



Встроенная системная программа Загрузчик JaCarta OS

Описание программы

RU.АЛДЕ.01.01.021 13 01

Содержание

О документе.....	3
1. Общие сведения	4
1.1. Назначение	4
1.2. Соглашение о терминах и обозначениях	4
1.3. Общие сведения об APDU.....	4
1.4. Формат представления данных.....	4
1.5. Перечень APDU-команд загрузчика платформы	4
2. Содержание APDU-команд и ответов	6
2.1. Общие команды.....	6
2.1.1. Вычислить серийный номер.....	6
2.1.2. Сообщить уникальный идентификатор микроконтроллера.....	6
2.1.3. Сообщить структуру вычисления серийного номера.....	7
2.1.4. Сообщить размер флеш-памяти микроконтроллера	8
2.1.5. Сообщить размер SRAM-памяти микроконтроллера	8
2.1.6. Сообщить ID микроконтроллера.....	9
2.1.7. Включить светодиод	10
2.1.8. Сообщить информацию об изделии.....	10
2.1.9. Инициализировать систему	11
2.1.10. Выполнить перезагрузку	12
2.1.11. Сообщить адрес загрузчика	12
2.1.12. Тестировать кнопку.....	13
2.1.13. Перезагрузить в загрузчик производителя	14
2.2. Команды защищённого обновления	14
2.2.1. Начать защищённое обновление	14
2.2.2. Продолжить защищённое обновление.....	15
2.2.3. Завершить защищённое обновление.....	16
2.3. Команды работы с флеш-памятью.....	17
2.3.1. Записать данные во флеш-память.....	17
2.3.2. Считать флеш-память.....	17
2.3.3. Очистить флеш-память	18
Общие коды состояния	20
Ресурсы.....	21
Список литературы.....	21

О документе

Настоящий документ содержит описание работы встроенной системной программы «Загрузчик JaCarta OS» RU.АЛДЕ.01.01.021 посредством специализированного программного интерфейса взаимодействия (APDU) в соответствии со стандартом ISO/IEC 7816-4.

1. Общие сведения

1.1. Назначение

Встроенная системная программа «Загрузчик JaCarta OS» RU.АЛДЕ.01.01.021 предназначена для выполнения загрузки менеджера приложений при включении изделий на которых установлено программное средство «Встроенная системная программа JaCarta OS» RU.АЛДЕ.01.02.002-01, первоначальной установки менеджера приложений и первоначальной установки производственных параметров изделий.

Встроенная системная программа «Загрузчик JaCarta OS» способна обрабатывать APDU-команды до загрузки менеджера приложений.

1.2. Соглашение о терминах и обозначениях

В настоящем документе шестнадцатеричные числа представляются в формате $H_{n-1}[H_{n-2}]...[H_0]h$, где H_0-H_{n-1} — шестнадцатеричные цифры, n — разрядность числа в шестнадцатеричном представлении, h — латинская буква h . Буква X означает, что на её месте может быть любая шестнадцатеричная цифра.

Примеры: A0h, 670Ch, 0Xh.

1.3. Общие сведения об APDU

APDU для загрузчика платформы соответствуют стандартам ISO/IEC 7816 [1], [2].

APDU передаются по протоколу T = 1 [1].

Поля данных увеличенной длины (extended length fields, см. [1], [2]) загрузчиком платформы не поддерживаются.

Первые четыре байта APDU-команды уникальны.

Для команд, предполагающих наличие поля данных в ответе, длина ожидаемого поля данных ответа составляет 256 байт, а поле L_e игнорируется.

Загрузчик платформы единовременно обрабатывает только одну команду и при её выполнении возвращает ответ, содержащий данные и код состояния или только код состояния. Эта пара операций происходит синхронно, то есть за каждым вызовом команды APDU следует ответное сообщение. Загрузчик платформы сам по себе не инициирует никаких внешних операций без вызова команд APDU.

В настоящем документе для описания каждой APDU-команды и ответа на неё используются следующие таблицы:

- таблица, отражающая общую структуру APDU-команд и данные, специфичные для конкретной команды;
- таблица, отражающая структуру поля данных APDU-ответа (при наличии поля данных);
- таблица специфичных кодов состояния, которые могут содержаться в APDU-ответе.

Кроме того, в конце настоящего документа (таблица 49, с. 20) приведены коды состояния, которые могут встречаться в APDU-ответах на все описанные настоящим документе APDU-команды.

1.4. Формат представления данных

За исключением случаев, когда в описании APDU явно указано иное, в APDU-командах и APDU-ответах многобайтные числа представляются в порядке следования байтов от младшего к старшему (little-endian).

1.5. Перечень APDU-команд загрузчика платформы

Перечень APDU-команд представлен в таблице 1.

Доступность APDU-команд определяется режимом работы:

- BL – BLANK;
- TRN – TRANSPORT;
- ID – IDLE;
- CB – CCID_BOOT;
- UF – UPDATE_FW;
- TER – TERMINATED.

Таблица 1 – Перечень APDU-команд

CLA	INS	P1	P2	Название	Доступность команды					
					BL	TRN	ID	CB	UF	TER
80	C0	00	00	Вычислить серийный номер	+	-	-	+	+	-
80	C0	00	01	Сообщить уникальный идентификатор микроконтроллера	+	-	-	+	+	-
80	C0	00	02	Сообщить структуру вычисления серийного номера	+	-	-	+	+	-
80	C0	00	03	Сообщить размер флеш-памяти микроконтроллера	+	-	-	+	+	-
80	C0	00	04	Сообщить размер SRAM-памяти микроконтроллера	+	-	-	+	+	-
80	C0	00	05	Сообщить ID микроконтроллера	+	-	-	+	+	-
80	C0	01	00	Включить светодиод	+	-	-	+	+	-
80	C0	02	00	Сообщить информацию об изделии	+	-	-	+	+	-
80	C0	03	00	Инициализировать систему	+	-	-	-	-	-
80	C0	05	00	Выполнить перезагрузку	+	-	-	+	+	-
80	C0	06	00	Сообщить адрес загрузчика	+	-	-	+	+	-
80	C0	07	00	Тестировать кнопку	+	-	-	+	+	-
80	C0	08	00	Перезагрузить в загрузчик производителя	+	-	-	-	-	-
80	C2	00	00	Начать защищённое обновление	-	-	-	-	+	-
			10		-	-	-	-	+	-
80	C2	10	00	Продолжить защищённое обновление	-	-	-	-	+	-
80	C2	20	00	Завершить защищённое обновление	-	-	-	-	+	-
80	C6	03	XX	Записать данные во флеш-память	+	-	-	+	-	-
80	C6	04	00	Считать флеш-память	+	-	-	+	-	-
80	C7	XX	XX	Очистить флеш-память	+	-	-	+	-	+

2. Содержание APDU-команд и ответов

2.1. Общие команды

2.1.1. Вычислить серийный номер

Команда позволяет вычислить серийный номер для нанесения на корпус изделия. Серийный номер представляет собой результат вычисления по алгоритму CRC32 от структуры вычисления серийного номера, приведённой в описании команды «Сообщить структуру вычисления серийного номера» на с. 7.

Содержание команды приведено в таблице 2.

Таблица 2 – Команда «Вычислить серийный номер»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	00h	Команда «Вычислить серийный номер»
P2	00h	—
L _c	—	Игнорируется
Data	—	»
L _e	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 3.

Таблица 3 – Состав поля данных APDU-ответа на команду «Вычислить серийный номер»

Длина, Б	Значение
4	Серийный номер изделия

Специфические коды состояния, которые могут содержаться в ответе на команду «Вычислить серийный номер», приведены в таблице 4.

Таблица 4 – Специфические коды состояния в APDU-ответе на команду «Вычислить серийный номер»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.2. Сообщить уникальный идентификатор микроконтроллера

Команда позволяет получить значение и контрольную сумму значения уникального идентификатора (UID) микроконтроллера.

Содержание команды приведено в таблице 5.

Таблица 5 – Команда «Сообщить уникальный идентификатор микроконтроллера»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды

Поле	Значение	Описание
P1	00h	Команда «Сообщить уникальный идентификатор микроконтроллера»
P2	01h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 6.

Таблица 6 – Состав поля данных APDU-ответа на команду «Сообщить уникальный идентификатор микроконтроллера»

Длина, Б	Значение
16	Уникальный идентификатор микроконтроллера.
4	Контрольная сумма уникального идентификатора, CRC-32.

Специфичные коды состояния, которые могут содержаться в ответе на команду «Сообщить уникальный идентификатор микроконтроллера», приведены в таблице 7.

Таблица 7 – Специфичные коды состояния в APDU-ответе на команду «Сообщить уникальный идентификатор микроконтроллера»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.3. Сообщить структуру вычисления серийного номера

Команда позволяет получить структуру вычисления серийного номера.

Содержание команды приведено в таблице 8.

Таблица 8 – Команда «Сообщить структуру вычисления серийного номера»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	00h	Команда «Сообщить структуру вычисления серийного номера»
P2	02h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 9.

Таблица 9 – Состав поля данных APDU-ответа на команду «Сообщить структуру вычисления серийного номера»

Длина, Б	Значение
8	12h 06h XXXXXXXX 00h 01h – структура для вычисления серийного номера, где XXXXXXXX – контрольная сумма, вычисленная по алгоритму CRC32 от UID микроконтроллера.

Серийный номер является результатом вычисления по алгоритму CRC32 от данной структуры.

Значение серийного номера можно узнать при помощи команды «Вычислить серийный номер».

Специфичные коды состояния, которые могут содержаться в ответе на команду «Сообщить структуру вычисления серийного номера», приведены в таблице 10.

Таблица 10 – Специфичные коды состояния в APDU-ответе на команду «Сообщить структуру вычисления серийного номера»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.4. Сообщить размер флеш-памяти микроконтроллера

Команда позволяет получить значение размера флеш-памяти микроконтроллера.

Содержание команды приведено в таблице 11.

Таблица 11 – Команда «Сообщить размер флеш-памяти микроконтроллера»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	00h	Команда «Сообщить размер флеш-памяти микроконтроллера»
P2	03h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 12.

Таблица 12 – Состав поля данных APDU-ответа на команду «Сообщить размер флеш-памяти микроконтроллера»

Длина, Б	Значение
4	Значение размера флеш-памяти микроконтроллера

Специфичные коды состояния, которые могут содержаться в ответе на команду «Сообщить размер флеш-памяти микроконтроллера», приведены в таблице 13.

Таблица 13 – Специфичные коды состояния в APDU-ответе на команду «Сообщить размер флеш-памяти микроконтроллера»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.5. Сообщить размер SRAM-памяти микроконтроллера

Команда позволяет получить значение размера SRAM-памяти микроконтроллера.

Содержание команды приведено в таблице 14.

Таблица 14 – Команда «Сообщить размер SRAM-памяти микроконтроллера»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	00h	Команда «Сообщить размер SRAM-памяти микроконтроллера»
P2	04h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 15.

Таблица 15 – Состав поля данных APDU-ответа на команду «Сообщить размер SRAM-памяти микроконтроллера»

Длина, Б	Значение
4	Значение размера SRAM-памяти микроконтроллера

Специфичные коды состояния, которые могут содержаться в ответе на команду «Сообщить размер SRAM-памяти микроконтроллера», приведены в таблице 16.

Таблица 16 – Специфичные коды состояния в APDU-ответе на команду «Сообщить размер SRAM-памяти микроконтроллера»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.6. Сообщить ID микроконтроллера

Команда позволяет получить ID микроконтроллеров NXP Kinetis K22 и LPC18XX. Для других микроконтроллеров поле Data APDU-ответа будет отсутствовать.

Таблица 17 – Команда «Сообщить ID микроконтроллера»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	00h	Команда «Сообщить ID микроконтроллера»
P2	05h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

Таблица 18 – Состав поля данных APDU-ответа на команду «Сообщить ID микроконтроллера»

Длина, Б	Значение
1	Значение ID микроконтроллера

Таблица 19 – Специфичные коды состояния в APDU-ответе на команду «Сообщить ID микроконтроллера»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.7. Включить светодиод

Команда позволяет включить светодиод (перевести в режим постоянного свечения). Если светодиод уже был переведён в режим постоянного свечения командой «Включить светодиод», то повторная команда приведёт к отключению светодиода.

Содержание команды приведено в таблице 20.

Таблица 20 – Команда «Включить светодиод»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	01h	Команда «Включить светодиод»
P2	00h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

Специфичные коды состояния, которые могут содержаться в ответе на команду «Включить светодиод», приведены в таблице 21.

Таблица 21 – Специфичные коды состояния в APDU-ответе на команду «Включить светодиод»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.8. Сообщить информацию об изделии

Содержание команды приведено в таблице 22.

Таблица 22 – Команда «Сообщить информацию об изделии»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])

Поле	Значение	Описание
INS	C0h	Общие команды
P1	02h	Команда «Сообщить информацию об изделии»
P2	00h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 23.

Таблица 23 – Состав поля данных APDU-ответа на команду «Сообщить информацию об изделии»

Длина, Б	Значение
27	• 1 байт – статус изделия; • 2 байта – количество ошибок вычисления контрольной суммы сектора служебной информации; • 4 байта – версия загрузчика платформы; • 4 байта – версия менеджера приложений; • 4 байта – адрес хранилища приложений; • 4 байта – размер хранилища приложений; • 4 байта – адрес файловой системы; • 4 байта – количество блоков файловой системы, выделяемых под хранение данных

Специфичные коды состояния, которые могут содержаться в ответе на команду «Сообщить информацию об изделии», приведены в таблице 24.

Таблица 24 – Специфичные коды состояния в APDU-ответе на команду «Сообщить информацию об изделии»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.9. Инициализировать систему

Команда устанавливает транспортный ключ, ключ производства и ключ обновления по умолчанию. Содержание команды приведено в таблице 25.

Таблица 25 – Команда «Инициализировать систему»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	03h	Команда «Инициализировать систему»
P2	00h	—
Lc	60h	—
Data	XX...XXh	• 32 байта – значение транспортного ключа; • 32 байта – значение ключа производства; • 32 байта – значение ключа обновления по умолчанию

Поле	Значение	Описание
L _e	—	Игнорируется
Специфичные коды состояния, которые могут содержаться в ответе на команду «Инициализировать систему», приведены в таблице 26.		

Таблица 26 — Специфичные коды состояния в APDU-ответе на команду «Инициализировать систему»

SW1 SW2	Значение
6807	Система уже инициализирована
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.10. Выполнить перезагрузку

Содержание команды приведено в таблице 27.

Таблица 27 — Команда «Выполнить перезагрузку»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	05h	Команда «Выполнить перезагрузку»
P2	00h	—
L _c	—	Игнорируется
Data	—	»
L _e	—	»

Специфичные коды состояния, которые могут содержаться в ответе на команду «Выполнить перезагрузку», приведены в таблице 28.

Таблица 28 — Специфичные коды состояния в APDU-ответе на команду «Выполнить перезагрузку»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.11. Сообщить адрес загрузчика

Команда позволяет получить адрес загрузчика во флеш-памяти микроконтроллера.

Содержание команды приведено в таблице 29.

Таблица 29 — Команда «Сообщить адрес загрузчика»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды

Поле	Значение	Описание
P1	06h	Команда «Сообщить адрес загрузчика»
P2	00h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 30.

Таблица 30 — Состав поля данных APDU-ответа на команду «Сообщить адрес загрузчика»

Длина, Б	Значение
4	адрес, с которого выполняется текущий загрузчик
Специфические коды состояния, которые могут содержаться в ответе на команду «Сообщить адрес загрузчика», приведены в таблице Таблица 31.	

Таблица 31 — Специфические коды состояния в APDU-ответе на команду «Сообщить адрес загрузчика»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.12. Тестировать кнопку

Команда переводит изделия, оснащённые кнопкой, в состояние ожидания нажатия кнопки. Предназначена для микроконтроллеров NXP Kinetis K22.

Во время ожидания будет мигать светодиод с частотой 10Гц.

Содержание команды приведено в таблице 32.

Таблица 32 — Команда «Тестировать кнопку»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	07h	Команда «Тестировать кнопку»
P2	00h	—
Lc	—	Если поле отсутствует, то время ожидания нажатия кнопки составит 30 секунд, иначе см. описание поля Data данной команды.
Data	XXh	1 байт — время ожидания нажатия кнопки в секундах: при Data = 00h время ожидания не ограничено, иначе — не более 59 секунд.
Le		Игнорируется

Специфические коды состояния, которые могут содержаться в ответе на команду «Тестировать кнопку», приведены в таблице 33.

Таблица 33 – Специфические коды состояния в APDU-ответе на команду «Тестировать кнопку»

SW1 SW2	Значение
680Bh	В отведённое время кнопка не была нажата.
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.1.13. Перезагрузить в загрузчик производителя

Команда стирает первый сектора флеш-памяти и инициирует перезагрузку микроконтроллера. В отсутствие данных в первом секторе переход в загрузчик производителя осуществляется автоматически при перезагрузке. Команда необратима. Предназначена для микроконтроллеров MN17xx и LPC18xx.

Содержание команды приведено в таблице 34.

Таблица 34 – Команда «Перезагрузить в загрузчик производителя»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C0h	Общие команды
P1	08h	Команда «Перезагрузить в загрузчик производителя»
P2	00h	—
Lc	—	Игнорируется
Data		»
Le		»

Специфические коды состояния, которые могут содержаться в ответе на команду «Перезагрузить в загрузчик производителя», приведены в таблице 35.

Таблица 35 – Специфические коды состояния в APDU-ответе на команду «Перезагрузить в загрузчик производителя»

SW1 SW2	Значение
9000h	Команда выполнена успешно

2.2. Команды защищённого обновления

2.2.1. Начать защищённое обновление

Команда позволяет обновить JaCarta OS при помощи зашифрованного файла обновления.

Содержание команды приведено в таблице 36.

Таблица 36 – Команда «Начать защищённое обновление»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C2h	Команды защищённого обновления

Поле	Значение	Описание
P1	00h	Команда «Начать защищённое обновление»
P2	XXh	00h — начать защищённое обновление с проверкой наложения файла обновления на область хранилища приложений. 10h — начать защищённое обновление без проверки наложения файла обновления на область хранилища приложений (возможно повреждение хранилища).
Lc	80h	—
Data	XXh..XXh	Заголовок длиной 128 байт зашифрованного загружаемого файла обновления
Le	—	Игнорируется

Специфичные коды состояния, которые могут содержаться в ответе на команду «Начать защищённое обновление», приведены в таблице 37.

Таблица 37 — Специфичные коды состояния в APDU-ответе на команду «Начать защищённое обновление»

SW1 SW2	Значение
6804h	Отсутствует библиотека шифрования.
6805h	Неверный заголовок файла обновления (Ошибка подписи).
680Ah	Файл обновления накладывается на хранилище приложений.
680Bh	Файл обновления накладывается на область микропрограммы загрузчика OS.
680Dh	Файл обновления накладывается на сектор служебной информации.
680Ch	Файл обновления накладывается на файловую систему.
6B28h	Идентификатора модели микроконтроллера (MCID), указанный в файле обновления, не совпадает MCID микроконтроллера изделия.
6B32h	Извлечение ключа обновления из контейнера невозможно.
9000h	Команда выполнена успешно.



Общие коды состояния приведены в таблице 49 (с. 20).

2.2.2. Продолжить защищённое обновление

Команда позволяет продолжить защищённое обновление JaCarta OS, начатое командой «Начать защищённое обновление».

Содержание команды приведено в таблице 38.

Таблица 38 — Команда «Продолжить защищённое обновление»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C2h	Команды защищённого обновления
P1	10h	Команда «Продолжить защищённое обновление»
P2	00h	—
Lc	01h - FFh	Длина передаваемых данных
Data	XXh..XXh	Передаваемый фрагмент данных
Le	—	Игнорируется

Специфичные коды состояния, которые могут содержаться в ответе на команду «Продолжить защищённое обновление», приведены в таблице 39.

Таблица 39 – Специфичные коды состояния в APDU-ответе на команду «Продолжить защищённое обновление»

SW1 SW2	Значение
6803h	Ошибка записи файла обновления
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.2.3. Завершить защищённое обновление

Команда позволяет завершить защищённое обновление JaCarta OS, продолженное командой «Продолжить защищённое обновление».

Содержание команды приведено в таблице 40.

Таблица 40 – Команда «Завершить защищённое обновление»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C2h	Команды защищённого обновления
P1	20h	Команда «Завершить защищённое обновление»
P2	00h	—
Lc	—	Игнорируется
Data	—	»
Le	—	»

Специфичные коды состояния, которые могут содержаться в ответе на команду «Завершить защищённое обновление», приведены в таблице 41.

Таблица 41 – Специфичные коды состояния в APDU-ответе на команду «Завершить защищённое обновление»

SW1 SW2	Значение
6809h	Ошибка ключа шифрования (контрольная сумма файла обновления, вычисленная по алгоритму CRC32, не совпадает с указанной в заголовке файла обновления)
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.3. Команды работы с флеш-памятью

2.3.1. Записать данные во флеш-память

Команда позволяет записать блок данных размером 2048 байт в сектор флеш-памяти микроконтроллера по указанному адресу сектора. Размер сектора составляет 2048 байт. Адрес сектора вычисляется как номер сектора (начиная с нулевого) умноженный 2048. Запись возможна в сектора с адресами большими, чем адрес последнего занимаемого загрузчиком OS целиком сектора. Первые восемь команд формируют в оперативной памяти микроконтроллера блок данных размером 2048 байт. Девятая команда записывает эти данные в сектор флеш-памяти.

Содержание команды приведено в таблице 42.

Таблица 42 – Команда «Записать данные во флеш-память»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C6h	Команды работы с флеш-памятью
P1	03h	Команда «Записать данные во флеш-память»
P2	XXh	00h – 07h – для первых восьми команд (записи первых восьми блоков по 255 байт в оперативную память микроконтроллера); 08h – для записи оставшихся восьми байт; 09h – для записи заполненного сектора во флеш-память, по адресу сектора, указанному в этой команде
Lc	XXh	- FFh – при P2 с 00h по 07h; 08h – при P2 = 08h; 04h – при P2 = 09h
Data	XX..XXh	При P2 с 00h по 08h – данные. При P2 = 09h – адрес сектора, по которому будет производиться запись
Le	–	Игнорируется

Специфичные коды состояния, которые могут содержаться в ответе на команду «Записать данные во флеш-память», приведены в таблице 43.

Таблица 43 – Специфичные коды состояния в APDU-ответе на команду «Записать данные во флеш-память»

SW1 SW2	Значение
6801h	Указан недопустимый адрес сектора
6803h	Ошибка при записи флеш-памяти
680Bh	Указан адрес меньший, чем адрес последнего байта сектора, целиком занятого загрузчиком платформы
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.3.2. Считать флеш-память

Команда позволяет прочесть данные по указанному адресу.

Содержание команды приведено в таблице 44.

Таблица 44 – Команда «Считать флеш-память»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C6h	Команды работы с флеш-памятью
P1	04h	Команда «Считать флеш-память»
P2	00h	—
Lc	08h	—
Data	XX..XXh	• 4 байта – адрес во флеш-памяти; • 4 байта – размер возвращаемых данных. Размер, превышающий 256 байт недопустим
Le	—	Игнорируется

В случае успешного выполнения команды APDU-ответ содержит поле данных согласно таблице 45.

Таблица 45 – Состав поля данных APDU-ответа на команду «Считать флеш-память»

Длина, Б	Значение
255	Данные

Специфичные коды состояния, которые могут содержаться в ответе на команду «Считать флеш-память», приведены в таблице 46.

Таблица 46 – Специфичные коды состояния в APDU-ответе на команду «Считать флеш-память»

SW1 SW2	Значение
9000h	Команда выполнена успешно



Общие коды состояния приведены в таблице 49 (с. 20).

2.3.3. Очистить флеш-память

Команда позволяет заполнить нулями или единицами (в зависимости от решения производителя микроконтроллера) всю флеш-память микроконтроллера (за исключением флеш-памяти, занимаемой загрузчиком OS) в режимах:

- TERMINATED;
- CCID_BOOT;
- UPDATE_FW (только, если невозможно извлечение ключа обновления из контейнера см. [Ошибка! Источник ссылки не найден.]).

После удачного выполнения данной команды устройство переходит в состояние BLANK.

Содержание команды приведено в таблице 47.

Таблица 47 – Команда «Очистить флеш-память»

Поле	Значение	Описание
CLA	80h	Класс команды (см. [2])
INS	C7h	Команды работы с флеш-памятью
P1	XXh	Игнорируется»

Поле	Значение	Описание
P2	XXh	Игнорируется

Специфичные коды состояния, которые могут содержаться в ответе на команду «Очистить флеш-память», приведены в таблице 48.

Таблица 48 – Специфичные коды состояния в APDU-ответе на команду «Очистить флеш-память»

SW1 SW2	Значение
9000h	Команда выполнена успешно
6A82h ¹	Ключ обновления может быть извлечён из контейнера

 Общие коды состояния приведены в таблице 49 (с. 20).

¹ SW1–SW2 6A82h может быть получен только в режиме UPDATE_FW.
АО «Аладдин Р. Д.», 1995–2025

Общие коды состояния

Значения и описания двухбайтовых кодов состояния, которые могут содержаться в полях SW1 и SW2 APDU-ответов на каждую из описанных в настоящем документе APDU-команд, приведены в таблице 49.

Таблица 49 – Общие коды состояния

Код	Описание	Примечание
6700h	Некорректная длина поля данных APDU-команды	—
6785h	Команда запрещена блоком FIREWALL	—
68FFh	Модульная платформа находится в режиме TERMINATED	Для всех APDU-команд, кроме «Очистить флеш-память».
6A86h	Недопустимое значение параметра команды	—
6D00h	Недопустимое значение инструкции команды	—
6E00h	Недопустимое значения класса команды	—

 Поддерживаются и другие коды состояния, соответствующие ISO/IEC 7816-4 [2].

Ресурсы

Список литературы

- 1 ГОСТ Р ИСО/МЭК 7816-3 — 2013. Карты идентификационные. Карты на интегральных схемах. Часть 3. Карты с контактами. Электрический интерфейс и протоколы передачи [Текст] — Взамен ГОСТ Р ИСО МЭК 7816-3—2006. — Введ. 2013—11—22. — М. : Стандартинформ, 2014. — 52 с.
 - 2 ГОСТ Р ИСО/МЭК 7816-4 — 2013. Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена [Текст] — Взамен ГОСТ Р ИСО МЭК 7816-4—2004. — Введ. 2013—11—22. — М. : Стандартинформ, 2014. — 95 с.
-

Коротко о компании

Основанная в апреле 1995 года компания «Аладдин Р. Д.» — российский разработчик (вендор) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления:

- обеспечение безопасного доступа к информационным ресурсам предприятия, веб-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация);
- электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI;
- защита персональных данных, данных на дисках компьютеров, серверов, баз данных.

Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии:

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа;
- система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты;
- система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Минобороны России № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям
ГОСТ Р ИСО 9001—2015 (ISO 9001:2015). Сертификат СМК № РОСС RU.ФК14.К00011 от 20.07.18.

© ЗАО «Аладдин Р. Д.», 1995—2025. Все права защищены
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin.ru
Web: www.aladdin.ru