОЗУ 4Гбайт или больше;
    - Жесткий диск 250ГБ или более;
    - монитор;
    - сетевой интерфейс Ethernet;
    - ОС Ubuntu 16.04 LTS;
    - Эмулятор терминала (minicom или picocom) (используется для наблюдения за процессом установки СДЗ «TSM» ПАК);
    - Опционально - АПМДЗ Соболь 3.0 (используется как датчик случайных чисел);
2. СПО «Установщик СДЗ «TSM» (состав см. в таблице 2).
3. Кабель USB-microUSB для загрузки файлов дистрибутива в ПАК по последовательному протоколу.
4. Кабель USB-microUSB или USB-RS-232 (в зависимости от типа ПАК) для организации отладочного интерфейса между АРМ-СДЗ к ПАК.

На рисунке 1 представлена схема подключения АРМ-СДЗ к ПАК MXIMX6Q-SDB.

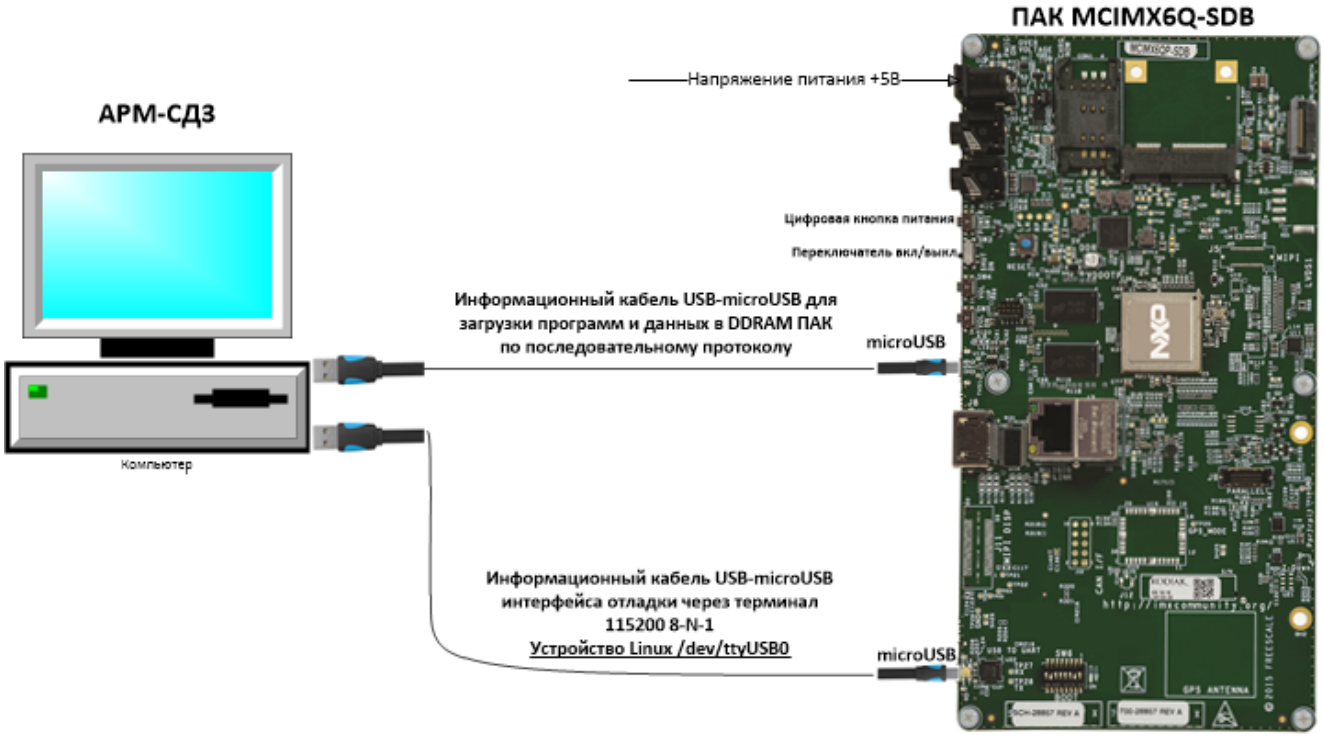

Рисунок 1 - Схема подключения АРМ-СДЗ и ПАК MCIMX6Q-SDB

На рисунке 2 представлена схема подключения АРМ-СДЗ к ПАК SK-iMX6-MB-SODIMM .

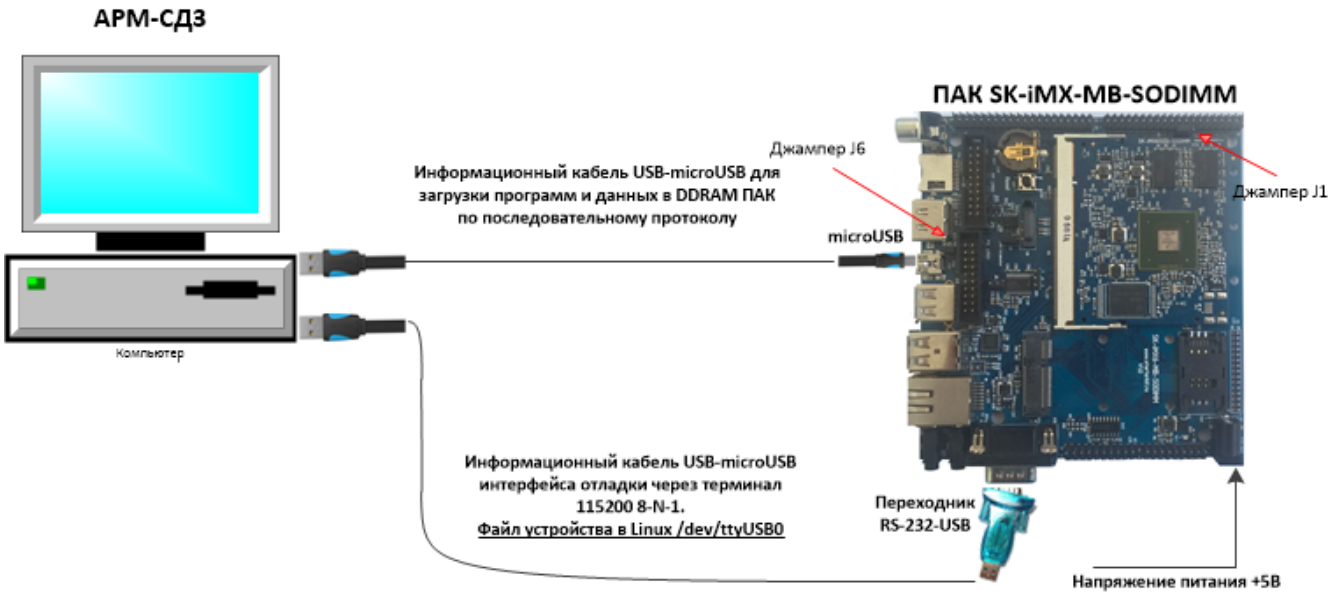

Рисунок 2 - Схема подключения АРМ-СДЗ и ПАК SK-iMX6-MB-SODIMM

2.2. Предварительная подготовка

1. Убедитесь, что ПАК и АРМ-СДЗ соединены в соответствии со схемой на рисунке 1 или рисунке 2, в зависимости на какой ПАК производится

установка.

2. Выберите режим последовательной загрузки через USB-OTG порт (BOOT_MODE[1:0]=01).

Примечание 1 - Для ПАК SK iMX6 MB SODIMM это можно сделать, замкнув джампер J1. Джампер J2 при этом должен быть разомкнут.

Примечание 2 - Для ПАК MCIMX6Q-SDB это можно сделать, переключив SW6 [off on off off off on off], при этом SD-каты должны быть извлечены или не содержать загрузочных образов.

3. Подайте питание на целевую платформу.

2.3. СПО «Установщик СДЗ состоит из следующих компонент:

1) Питон-скрипта imx_usb_loader.py (является консольной программой-фронтэндом);
2) Программы imx_usb, реализующий последовательный протокол загрузки данных (работает совместно с ROM-предзагрузчиком микропроцессора i.MX6;
3) Дистрибутива СДЗ «TSM» в виде tar-архива с файлами из Таблицы 1.

Примечание - Программы imx_usb_loader.py и imx_usb должны находится в одном и том же каталоге на диске.

2.4. Алгоритм работы СПО «Установщик СДЗ»

1) Старт работы СПО «Установщик СДЗ» происходит по запуску команды sudo ./imx_usb_loader.py с параметрами из таблицы 2:

Таблица 2 – Параметры imx_usb_loader.py

Параметр и значение	**Описание**
--platform_id=<ID-платформы >	ID-платформы, соответствующий цифровому значению [N] из файла параметров
--serial=<серийный номер>	Серийный номер, аналогичный номеру в формуляре
--operator_id = <идентификационный номер оператора>	Идентификационный номер оператора производства
--distr_path	Путь к tar-архиву дистрибутива СДЗ «TSM»
--open_key_path	Путь к файлу с хэш-суммой открытого ключа

2) После старта программа imx_usb_loader.py выполнит следующие действия:
   - сгенерирует с использованием датчика случайных чисел 32-битное (уникальное) число – UNIQ_ID_32 для записи в OTP память микропроцессора;
   - на основе параметра platform_id выберет из tar-архива дистрибутива

соответствующий файл параметров par[N].sbin и на его основе сгенерирует конфигурационный файл для программы imx_usb. (UNIQ_ID_32, serial, хэш-сумма открытого ключа передаются программе imx_usb через конфигурационный файл);

- запустит программу imx_usb.

3) Программа imx_usb, используя протокол SDP[2] (англ. Serial Download Protocol), произведет следующие действия:
    - инициализирует внешнюю ОЗУ (DDRAM) ПАК;
    - загрузит в DDRAM ПАК:
        - файл raminit.sbin;
        - tar-архив дистрибутива СДЗ «TSM»;
        - структуру данных разделов ЗН;
        - серийный номер для ПАК (параметр serial);
        - хэш-сумму публичного ключа электронной подписи;
        - уникальный идентификационный номер (UNIQ_ID_32) для ПАК;
    - запустит на выполнение raminit.sbin (данная программа исполняется на ПАК).

Примечание – для дальнейшего понимания хода установочной процедцры оператор должен наблюдать за сообщениями, появляющимися в программе эмуляции терминала (minicom или picocom).

4) Программа raminit.sbin, выполняясь на микропроцессоре ПАК, выполнит следующие действия:
    - установит файлы дистрибутива из таблицы 1 в соответствии документом «Формат SD»;
    - запишет на ЗН параметры СДЗ и параметры пользователей СЗД (конфигурацию по умолчанию);
    - обновит контрольные суммы для областей файлов boot.sbin, par[N].sbin по ГОСТ Р 34.11-2012;
    - разобьет ЗН на разделы в соответствии со структурой данных разделов ЗН;

[2] Описание SDP приведено документе в i.MX 6Dual/6Quad Applications Processor Reference Manual

- обновит контрольные суммы для 1-го раздела ЗН (на нем хранятся файлы tee.sbin, sdz.sbin);
- запишет в OTP хэш-сумму публичного ключа электронной подписи;
- запишет в OTP уникальный идентификационный номер (UNIQ_ID_32) для ПАК;
- запишет в OTP серийный номер;
- произведет дополнительные записи в OTP в соответствии с таблицей 3 (см. ниже);
- произведет верификацию записанных на загрузочных носитель файлов дистрибутива и памяти OTP и в случае ошибки верификации сообщит об ошибке оператору АРМ-СДЗ (через окно терминала).
- в случае успешной верификации, заблокирует возможность изменения OTP на ПАК и возможность загружать неподписанный цифровой подписью загрузчик.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	Замененных	новых	Аннулированных					