



СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ALADDIN CRYPTOFLASH

Описание программы
RU.АЛДЕ.01.02.007 13 01

СОДЕРЖАНИЕ

Аннотация.....	3
Сокращения и обозначения.....	4
1. Общие сведения	5
1.1. Назначение.....	5
1.2. Совместное использование с другими изделиями.....	5
2. Содержание APDU-команд и ответов СПО Aladdin CryptoFlash.....	7
2.1. Список APDU-команд	7
2.2. Список SW-ответов СПО Aladdin CryptoFlash.....	29
2.3. Список параметров работы СПО Aladdin CryptoFlash.....	30
2.4. Список входных функций СПО Aladdin CryptoFlash	37
2.5. Жизненные циклы СПО Aladdin CryptoFlash	38
2.6. Логика работы СПО Aladdin CryptoFlash	38
3. Дополнительная информация СПО Aladdin CryptoFlash.....	42
3.1. Модуль туннелирования APDU-команд через MSCD-интерфейс.....	42
3.2. Структура данных ответа на SCSI-команду INQUIRY (12h)	43

АННОТАЦИЯ

Данный документ содержит описание работы специального программного обеспечения «Специальное программное обеспечение Aladdin CryptoFlash» RU.АЛДЕ.01.02.007 (далее – СПО Aladdin CryptoFlash) – программного компонента изделия «Средство криптографической защиты информации «Aladdin CryptoFlash – защищённый флеш-накопитель со встроенным шифрованием данных» АЛДЕ.468999.001 (далее – изделие), реализующего функции шифрования данных при доступе на microSD-карту специализированного съёмного машинного носителя (далее – ССМНИ), входящего в состав изделия, а также описание APDU команд и ответов СПО Aladdin CryptoFlash.

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

Используемые сокращения:

ЗК	защищённый канал
ПО	программное обеспечение
СПО	специализированное программное обеспечение
ССМНИ	специализированный съёмный машинный носитель информации

В документе используются следующие обозначения:

- **карта памяти** - используемая в составе изделия карта памяти формата Secure Digital Memory Card (SD)

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение

СПО Aladdin CryptoFlash предназначено для функционирования в микроконтроллерах общего назначения ССМНИ и реализации функций аутентификации, датчика случайных чисел, а также следующих криптографических функций и протоколов:

- генерация псевдослучайных последовательностей;
- шифрование и расшифрование данных согласно ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 «Магма» в режиме DEC в соответствии с рекомендациями по стандартизации Р 1323565.1.042-2022 «Информационная технология. Криптографическая защита информации. Режим работы блочных шифров, предназначенный для защиты носителей информации с блочно-ориентированной структурой»;
- шифрование и расшифрование данных согласно ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 «Магма» в режиме гаммирования в соответствии с ГОСТ Р 34.13-2015/ГОСТ 34.13-2018;
- контроль целостности данных посредством вычисления имитовставки согласно ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 «Магма» в режиме ГОСТ Р 34.13-2015/ГОСТ 34.13-2018;
- выработка ключа из пароля в соответствии с рекомендациями по стандартизации Р 1323565.1.040-2022;
- вычисление криптокопий секретных ключей с использованием алгоритма экспорта KExp15 ключа в соответствии с рекомендациями по стандартизации Р 1323565.1.017-2018;
- выработка общего ключа с аутентификацией на основе пароля в соответствии с рекомендациями по стандартизации Р 50.1.115-2016.

1.2. Совместное использование с другими изделиями

СПО Aladdin CryptoFlash является составной частью изделия «Средство криптографической защиты информации «Aladdin CryptoFlash – защищённый флеш-накопитель со встроенным шифрованием данных» АЛДЕ.468999.001 (изделие), которое предназначено для безопасного хранения и переноса информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, пользователями как внутри своей информационной системы, так и из сторонних информационных систем.

В состав изделия также входят программное средство «Программа управления Aladdin CryptoFlash» (далее – Программа управления) RU.АЛДЕ.03.12.012 и изделие «Специализированный съёмный машинный носитель информации Aladdin CryptoFlash» АЛДЕ.467669.062 (далее – ССМНИ), который имеет два раздела:

- **открытый раздел** — раздел памяти ССМНИ доступный как аутентифицированному, так и не аутентифицированному пользователю в проводнике операционной системы в виде подключаемого диска в режиме «только чтение», а также доступного в режиме «чтение/запись» аутентифицированному пользователю с ролью администратор, на котором располагается программное обеспечение, используемое для управления доступом и работы с защищёнными данными ССМНИ, а также иные данные, записанные администратором на данный раздел.
- **защищённый скрытый раздел** — раздел памяти ССМНИ, доступный пользователю в проводнике операционной системы после успешной аутентификации в Программе управления, в виде подключаемого диска в режиме «чтение/запись» или «только чтение».

СПО Aladdin CryptoFlash обеспечивает выполнение следующих функций изделия совместно с Программой управления:

- автоматический контроль целостности Программы управления и СПО Aladdin CryptoFlash, их компонентов, а также программного датчика случайных чисел;
- управление аутентификационной информацией администратора изделия;
- управление параметрами инициализации ССМНИ, к которым относятся:
 - идентификационная информация пользователя, ССМНИ;
 - аутентификационная информация пользователя;
 - парольная политика;
 - контроль доступа;
 - журналирование событий;
 - интерфейс взаимодействия;
- управление режимами использования ССМНИ в соответствии с заданными параметрами:
 - инициализация программного датчика случайных чисел;
 - инициализация ССМНИ;
 - сброс ССМНИ к заводским установкам;
 - разблокирование ССМНИ;
 - смена режима работы открытого раздела;
- выполнение регламентного (периодического) контроля целостности программы Программы управления и СПО Aladdin CryptoFlash, их компонентов, а также программного датчика случайных чисел;
- выполнение аудита безопасности:
 - полное или выборочное ознакомление с информацией в журнале событий;
 - экспорт событий из журнала ССМНИ;
 - очистка журнала;
- работа с защищённым разделом памяти ССМНИ:
 - подключение/отключение защищённого раздела памяти ССМНИ;
 - очистка защищённого раздела ССМНИ.

2. СОДЕРЖАНИЕ APDU-КОМАНД И ОТВЕТОВ СПО ALADDIN CRYPTOFLASH

2.1. Список APDU-команд

Название	Заголовок, hex
Сообщить версию	80 A6 00 00
Сообщить служебную информацию о карте памяти	80 A6 00 01
Сообщить список идентификаторов учётных записей	80 A6 00 02
Сообщить параметры учётной записи по идентификатору	80 A6 00 03
Сообщить параметры учётной записи по метке	80 A6 00 04
Сгенерировать псевдослучайную последовательность	80 A6 00 05
Сообщить статус устройства	80 A6 00 06
Чтение журнала событий	80 A6 00 07
Сообщить количество секторов диска	80 A6 00 08
Сообщить быстродействие ключевой схемы шифрования	80 A6 00 09
Считать данные из хранилища информации об устройстве	80 A6 00 0A
Сообщить количество установленных паролей учётной записи	80 A6 00 0B
Сообщить список мастер-ключей диверсификации	80 A6 00 0C
Выполнить алгоритм диверсификации KDF_TREE_GOSTR3411_2012_256	80 A6 00 0D
Создание новой учётной записи	80 A6 10 00
Смена параметров учётной записи	80 A6 10 01
Удаление учётной записи	80 A6 10 02
Обновление значения служебной информации о карте памяти	80 A6 10 03
Обновление внутреннего состояния ПДСЧ	80 A6 10 04
Обновление параметров журнала событий	80 A6 10 05
Очистка карты памяти	80 A6 10 06
Обновление жизненного цикла	80 A6 10 07
Установка типа шифрования диска	80 A6 10 08
Генерация нового ключа шифрования дисков	80 A6 10 09
Записать данные в хранилище информации об устройстве	80 A6 10 0A
Удалить хранилище информации об устройстве	80 A6 10 0B

Название	Заголовок, hex
Включить/отключить поддержку механизма туннелирования APDU-команд	80 A6 10 0C
Обновить полномочие очистки карты памяти в гостевом режиме	80 A6 10 0D
Генерация мастер-ключа диверсификации	80 A6 10 0E
Начать установку защищённого канала	80 A6 20 00
Завершить установку защищённого канала	80 A6 20 01
Изменить статус защищённого канала	80 A6 20 02
Перезагрузить устройство	80 A6 30 00
Обновление статуса подключения диска	80 A6 30 01
Проверить пароль	80 A6 40 00
Сменить пароль	80 A6 40 01
Перейти в режим гостя	80 A6 40 02
Сбросить к заводским настройкам	80 A6 40 03
Смена пароля сброса к заводским настройкам	80 A6 40 04
Установить ключ администратора	80 A6 40 05

2.1.1. Сообщить версию СПО Aladdin CryptoFlash

- Команда доступна в любом режиме работы.
- Команда возвращает версию СПО Aladdin CryptoFlash.
- Версия СПО Aladdin CryptoFlash – это дата изменений в СПО Aladdin CryptoFlash.
- Версия обязательно должна меняться разработчиком после внесения любых изменений в исходный код СПО Aladdin CryptoFlash.

2.1.1.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60000	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.1.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxx	Версия СПО Aladdin CryptoFlash (пример: 20 24 10 31)

Смещение	Длина, байт	Значение, hex	Примечание
4	2	9000	SW-ответ

2.1.2. Сообщить служебную информацию о карте памяти

Команда доступна в любом режиме работы

2.1.2.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60001	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.2.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	240	xxxxxxxx	Служебная информация о карте памяти
240	2	9000	SW-ответ

2.1.3. Сообщить список идентификаторов учётных записей

Команда доступна в любом режиме работы.

Возвращается список идентификаторов созданных учётных записей

2.1.3.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60002	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.3.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4X	xxxxxxxx	Идентификаторы учётных записей
4X	2	9000	SW-ответ

2.1.4. Сообщить параметры учётной записи по идентификатору

Команда доступна в любом режиме.

Возвращаются параметры учётной записи, идентификатор которой указан в поле данных APDU-команды.

Запрос параметров текущей аутентифицированной записи доступна также по идентификатору FFFFFFFFh.

2.1.4.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60003	Заголовок команды
4	1	08	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxxx	Идентификатор учётной записи

2.1.4.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	112	xxxxxxxx	Параметры учётной записи
112	2	9000	SW-ответ

2.1.5. Сообщить параметры учётной записи по метке

Команда доступна в любом режиме.

Возвращаются параметры учётной записи, метка которой указана в поле данных APDU-команды.

2.1.5.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60004	Заголовок команды
4	1	08	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	64	xxxxxxxx	Метка учётной записи

2.1.5.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	112	xxxxxxxx	Параметры учётной записи
112	2	9000	SW-ответ

2.1.6. Проверить пароль

Команда доступна только в режиме гостя:

1. Если учётная запись, идентификатор которой указан в APDU-команде, заблокирована возвращается соответствующая ошибка.
2. Если последовательных попыток неверного ввода пароля от 3 до 10, задержка 10 секунд. Если попыток больше 10-ти, задержка 30 секунд.
3. Аутентификация производится путём расшифрования блока ключа K1.
4. В случае успешной аутентификации в журнале событий регистрируется «*Успешная аутентификация учётной записи*» (см. Журналирование событий).
5. В случае неуспешной аутентификации в журнале событий регистрируется «*Неуспешная аутентификация учётной записи*» (см. Журналирование событий), а также «*Блокирование пароля учётной записи*» (см. Журналирование событий), если значение

«Счётчик неудачных попыток, идущих подряд» достигло значения 0 (см. Счётчики аутентификации).

2.1.6.2. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A64000	Заголовок команды
4	1	xx	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxxx	Идентификатор учётной записи
13	xx	xxxxxxxxxx	Значение пароля

2.1.6.3. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.7. Сменить пароль

- Команда доступна только аутентифицированной учётной записи
- Проверяется полномочие «Возможность смены пароля любой учётной записи», если указанный идентификатор в APDU-команде не соответствует идентификатору текущей учётной записи
- Проверяется значение нового пароля на соответствие параметру Парольные политики учётной записи
- В случае успешной смены, Счётчики аутентификации устанавливаются в максимальные значения
- В случае успешной смены, в журнал регистрируется событие «Смена пароля учётной записи» (см. Журналирование событий)

2.1.7.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A64001	Заголовок команды
4	1	xx	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxxx	Идентификатор учётной записи
13	xx	xxxxxxxxxx	Значение нового пароля

2.1.7.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	1	0x00 - пароль 0x01 - ключ	-
1	2	9000	SW-ответ

2.1.8. Перейти в режим гостя

Команда доступна в любом режиме.

Сбрасывается флаг аутентификации текущей учётной записи.

ВАЖНО! Состояние защищённого канала не меняется.

2.1.8.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A64002	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.8.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.9. Перезагрузить устройство

Команда доступна только аутентифицированной учётной записи.

Операция реализуется с помощью IPC-сообщения *VSC_ITEM_SD_RESTART_DEVICE*, которое запускает таймер на 1 секунду, по прерыванию которого перезагружается USB-изделие.

2.1.9.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A63000	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.9.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.10. Начать установку защищённого канала

Команда доступна в любом режиме.

Повторная установка защищённого канала недоступна до закрытия текущего.

2.1.10.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A62000	Заголовок команды
4	1	48	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

Смещение	Длина, байт	Значение, hex	Примечание
9	4	xxxxxxxx	Идентификатор учётной записи
13	64	xxxxxxxxxx	Значение сообщения U1

2.1.10.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	64	xxxxxxxxxx	Значение сообщения U2
64	2	9000	SW-ответ

2.1.11. Завершить установку защищённого канала

Команда доступна в любом режиме, после выполнения команды Завершить установку защищённого канала.

В случае неуспешной проверки переданного значения MAC, в журнале событий регистрируется «Неуспешная аутентификация учётной записи» (см. Журналирование событий), а также «Блокирование пароля учётной записи» (см. Журналирование событий), если значение «Счётчик неудачных попыток, идущих подряд» равен 0 (см. Счётчики аутентификации).

2.1.11.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A62001	Заголовок команды
4	1	24	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	32	xxxxxxxxxx	Значение MACA

2.1.11.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	32	xxxxxxxxxx	Значение MACB
32	2	9000	SW-ответ

2.1.12. Изменить статус защищённого канала

Команда доступна в любом режиме работы.

Защищённый канал не создан (00h) – в этом статусе команды доступны только по открытому каналу.

Защищённый канал создан (02h) – в этом статусе команды доступны как по ЗК, так и по открытому каналу.

Защищённый канал в эксклюзивном режиме (03h) – в этом статусе команды доступны только по ЗК.

2.1.12.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A62002	Заголовок команды

Смещение	Длина, байт	Значение, hex	Примечание
4	1	05	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	00h – Защищённый канал не создан 02h – Защищённый канал создан 03h – Защищённый канал в эксклюзивном режиме

2.1.12.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.13. Создание новой учётной записи

Команда доступна только аутентифицированной учётной записи.

Команда доступна учётной записи с полномочием «*Возможность создания новой учётной записи*» (см. Администраторские полномочия учётной записи).

Создаётся новая учётная запись с паролем по умолчанию.

В журнале регистрируется событие «*Создание новой учётной записи*» (см. Журналирование событий).

2.1.13.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61000	Заголовок команды
4	1	74	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	112	xxxxxxxxxxx	Параметры учётной записи

2.1.13.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	112	xxxxxxxxxxx	Параметры учётной записи
112	2	9000	SW-ответ

2.1.14. Смена параметров учётной записи

Команда доступна только аутентифицированной учётной записи.

Команда доступна учётной записи с полномочием «*Возможность создания новой учётной записи*» (см. Администраторские полномочия учётной записи).

Смена параметров текущей учётной записи невозможна.

2.1.14.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61001	Заголовок команды
4	1	74	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	112	xxxxxxxxxx	Параметры учётной записи

2.1.14.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	112	xxxxxxxxxx	Параметры учётной записи
112	2	9000	SW-ответ

2.1.15. Удаление учётной записи

Команда доступна только аутентифицированной учётной записи.

Удаление текущей учётной записи доступно согласно полномочию «*Возможность удаления текущей учётной записи*» (см. Администраторские полномочия учётной записи).

Удаление других учётных записей доступно согласно полномочию «*Возможность удаления любой учётной записи*» (см. Администраторские полномочия учётной записи).

В журнале регистрируется событие «*Удаление учётной записи*» (см. Журналирование событий)

2.1.15.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61002	Заголовок команды
4	1	08	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxxx	Идентификатор учётной записи

2.1.15.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.16. Обновление значения служебной информации о карте памяти

Команда доступна только аутентифицированной учётной записи.

Назначение - смена всех параметров карты памяти, если данная возможность установлена в структуре Служебная информация о карте памяти и установлено полномочие "Возможность обновления конфигурации служебной информации о карте памяти" в Администраторские полномочия учётной записи

2.1.16.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61003	Заголовок команды

Смещение	Длина, байт	Значение, hex	Примечание
4	1	F4	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	240	xxxxxxxxxx	Служебная информация о карте памяти

2.1.16.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	240	xxxxxxxxxx	Служебная информация о карте памяти
240	2	9000	SW-ответ

2.1.17. Обновление внутреннего состояния ПДСЧ

Команда доступна только аутентифицированной учётной записи.

Команда доступна согласно полномочию «Возможность обновления внутреннего состояния ПДСЧ» (см. [Администраторские полномочия учётной записи](#)).

В журнале регистрируется событие «Обновление внутреннего состояния ПДСЧ» (см. Журналирование событий).

2.1.17.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61004	Заголовок команды
4	1	30	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	36	xxxxxxxxxx	ПДСЧ для обновления внутреннего состояния ПДСЧ
45	8	xxxxxxxxxx	Имитовставка от значения ПДСЧ для обновления внутреннего состояния ПДСЧ по ГОСТ Р 34.13—2015 (ГОСТ 34.13—2018) с применением блочного шифра «Магма» по ГОСТ Р 34.12—2015 (ГОСТ 34.12—2018) с ключом 3931C96D3251E31927EA6DFDB088845D-AE1E9127191BF22FA2D9E6F9B4D5A86Ah

2.1.17.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.18. Обновление жизненного цикла

Команда доступна только аутентифицированной учётной записи.

Команда доступна согласно полномочию "Возможность изменения параметра "Жизненные циклы СПО Aladdin CryptoFlash" (см. [Администраторские полномочия учётной записи](#)).

2.1.18.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61007	Заголовок команды
4	1	05	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Жизненные циклы СПО Aladdin CryptoFlash

2.1.18.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	240	xxxxxxxxxx	Служебная информация о карте памяти
240	2	9000	SW-ответ

2.1.19. Установка типа шифрования диска

Команда доступна только аутентифицированной учётной записи.

Параметры вступают в силу после перезагрузки устройства.

Команда доступна согласно полномочию «Возможность изменения типа шифрования диска» (см. [Администраторские полномочия учётной записи](#)).

Если меняется тип шифрования диска, автоматически, выставляется блокирование режима чтение/запись защищенных разделов.

2.1.19.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61008	Заголовок команды
4	1	06	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Порядковый номер диска
10	1	xx	Тип шифрования диска

2.1.19.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	240	xxxxxxxxxx	Служебная информация о карте памяти
240	2	9000	SW-ответ

2.1.20. Генерация нового ключа шифрования дисков

Команда доступна только аутентифицированной учётной записи

Генерируется новое значение ключа шифрования разделов K1.

Если учётных записей больше одного, то K1 сохраняется на старом значении ключа K0.

Если учётная запись только одна, генерируется новое значение ключа K0, на котором сохраняется ключ K1

Счётчики DEC (*Little Endian*), которые хранятся в области памяти защищённого раздела, инициализируются значениями 0x00000000.

Если режим чтения/записи раздела был заблокирован по причине превышения максимального количества перезаписи сектора - разблокируется.

2.1.20.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61009	Заголовок команды
4	1	4	Размер данных команды
5	4	xxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.20.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.21. Сгенерировать псевдослучайную последовательность

Команда доступна в любом режиме работы.

2.1.21.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60005	Заголовок команды
4	1	05	Размер данных команды
5	4	xxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Длина псевдослучайной последовательности 00h = 256

2.1.21.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	xx	xxxxxxxxxx	Псевдослучайная последовательность
xx	2	9000	SW-ответ

2.1.22. Сообщить статус устройства

Флаг "Карта памяти зарегистрирована" является динамическим и не хранится в статусе устройства, устанавливается в ответе на APDU-команду в зависимости от жизненного цикла СПО Aladdin CryptoFlash

1. Выполнение процедуры [Детектирование замены карты памяти](#)
2. Запрос статуса устройства IPC-сообщением типа `VSC_ITEM_SD_GET_STATUS`
3. В ответе на команду устанавливается флаг «Карта памяти зарегистрирована» в зависимости от [Жизненные циклы СПО ALADDIN CRYPTOFLASH](#)

2.1.22.2. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60006	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.22.3. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxxxx	Статус работы устройства
4	2	9000	SW-ответ

2.1.23. Сбросить к заводским настройкам

Команда доступна в любом режиме работы.

Задержка в 1 секунду до проверки пароля.

В случае успешной проверки пароля:

1. Удаляются все объекты, кроме журнала.
2. Создаётся объект учётной записи, по умолчанию (метка – “Security Officer”, пароль – ‘1234567890’, идентификатор – 00000000h).
3. Создаётся объект с паролем по умолчанию для сброса к заводским настройкам (*пароль – ‘1234567890’*).
4. Создаётся объект для хранения текущей структуры [Служебная информация о карте памяти](#).
5. Создаётся объект для хранения внутреннего состояния ПДСЧ.
6. В журнале регистрируется событие «Сброс к заводским настройкам» (см. [Журналирование событий](#)).
7. Выполняется очистка съёмных дисков карты памяти.
8. Если режим чтения/записи разделов был заблокирован по причине превышения максимального количества перезаписи сектора - разблокируется.

2.1.23.2. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A64003	Заголовок команды
4	1	xx	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	xx	xxxxxxxxxx	Значение пароля сброса к заводским настройкам

2.1.23.3. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.24. Смена пароля сброса к заводским настройкам

Команда доступна в любом режиме работы.

2.1.24.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A64004	Заголовок команды
4	1	xx	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Длина текущего пароля
10	xx	xxxxxxxxxx	Текущее значение пароля сброса к заводским настройкам
xx	1	xx	Длина нового пароля (6 – 32)
xx	xx	xxxxxxxxxx	Новое значение пароля сброса к заводским настройкам

2.1.24.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.25. Чтение журнала событий

Команда доступна только аутентифицированной учётной записи.

Команда доступна согласно полномочию «*Возможность чтения журнала*» (см. [Администраторские полномочия учётной записи](#)).

Если журнал **не переполнен** доступны данные для чтения до значения «*Текущее смещение записи нового события*» (см. [Параметры журнала](#)).

Если журнал **переполнен** доступны данные для чтения до значения «*Максимальный размер журнала событий*» (см. [Параметры журнала](#)).

2.1.25.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60007	Заголовок команды
4	1	09	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxxxxx	Смещение в журнале
13	1	xx	Длина данных для чтения. 00h = 256

2.1.25.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	xx	xxxxxxxxxxxx	Считанные данные

Смещение	Длина, байт	Значение, hex	Примечание
xx	2	9000	SW-ответ

2.1.26. Обновление параметров журнала событий

При обработке данной команды:

1. Изменяется размер объекта *FILE_NAME_JOURNAL*, если поле «Максимальный размер журнала событий» отличается от текущего значения
2. Переданное значение «Текущее смещение записи нового события» игнорируется и устанавливается в 16
3. Переданное значение [Байт статуса журнала](#) игнорируется и устанавливается в значение 0
4. Поле [Байт настроек журнала](#) устанавливается в значение переданное в APDU-команде
5. Регистрируется «Очистка журнала событий» (см. [Журналирование событий](#))

2.1.26.2. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61005	Заголовок команды
4	1	14	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	16	xxxxxxxxxx	Параметры журнала

2.1.26.3. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	16	xxxxxxxxxxxx	Параметры журнала
16	2	9000	SW-ответ

2.1.27. Обновление статуса подключения диска

Команда доступна только аутентифицированной учётной записи.

Команда доступна согласно полномочию на обновление статуса диска (см. [Полномочия учётной записи для работы с разделами карты памяти](#)).

Команда доступна только в режиме «Работа» (см. [Жизненные циклы СПО ALADDIN CRYPTOFLASH](#)), который проверяется после выполнения операции [Детектирование замены карты памяти](#).

Если в Флаги настроек раздела карты памяти указано, что данные подключаемого раздела шифруются, необходимо активировать [Модуль шифрования](#).

Если подключение диска доступно, то оно производится с помощью IPC-сообщения *VSC_ITEM_SD_LUN_CHANGE_STATE*.

2.1.27.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A63001	Заголовок команды

Смещение	Длина, байт	Значение, hex	Примечание
4	1	06	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Номер диска (0..7)
10	1	xx	Статус диска: 01h – не подключён, 02h – подключён в режиме только чтения, 03h – подключён в режиме чтение/запись

2.1.27.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxxxxxx	Статус работы устройства
4	2	9000	SW-ответ

2.1.28. Очистка карты памяти

Команда доступна только аутентифицированной учётной записи, если не выставлена возможность очистки карты памяти в режиме гостя (см. [Служебная информация о карте памяти](#))

Команда доступна согласно полномочиям «*Возможность выполнения очистки всей карты памяти*» и «*Возможность выполнения очистки LUNx*» (см. [Администраторские полномочия учётной записи](#)).

2.1.28.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A61006	Заголовок команды
4	1	06	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Номер диска (0..7) , если > 7, то очистка всей памяти

2.1.28.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxxxxxx	Статус работы устройства
4	2	9000	SW-ответ

2.1.29. Сообщить количество секторов диска

Команда доступна в любом режиме работы.

Количество секторов СПО Aladdin CryptoFlash запрашивает IPC-сообщением
VSC_ITEM_SD_GET_SECTORS.

2.1.29.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60008	Заголовок команды
4	1	06	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Номер диска (0..7), если > 7, то количество секторов всей карты памяти

2.1.29.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxxxxxx	Количество секторов размером 512 байт, Little Endian
4	2	9000	SW-ответ

2.1.30. Сообщить быстродействие ключевой схемы шифрования

Команда доступна, если включён [Тестовый режим работы изделия](#), иначе возвращается SW-ответ 6A86h

Данная команда замеряет быстродействие указанной схемы шифрования дисков.

2.1.30.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A60009	Заголовок команды
4	1	0B	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Тип шифрования диска
10	1	xx	Порядковый номер раздела
11	1	xx	Порядковый номер сектора
12	1	xx	Размер сектора (значение * 512)
13	1	xx	Количество секторов для записи
14	1	xx	Общий объём данных для шифрования, МБ
15	1	xx	Скорость чтения/записи по USB без шифрования, МБ

2.1.30.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxxxxxx	Общее время замера (миллисекунды), Little Endian
4	4	xxxxxxxxxxxx	Скорости шифрования ключевой схемы (КБ/с), Little Endian

Смещение	Длина, байт	Значение, hex	Примечание
8	4	xxxxxxxxxxxx	Расчётные ожидаемые скорости чтения/записи по USB(КБ/с), Little Endian
12	2	9000	SW-ответ

2.1.31. Считать данные из хранилища информации об устройстве

Команда доступна в любом режиме работы.

Данная команда возвращает данные, считанные из хранилища информации об устройстве, начиная с указанного смещения.

2.1.31.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6000A	Заголовок команды
4	1	07	Размер данных команды
5	4	xxxxxxx	Текущие дата и время в формате UNIXTIME
9	2	xxxx	Смещение в хранилище информации (Little Endian)
11	1	xx	Количество ожидаемых данных в байтах. Максимум 251

2.1.31.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	xx	xxxxxxxxxxxx	Считанные данные
xx	2	9000	SW-ответ

2.1.32. Записать данные в хранилище информации об устройстве

Команда доступна только в режиме аутентифицированной учётной записи администратора.

Данная команда записывает данные в хранилище информации об устройстве, начиная с указанного смещения.

2.1.32.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6100A	Заголовок команды
4	1	xx	Размер данных команды
5	4	xxxxxxx	Текущие дата и время в формате UNIXTIME
9	2	xxxx	Смещение в хранилище информации (Little Endian)
11	xx	xxxxxxxxxxxx	Данные для записи

2.1.32.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.33. Удалить хранилище информации об устройстве

Команда доступна только в режиме аутентифицированной учётной записи администратора.

Данная команда удаляет хранилище информации об устройстве.

2.1.33.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6100B	Заголовок команды
4	1	4	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.33.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.1.34. Включить/отключить поддержку механизма туннелирования APDU-команд

Команда доступна только аутентифицированной учётной записи.

Данная команда включает/отключает поддержку механизма туннелирования в настройках диска (см. [Флаги настроек раздела карты памяти](#))

2.1.34.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6100C	Заголовок команды
4	1	6	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	Порядковый номер диска (0 .. 7)
10	1	xx	0 - Отключить 1 - Включить

2.1.34.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	240	xxxxxxxx	Служебная информация о карте памяти
240	2	9000	SW-ответ

2.1.35. Обновить полномочие очистки карты памяти в гостевом режиме

Команда доступна только аутентифицированной учётной записи с полномочиями на очистку всей карты памяти (см. [Администраторские полномочия учётной записи](#))

Данная команда обновляет "Полномочие на выполнение команды [Очистка карты памяти в режиме гостя ...](#) " (см. [Служебная информация о карте памяти](#))

2.1.35.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6100D	Заголовок команды
4	1	5	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	1	xx	0b00000000 - Очистка карты памяти в режиме гостя недоступна 0b00000001 - Очистка карты памяти в режиме гостя доступна для диска 0 0b00000011 - Очистка карты памяти в режиме гостя доступна для дисков 0, 1 0bxxxxxxx - ... 0b11111111 - Очистка карты памяти в режиме гостя доступна для всей карты памяти

2.1.35.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	240	xxxxxxxx	Служебная информация о карте памяти
240	2	9000	SW-ответ

2.1.36. Установить ключ администратора

- Команда доступна только аутентифицированной учётной записи "Security Officer"
- Успешное выполнение данной команды снимает ограничение на количество ввода неверного пароля. Ведение счётчиков учётной записи прекращается. Парольные политики учётной записи, также, игнорируются, кроме "Количество предыдущих значений пароля учётной записи, с которыми не должен совпадать новый".
- В случае успешной смены, Счётчики аутентификации устанавливаются в максимальные значения
- В случае успешной смены, в журнал регистрируется событие «Смена пароля учётной записи» (см. Журналирование событий)

2.1.36.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A64005	Заголовок команды
4	1	28	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	00000000	Идентификатор учётной записи

13	32	xxxxxxxxxx	Значение нового пароля
----	----	------------	------------------------

2.1.36.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	1	01	тип - ключ
1	2	9000	SW-ответ

2.1.37. Сообщить количество установленных паролей учётной записи

- Команда доступна в любом режиме.
- Возвращает количество установленных паролей учётной записи, идентификатор которой указан в поле данных APDU-команды.

2.1.37.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6000B	Заголовок команды
4	1	08	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxx	Идентификатор учётной записи

2.1.37.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4	xxxxxxxx	Количество установленных паролей (Little Endian)
4	2	9000	SW-ответ

2.1.38. Сообщить список мастер-ключей диверсификации

- Команда доступна только учётной записи администратора.
- Возвращает список мастер-ключей в виде последовательности даты и времени генерации ключей в формате UNIXTIME.

2.1.38.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6000C	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.38.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	4x	xxxxxxxx .. xxxxxxxx	Количество установленных паролей (Little Endian)
4x	2	9000	SW-ответ

2.1.39. Выполнить алгоритм диверсификации KDF_TREE_GOSTR3411_2012_256

- Команда доступна только учётной записи администратора.
- Возвращает 256-битную последовательность, полученную в результате выполнения алгоритма диверсификации KDF_TREE_GOSTR3411_2012_256 согласно Р 50.1.113—2016.

Параметры алгоритма диверсификации KDF_TREE_GOSTR3411_2012_256:

- Kin - мастер-ключ диверсификации, индекс которого указан в APDU-команде
- label - { 0x26, 0xbd, 0xb8, 0x78 }
- seed - последовательность байт, передаваемая в APDU-команде
- R - 1
- L - 256

2.1.39.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6000D	Заголовок команды
4	1	xx	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME
9	4	xxxxxxxx	Индекс мастер-ключа диверсификации (Little Endian)
13	xx	xxxx .. xxxx	последовательность байт, используемая в качестве seed

2.1.39.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	32	xxxx .. xxxx	256-битная последовательность, полученная в результате выполнения алгоритма диверсификации KDF_TREE_GOSTR3411_2012_256 согласно Р 50.1.113—2016
32	2	9000	SW-ответ

2.1.40. Генерация мастер-ключа диверсификации

- Команда доступна только учётной записи администратора.
- Генерируется новое значение и добавляется в список мастер-ключей.
- Новое значение мастер-ключа сохраняется в области памяти неактивированного мастер-ключа (то есть, индекс которого ни разу не передавался в команде Выполнить алгоритм диверсификации KDF_TREE_GOSTR3411_2012_256), тем самым заменяя его.
- Если все сгенерированные ключи активированы, то новое значение мастер-ключа добавляется в конец списка.

2.1.40.1. CAPDU-команда

Смещение	Длина, байт	Значение, hex	Примечание
0	4	80A6000E	Заголовок команды
4	1	04	Размер данных команды
5	4	xxxxxxxx	Текущие дата и время в формате UNIXTIME

2.1.40.2. RAPDU-ответ

Смещение	Длина, байт	Значение, hex	Примечание
0	2	9000	SW-ответ

2.2. Список SW-ответов СПО Aladdin CryptoFlash

Наименование	Значение, hex
Отсутствуют криптографические библиотеки	6504
Ошибка работы с файловой системой	6581
Некорректная длина APDU-команды	6700
В APDU-команде отсутствует поле «UNIXTIME»	6701
Требуется сброс аутентификации учётной записи	6702
Введён некорректный пароль	6703
Учётная запись заблокирована	6704
Учётная запись с указанным идентификатором уже существует	6705
Учётная запись с указанной меткой уже существует	6706
Учётная запись не существует	6707
Требуется предварительная аутентификация	6708

Наименование	Значение, hex
Генерация псевдослучайной последовательности завершена с ошибкой	6709
Некорректные данные команды	670B
Отсутствуют полномочия на выполнение команды	670F
Устройство не инициализировано для выполнения переданных команд	6710
Пароль не соответствует парольным политикам	671E
Требуется смена пароля текущей учётной записи	671F
Некорректная команда защищённого канала	6721
Ожидается команда по защищённому каналу	6722
Некорректный тип публичного ключа для построения защищённого канала	6725
Исчерпаны счётчики для построения защищённого канала	6727
Ошибка вычисления Qb при построении защищённого канала	6751
Ошибка вычисления beta при построении защищённого канала	6752
Ошибка вычисления общего секрета при построении защищённого канала	6753
Ошибка вычисления U2 при построении защищённого канала	6754
Ошибка сравнения MAC при построении защищённого канала	6755
Необходимо обновить параметры журнала событий	6760
Необходимо предварительно отключить диск	6761

2.3. Список параметров работы СПО Aladdin CryptoFlash

2.3.1. Статус работы СПО Aladdin CryptoFlash

Бит	Значение
0..1	Статус подключения LUN0 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
2..3	Статус подключения LUN1 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)

Бит	Значение
4..5	Статус подключения LUN2 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
6..7	Статус подключения LUN3 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
8..9	Статус подключения LUN4 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
10..11	Статус подключения LUN5 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
12..13	Статус подключения LUN6 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
14..15	Статус подключения LUN7 (00 – не доступен для работы, 01 – не подключён, 10 – подключён в режиме только чтение, 11 – подключён в режиме чтение/запись)
16	Карта памяти зарегистрирована (0 – нет, 1 – да)
17 .. 24	Флаги блокировки режима чтение/запись для LUN(b-17) с соответствующим битом (0 - нет, 1 - да)
25 .. 31	Зарезервировано

2.3.2. Служебная информация о карте памяти

Служебная информация о карте памяти хранится в памяти микроконтроллера. Конкретные значения параметров определяются на этапе производства изделия.

Смещение	Длина, байт	Значение
0	4	Доступность изменения параметров карты памяти изделия: 5A5A5A5Ah – Доступно. A5A5A5A5h – Недоступно. Настройки параметров карты памяти константные
4	16	Серийный номер карты памяти (формируется при активации карты памяти)
20	4	Количество разделов карты памяти (1 – 8)
24	23	Настраиваемые параметры раздела карты памяти (LUN0)
47	23	Настраиваемые параметры раздела карты памяти (LUN1)
70	23	Настраиваемые параметры раздела карты памяти (LUN2)
93	23	Настраиваемые параметры раздела карты памяти (LUN3)
116	23	Настраиваемые параметры раздела карты памяти (LUN4)

Смещение	Длина, байт	Значение
139	23	Настраиваемые параметры раздела карты памяти (LUN5)
162	23	Настраиваемые параметры раздела карты памяти (LUN6)
186	23	Настраиваемые параметры раздела карты памяти (LUN7)
208	1	Максимальное количество учётных записей (1 .. 15)
209	1	Жизненные циклы СПО Aladdin CryptoFlash
210	4	Полномочия учётной записи для работы с разделами карты памяти (администратор)
214	1	Полномочие на выполнение команды Очистка карты памяти в режиме гостя (номер бита соответствует номеру диска)
215	1	Флаги блокировки режима чтение/запись для раздела с соответствующим битом (0 - нет, 1 - да)
216	4	Парольные политики учётной записи администратора
220	2	Максимальное значение счётчика неудачных попыток аутентификации учётной записи администратора, идущих подряд
222	2	Максимальное значение счётчика суммарных неудачных попыток аутентификации учётной записи администратора
224	12	Зарезервировано
236	4	Контрольная сумма служебной информации о карте памяти (CRC32)

2.3.2.1. Настраиваемые параметры раздела карты памяти

Смещение	Длина, байт	Значение
0	16	Наименование раздела, idProduct
16	4	Количество секторов в разделе размером 512 байт
20	2	Флаги настроек раздела карты памяти (Little Endian)
22	1	https://en.wikipedia.org/wiki/SCSI_Peripheral_Device_Type (только 00h и 1Fh)

Тип шифрования диска

Значение	Наименование
0	Без шифрования
1	Зарезервировано
2	Зарезервировано
3	Ключевая схема шифрования дисков на базе DEC Магма
4	Зарезервировано
5	Ключевая схема шифрования дисков (<i>зарезервировано</i>)

Флаги настроек раздела карты памяти

Бит	Значение
0	Съёмный диск (0 – нет, 1 – да)
1	Доступно только чтение (0 – нет, 1 – да)
2	Поддержка стандартных SCSI-команд (0 – нет, 1 – да)
3	Зарезервировано
4..7	Зарезервировано
8..10	Тип шифрования диска
11	Поддержка механизма Модуль туннелирования APDU-команд через MSCD-интерфейс (0 - нет, 1 - да)
12	Защита раздела от записи (0 - нет, 1 - да. Данный флаг доступен только для чтения) Если установлен флаг "Поддержка механизма Модуль туннелирования APDU-команд через MSCD-интерфейс": – Флаг "Защита раздела от записи" после подачи питания, автоматически, устанавливается в значение флага "Доступно только чтение". – Флаг "Доступно только чтение" сбрасывается в значение 0, разрешая чтение/запись на уровне SCSI-драйвера. – Если флаг "Защита раздела от записи" установлен, команды записи игнорируются изделием, не возвращая ошибку записи.
13..15	Зарезервировано

2.3.3. Администраторские полномочия учётной записи

Бит	Значение
0	Возможность создания новой учётной записи (0 – нет, 1 – да)
1	Возможность удаления любой учётной записи (0 – нет, 1 – да)
2	Возможность удаления текущей учётной записи (0 – нет, 1 – да)
3	Возможность смены пароля любой учётной записи (0 – нет, 1 – да)
4	Возможность настройки параметров журнала (0 – нет, 1 – да)
5	Возможность обновления внутреннего состояния ПДСЧ (0 – нет, 1 – да)
6	Возможность чтения журнала (0 – нет, 1 – да)
7	Возможность выполнения очистки всей карты памяти (0 – нет, 1 – да)
8	Возможность обновления конфигурации служебной информации о карте памяти (0 – нет, 1 – да)
9	Возможность изменения параметра «Жизненные циклы СПО Aladdin CryptoFlash» (0 – нет, 1 – да)
10	Возможность изменения типа шифрования диска (0 – нет, 1 – да)
11	Возможность выполнения очистки LUN0 (0 – нет, 1 – да)

Бит	Значение
12	Возможность выполнения очистки LUN1 (0 – нет, 1 – да)
13	Возможность выполнения очистки LUN2 (0 – нет, 1 – да)
14	Возможность выполнения очистки LUN3 (0 – нет, 1 – да)
15	Возможность выполнения очистки LUN4 (0 – нет, 1 – да)
16	Возможность выполнения очистки LUN5 (0 – нет, 1 – да)
17	Возможность выполнения очистки LUN6 (0 – нет, 1 – да)
18	Возможность выполнения очистки LUN7 (0 – нет, 1 – да)
19 .. 31	Зарезервировано

2.3.4. Полномочия учётной записи для работы с разделами карты памяти

Бит	Значение
0..1	Возможность работы с LUN0 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
2..3	Возможность работы с LUN1 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
4..5	Возможность работы с LUN2 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
6..7	Возможность работы с LUN3 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
8..9	Возможность работы с LUN4 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
10..11	Возможность работы с LUN5 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
12..13	Возможность работы с LUN6 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
14..15	Возможность работы с LUN7 (00 – не доступен для работы, 01 – доступно только отключение, 10 – доступно отключение и подключение в режиме только чтение, 11 – доступно отключение и подключение в режиме чтение/запись)
16 .. 31	Зарезервировано

2.3.5. Парольные политики учётной записи

Бит	Значение
0	Обязательное наличие прописных букв (от А до Z или от А до Я в кодировке Windows-1251, т.е. символов, коды которых находятся в диапазонах 41h–5Ah и C0h–DFh).
1	Обязательное наличие строчных букв (от а до z или от а до я в кодировке Windows-1251, т.е. символов, коды которых находятся в диапазонах 61h–7Ah и E0h–FFh)
2	Обязательное наличие цифр (от 0 до 9, т.е. символов, коды которых находятся в диапазоне 30h–39h)
3	Обязательное наличие специальных символов (!, \$, #, % и др. символов, коды которых находятся в диапазонах 20h–2Fh, 3Ah–40h, 5Bh–60h и 7Bh–7Eh)
4	Запрет пароля, состоящего из повторяющегося символа
5	Ограничение на использование пароля по умолчанию
6	Обязательная смена текущего пароля
7	Возможность смены пароля
8..12	Минимальная длина пароля (Значения меньше 6 некорректны)
13..21	Срок действия пароля пользователя (000000000 – не ограничено, .. , 111111111 – 511 дней)
22..25	Количество предыдущих значений пароля учётной записи, с которыми не должен совпадать новый (4 бита, максимум 15 паролей)
26..31	Зарезервировано

2.3.6. Параметры журнала

Смещение	Длина, байт	Значение
0	1	Метка журнала событий A5h
1	4	Максимальный размер журнала событий (Little endian)
5	4	Текущее смещение записи нового события (Little endian)
9	1	Байт статуса журнала
10	1	Байт настроек журнала
11	4	Зарезервировано
15	1	Контрольная сумма параметров журнала

2.3.6.1. Байт статуса журнала

Бит	Значение
0	Журнал переполнен
1	Доступ к скрытым разделам заблокирован в результате переполнения журнала
2	Наличие непрочитанных событий НСД

Бит	Значение
3..7	Зарезервировано

2.3.6.2. Байт настроек журнала

Бит	Значение
0	Включить механизм детектирования переполнения журнала
1	При однократном переполнении журнала производится блокировка доступа к скрытому разделу. Ротация данных журнала при этом продолжается.
2	При однократном переполнении журнала производится блокировка работы носителя. Ротация данных журнала и журналирование событий прекращается. Разблокировка выполняется аудитором.
3	Запрет администрирования носителя при наличии непрочитанных событий НСД в системном журнале.
4..7	Зарезервировано

2.3.6.3. Структура записи события в журнале

Смещение	Длина, байт	Значение
0	2	Идентификатор события
2	4	Дата и время события в Unixtime
6	10	Данные события

2.3.7. Параметры учётной записи

Смещение	Длина, байт	Значение
0	4	Идентификатор стороны В (00000000h .. 0000000Eh), Little Endian
4	64	Метка учётной записи.
68	16	Случайная последовательность для выработки производных из пароля учётной записи
84	4	Парольные политики учётной записи
88	4	Администраторские полномочия учётной записи
92	4	Полномочия учётной записи для работы с разделами карты памяти
96	12	Счётчики аутентификации
108	4	Дата и время обновления пароля в Unixtime

2.3.7.1. Счётчики аутентификации

Смещение	Длина, байт	Значение
0	2	Счётчик неудачных попыток, идущих подряд, Little Endian
2	2	Максимальное значение счётчика неудачных попыток, идущих подряд, Little Endian

Смещение	Длина, байт	Значение
4	2	Счётчик неудачных попыток, Little Endian
6	2	Максимальное значение счётчика неудачных попыток, Little Endian
8	4	Зарезервировано

2.4. Список входных функций СПО Aladdin CryptoFlash

2.4.1. Установка СПО Aladdin CryptoFlash

В СПО Aladdin CryptoFlash операции загрузки, установки, удаления СПО Aladdin CryptoFlash обеспечивает диспетчер приложений (AID: A0 00 00 04 48 FF 00 00).

Установка СПО Aladdin CryptoFlash происходит на этапе загрузки конфигурации устройства на производстве.

При установке СПО Aladdin CryptoFlash проверяется наличие гостовских библиотек.

Если библиотеки не обнаружены – возвращается ошибка.

При установке СПО Aladdin CryptoFlash передаётся [Служебная информация о карте памяти](#), которая проверяется на корректность.

Если вышеуказанная структура корректна:

1. Создаётся объект учётной записи, по умолчанию (метка - "Security Officer", пароль - '1234567890', идентификатор – 00000000h)
2. Создаётся объект с паролем по умолчанию для сброса к заводским настройкам (пароль - '1234567890')
3. Создаётся объект для хранения структуры [Служебная информация о карте памяти](#)
4. Создаётся объект для хранения журнала событий размером 16КБ
5. Создаётся объект для хранения внутреннего состояния ПДСЧ
6. Создаётся объект хранения ключа шифрования K1

Если вышеуказанная структура некорректна – возвращается ошибка о невозможности установки СПО Aladdin CryptoFlash

2.4.2. Инициализация кэша СПО Aladdin CryptoFlash

Кэш СПО Aladdin CryptoFlash очищается нулями 00h

Проверяется наличие гостовских библиотек, если их нет – возврат ошибки

2.4.3. Выбор СПО Aladdin CryptoFlash

Осуществляется командой следующего формата:

```
(line: 1, command size: 17)
--> 00 A4 04 00 0E A0 00 00 04 48 00 0B D0 A1 46 6C 61 73 68
<-- 90 00
(Reader: 0, status: 0x00000000, time: 15 ms)
```

2.4.4. Процесс работы СПО Aladdin CryptoFlash

1. Если открыт ЗК – расшифровка CAPDU-команды от терминала
2. Обработка CAPDU-команды от терминала
3. Если открыт ЗК – шифрование RAPDU-ответа для терминала
4. Возврат RAPDU-ответа терминалу

2.4.5. Deselect СПО Aladdin CryptoFlash

Не выполняется никаких действий.

2.4.6. Удаление СПО Aladdin CryptoFlash

1. [Деактивация модуля](#) шифрования
2. Удаление всех объектов файловой системы СПО Aladdin CryptoFlash

2.4.7. Освобождение кэша СПО Aladdin CryptoFlash

Очистка кэша СПО Aladdin CryptoFlash путём заполнения случайными данными.

2.5. Жизненные циклы СПО Aladdin CryptoFlash

Наименование	Значение	Примечание
Параметризация	00h	Доступность разделов в режиме чтение/запись, вне зависимости от настроек. Данный режим необходим для возможности подготовки несъёмного раздела, который доступен только для чтения. Допустим, форматировать данный раздел и сохранить в нём СПО. В данном режиме недоступно подключение скрытых разделов. Переход в данный режим автоматический при детектировании замены карты памяти Также, установка данного режима доступна командой Обновление жизненного цикла
Работа	01h	Доступность разделов в соответствии с настройками разделов Установка данного режима доступна командой «Обновление жизненного цикла»

2.6. Логика работы СПО Aladdin CryptoFlash

2.6.1. Регистрация карты памяти

Для возможности регистрации карты памяти необходимо:

1. Запросить [Статус работы устройства](#) командой [Сообщить статус устройства](#)
2. Если в [Статус работы устройства](#) не установлен флаг «Карта памяти зарегистрирована», то выполнить пункт 3, иначе карта памяти уже зарегистрирована
3. Зарегистрировать карту памяти, отправив команду [Обновление жизненного цикла](#) с указанием в данных режим «Работа». Устройство регистрирует карту памяти, запросив

её серийный номер IPC-сообщением *VSC_ITEM_SD_GET_CID* и сохранив его в соответствующем поле параметров

2.6.2. Детектирование замены карты памяти

Детектирование карты памяти – это синхронный процесс.

Триггером являются APDU-команды:

1. Сообщить статус устройства
2. Обновление статуса подключения диска
3. Обновление жизненного цикла

При обработке вышеуказанных команд, СПО Aladdin CryptoFlash проверяет текущее значение [Жизненные циклы СПО ALADDIN CRYPTOFLASH](#)

1. Если текущий жизненный цикл «Работа», то запрашивается серийный номер карты памяти IPC-сообщением типа *VSC_ITEM_SD_GET_CID*
2. Если полученное значение не соответствует серийному номеру зарегистрированной карты памяти, то в журнале регистрируется событие «Обнаружение замены карты памяти» и жизненный цикл переводится в «Параметризация»

2.6.3. Модуль шифрования

В СПО Aladdin CryptoFlash реализован модуль шифрования, который активируется при подключении скрытого защищённого раздела командой [Обновление статуса подключения диска](#).

Данный модуль содержит все типы шифрования, указанные во [Флаги настроек раздела карты памяти](#) в поле [Тип шифрования](#)

После подключения скрытых дисков, модуль будет вызываться для шифрования данных секторов диска

2.6.3.1. Активация модуля

Перед подключением скрытого защищённого раздела командой [Обновление статуса подключения диска](#), СПО Aladdin CryptoFlash выполняет активацию модуля шифрования следующим образом:

1. Запрос адреса хранения указателей на контекст модуля шифрования IPC-сообщением типа *VSC_ITEM_SD_GET_ADDR_POINTERS_FOR_CIPHER_MODULE*
2. Если модуль шифрования не был ативирован ранее, создаются контексты шифрования для всех типов, активируется модуль шифрования путём регистрации в адресе хранения указателей на функцию шифрования и на контексты криптоалгоритмов

2.6.3.2. Деактивация модуля

После отключения всех защищённых разделов командой Обновление статуса подключения диска или во время отработки Удаление СПО Aladdin CryptoFlash выполняется деактивация модуля шифрования следующим образом:

1. Запрос адреса хранения указателей на контекст модуля шифрования IPC-сообщением типа *VSC_ITEM_SD_GET_ADDR_POINTERS_FOR_CIPHER_MODULE*
2. Если модуль шифрования был ативирован ранее, то удаляются контексты шифрования для всех типов, деактивируется модуль шифрования путём регистрации в адресе хранения указателей на NULL

2.6.4. Журналирование событий

Регистрация событий ведётся в объекте *FILE_NAME_JOURNAL*

Параметры работы журнала зависят от [Байт настроек журнала](#)

По умолчанию, ведётся кольцевая регистрация событий (см. [Структура записи события в журнале](#)), то есть, при достижении максимального размера журнала, устанавливается флаг, что он переполнен, но блокировки регистрации событий нет. *Последующие записи затирают старые события.*

Ниже представлена таблица регистрируемых событий в журнале

Название	ID	Данные	Примечание
Подключение ССМНИ к СВТ	0000h	-	Данное событие регистрируется в Инициализация кэша СПО ALADDIN CRYPTOFLASH
Создание новой учётной записи	0001h	4 байта - ID текущей учётной записи 4 байта - ID созданной учётной записи	Данное событие регистрируется при успешном выполнении команды Создание новой учётной записи
Удаление учётной записи	0002h	4 байта - ID текущей учётной записи 4 байта - ID удалённой учётной записи	Данное событие регистрируется при успешном выполнении команды Удаление учётной записи
Успешная аутентификация учётной записи	0003h	4 байта - ID учётной записи	Данное событие регистрируется при успешном выполнении команды Проверить пароль
Неуспешная аутентификация учётной записи	0004h	4 байта - ID учётной записи	Данное событие регистрируется при неуспешном выполнении команды Проверить пароль Также, в Байт статуса журнала фиксируется «Наличие непрочитанных событий НСД»
Блокирование пароля учётной записи	0005h	4 байта - ID учётной записи	Данное событие регистрируется при неуспешном выполнении команды Проверить пароль , если исчерпался «Счётчик неудачных попыток, идущих подряд» (см. Счётчики аутентификации)
Обновление статуса подключения защищённого диска	0006h	4 байта - ID текущей учётной записи 1 байт – номер диска 1 байт – статус диска	Данное событие регистрируется при успешном выполнении команды Обновление статуса подключения диска
Очистка журнала событий	0007h	4 байта - ID текущей учётной записи 4 байта – количество удалённых событий	Данное событие регистрируется при успешном выполнении команды Обновление параметров журнала событий
Очистка карты памяти	0008h	4 байта - ID текущей учётной записи	Данное событие регистрируется при успешном выполнении команды Очистка карты памяти

Название	ID	Данные	Примечание
		4 байта – количество очищенных секторов	
Сброс к заводским настройкам	0009h	-	Данное событие регистрируется при успешном выполнении команды Сбросить к заводским настройкам
Смена пароля учётной записи	000Ah	4 байта - ID текущей учётной записи 4 байта - ID учётной записи, пароль которой был сменён	Данное событие регистрируется при успешном выполнении команды Сменить пароль
Инициализация защищённого раздела	000Bh	4 байта - ID текущей учётной записи	Данное событие регистрируется при успешном выполнении команд Установка типа шифрования диска или Генерация нового ключа шифрования дисков
Замена карты памяти	000Ch	-	Данное событие регистрируется при обнаружении замены карты при выполнении Детектирование замены карты памяти
Обновление внутреннего состояния ПДСЧ	000Dh		Данное событие регистрируется при успешном выполнении команды Обновление внутреннего состояния ПДСЧ

3. ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ СПО ALADDIN CRYPTOFLASH

3.1. Модуль туннелирования APDU-команд через MSCD-интерфейс

Для работоспособности изделия на стендах, которые не поддерживают CCID-интерфейс, разработан механизм туннелирования APDU-команд через MSCD-интерфейс, который по умолчанию используется на всех стендах.

Если в настройках раздела включена поддержка механизма туннелирования APDU-команд (*флаг 1 << 11. см. [Флаги настроек раздела карты памяти](#)*), то данный модуль добавляется в обработку SCSI-команд *WRITE(10)/READ(10)* - <https://www.t10.org/lists/op-num.htm>, иначе все SCSI-команды обрабатываются стандартно.

Запросить параметры изделия возможно стандартной SCSI-командой *INQUIRY(12)*, в ответ на которую возвращается [Структура данных ответа на SCSI-команду INQUIRY \(12h\)](#).

Порядковый номер сектора раздела, через который туннелируются APDU-команды, не фиксированный, а определяется автоматически наличием корректной структуры туннелирования при обработке команды *WRITE(10)*.

В рамках управляющего СПО использование механизма туннелирования возможно двумя способами:

1. Чтение/запись любого файла и туннелирование APDU-команд по смещению, которое кратно 512.
2. Чтение/запись любого сектора и туннелирование команд по смещению 0.

Предпочитаемым вариантом является чтение/запись через файл, так как, в таком случае, не потребуются полномочия суперпользователя в Линукс.

Для корректной работы механизма туннелирования APDU-команд, файл должен открываться на чтение или запись как бинарный объект в эксклюзивном режиме без кэширования. Допустимо использование самого исполняемого файла СПО в качестве туннеля APDU-команд.

При туннелировании APDU-команд используется метка "*CCID2MSCD*", смещение которой всегда кратно 512 в буфере отправляемых данных на запись командой *WRITE(10)*, наличие которой запускает процедуру туннелирования APDU-команд.

Обработка SCSI-команды *WRITE(10)* на уровне изделия, если включена поддержка механизма туннелирования:

1. Проверка наличия метки и корректности структуры для запуска процедуры туннелирования.
2. Если запущена процедура туннелирования, фиксирование порядкового номера сектора и запуск обработки CAPDU-команды.
3. Если процедура туннелирования не запущена и отсутствует "*Защита раздела от записи*" (см. [Флаги настроек раздела карты памяти](#)), запись полученных данных на карту памяти.
4. Последующее чтение SCSI-командой *READ(10)* зафиксированного сектора на этапе 2, возвращает RAPDU-ответ и завершает процедуру туннелирования.

Структура механизма туннелирования имеет следующий вид:

Наименование	Смещение	Размер	Примечание
Метка механизма	0	12	“CCID2MSCD” – отправка APDU-команды (заполняется управляющим СПО, проверяется изделием при записи) “MSCD2CCID” – получение RAPDU-ответа (заполняется изделием, проверяется управляющим при чтении)
Заголовок APDU	12	4	Заполняется изделием при получении APDU-команды на обработку и возвращает данное значение вместе с RAPDU-ответом для возможности контроля со стороны СПО, что RAPDU-ответ соответствует отправленной APDU-команде
Длина данных	16	4	Длина APDU-команды (<i>Little Endian</i> , максимум 261) или RAPDU-ответа (<i>Little Endian</i> , максимум 258).
Статус обработки APDU-команд	20	4	0xA5A5A5A5 – Обработка APDU-команды не завершена 0x00000000 – обработка APDU-команды завершена
Зарезервировано	24	32	-
CRC32 от опциональных данных	56	4	Контрольная сумма APDU-команды или RAPDU-ответа (<i>Little Endian</i>)
CRC32	60	4	Контрольная сумма данной структуры, не включая опциональные данные, то есть смещение от 0 до 60 (<i>Little Endian</i>)
Опциональные данные	64	0 - 261	Данные отсутствуют (в случае, если обработка APDU-команды не завершена - 0 байт) APDU-команда (минимум 4 байта, максимум 261 байт) RAPDU-ответ (минимум 2 байта, максимум 258 байт)

Примечание:

Отправка APDU-команды с заголовком hex: 00 00 00 00, эмулирует смарт-карточный PowerOff-PowerOn.

При обработке данной команды изделие перезагружает смарт-карточную систему и возвращает в ответе значение ATR

3.2. Структура данных ответа на SCSI-команду INQUIRY (12h)

Изделие в ответ на стандартную SCSI-команду INQUIRY(12h) возвращает следующую структуру данных из 58 байт:

Бит	7	6	5	4	3	2	1	0
Байт								
0	PERIPHERAL QUALIFIER			PERIPHERAL DEVICE TYPE				
1	RMB	Reserved						
2	VERSION							
3	Obsolete	Obsolete	NORMACA	HISUP	RESPONSE DATA FORMAT			
4	ADDITIONAL LENGTH (N-4)							
5	SCCS	ACC	TPGS		3PC	Reserved		PROTECT
6	Obsolete	ENC SERV	VS	MULTIP	Obsolete	Obsolete	Obsolete	Obsolete
7	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	CMDQUE	VS
8	VENDOR IDENTIFICATION							
..								
15								
16	PRODUCT IDENTIFICATION							
..								
31								
32	PRODUCT REVISION LEVEL							
..								
35								
36	DRIVE SERIAL NUMBER							
..								
43								
44	Seagate fills this field with 00h							
..								
55								
56	Флаги настроек раздела карты памяти (MSB)							
57	Флаги настроек раздела карты памяти (LSB)							