УТВЕРЖДЕН
АКСФ.501490.030 91 -ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС АУТЕНТИФИКАЦИИ И ХРАНЕНИЯ ИНФОРМАЦИИ

«GUARDANT ID» версии 2

Руководство пользователя

АКСФ.501490.030 91
Версия документа 3.0

Аннотация

Настоящий документ является Руководством пользователя изделия «Программно-аппаратный комплекс аутентификации и хранения информации «Guardant ID» версии 2» (далее по тексту — ПАК «Guardant ID» v. 2. Данный документ разработан с целью удовлетворения требований к проектированию средства[1], о чем свидетельствует Таблица 1.

В состав ПАК «Guardant ID» v. 2 не входит модуль администрирования (управления). Возможности управления ограничиваются функциями, реализованными в изделии, в котором ПАК «Guardant ID» v. 2 применяется в качестве электронного идентификатора и описываются в эксплуатационной документации на это изделие (СЗИ от НСД, СДЗ и пр.).

Таблица 1 – Соответствие требований разделам документа

Содержание требования	**Раздел документа**
Требования к разработке Руководства пользователя	
На средство должно быть разработано руководство пользователя средства (при наличии пользователей средства) с описанием:	
режимов работы средства;	1.3.1
принципов безопасной работы средства;	3
функций и интерфейсов функций средства, доступных каждой роли пользователей;	2.2, 2.3
параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений;	3.2
типов событий безопасности, связанных с доступными пользователю функциями средства;	3.3
действий после сбоев и ошибок эксплуатации средства.	4

[1] Приказ ФСТЭК РФ от 30.07.2018 N 131 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

Перечень сокращений

PIN-код – аналог пароля

ПАК – программно аппаратный комплекс

ОС – операционная система

Содержание

1 Основные характеристики

1.1 Общие сведения

1.1.1 ПАК «Guardant ID» v. 2 является программно-аппаратным комплексом со встроенными средствами защиты информации и может применяться в значимых объектах критической информационной инфраструктуры 1 категории [2], в государственных информационных системах 1 класса защищённости [3], в автоматизированных системах управления производственными и технологическими процессами 1 класса защищённости [4], в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных[5], в информационных системах общего пользования II класса [6], в автоматизированных системах до класса защищенности 2А включительно для реализации следующих мер:

- многофакторная аутентификация пользователей и/или администраторов в информационных системах (ИАФ.1, ИАФ.2, ИАФ.4, ИАФ.6, ЗСВ.1 и их усиления);
- управление доступом субъектов доступа к объектам доступа (УПД.2, УПД.6).

1.1.2 ПАК «Guardant ID» v. 2 состоит из следующих компонентов:

- электронный идентификатор «Guardant ID» v.2. в форм-факторе USB-токена или USB-микротокена с предустановленным СПО Guardant ID v.2;

[2] В соответствии со статьей 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, №31, ст. 4736) и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (Собрание законодательства Российской Федерации, 2018, № 8, ст. 1204).

[3] В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от 11.02.2013 г. № 17).

[4] В соответствии с «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (приказ ФСТЭК России № 31 от 14.03.2014 г.).

[5] В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждены Приказом ФСТЭК России от 18.02.2013 г. № 21).

[6] В соответствии с «Требования о защите информации, содержащейся в информационных системах общего пользования» (утверждены Приказом ФСТЭК России от 31.08.2010 г. № 416/489).

– комплект документации.

1.1.3 Технические характеристики электронных идентификаторов «Guardant ID» v.2 приведены в Таблица 2.

Таблица 2. Характеристики аппаратной платформы

Характеристика	**Форм-фактор**	
	USB-токен	**USB-микротокен**
Интерфейс	USB 1.1+	USB 1.1+
Общий объём EEPROM	64 Кбайт	64 Кбайт
Габаритные размеры	58мм x 16мм x 8мм	17,8мм x 15,4мм x 5,8мм
Масса	6,3 г	1,6 г
Серийный номер (на корпусе)	32 бита, уникальный	32 бита, уникальный

1.1.4 Электронный идентификатор «Guardant ID» v.2. может быть представлен следующими моделями:

– Guardant ID 2.0 ндв2;

– Guardant ID 2.0 ндв2 микро.

1.2 Основные параметры и характеристики изделия[7]

1.2.1 ПАК «Guardant ID» v. 2 реализовывает следующие факторы аутентификации, необходимые для выполнения многофакторной аутентификации пользователей и/или администраторов в информационных системах (меры ИАФ.1 в части идентификации по имени пользователя и аутентификации по паролю пользователя, ИАФ.2 в части идентификации устройств в информационной системе, ИАФ.4 в части изменения аутентификационной информации (средств аутентификации), ИАФ.6 в части идентификации и аутентификации внешних пользователей, ЗСВ.1 в части идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре и их усиления):

– ПАК «Guardant ID» v. 2 обеспечивает хранение аутентификационной информации в памяти электронного идентификатора «Guardant ID»;

[7] Основные параметры и характеристики, которыми должен обладать ПАК «Guardant ID» v. 2, указаны в соответствии с требованиями приказов ФСТЭК России № 31 от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», № 17 от 11 февраля 2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и № 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, а также методического документа от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»).

- ПАК «Guardant ID» v. 2 обеспечивает программный интерфейс для выполнения операций чтения, записи и удаления над аутентификационными данными, хранящимися в памяти электронного идентификатора «Guardant ID»[8];
- ПАК «Guardant ID» v. 2 требует предъявление PIN-кода пользователя при доступе к аутентификационной информации, хранящейся в памяти электронного идентификатора «Guardant ID»;
- ПАК «Guardant ID» v. 2 проверяет соответствие значения предъявленного PIN-кода пользователя установленному эталонному значению PIN-кода пользователя;
- доступ к аутентификационной информации, хранящейся в памяти электронного идентификатор «Guardant ID», предоставляется только в случае совпадения значения предъявленного PIN-кода пользователя и эталонного значения PIN-кода пользователя[9].

1.2.2 ПАК «Guardant ID» v. 2 задает минимальную и максимальную длину PIN-кода в пределах от 1 до 31 байта. При использовании в качестве PIN-кода символьных строк в PIN-коде поддерживаются печатные (стандартные) символы ASCII с кодом символа от 33 ("восклицательный знак") до 126 ("~"), т.е. символы латиницы нижнего и верхнего регистров, десятичные цифры, а также символы, не принадлежащие к алфавитно-цифровому набору (спецсимволы). При этом задается минимальная сложность PIN-кода с определяемыми требованиями к сочетанию букв верхнего и нижнего регистра, цифр и специальных символов. (ИАФ.4 в части установления характеристик пароля).

1.2.3 В ПАК «Guardant ID» v. 2 установлено ограничение количества последовательных неуспешных попыток ввода PIN-кода пользователя и/или PIN-кода администратора и обеспечено блокирование электронного идентификатора «Guardant ID» при превышении пользователем или администратором ограничения количества неуспешных попыток ввода PIN-кода (УПД.6 в части ограничения количества неуспешных попыток входа в информационную систему).

[8] Указанная аутентификационная информация, которой владеет пользователь или администратор информационной системы, используется при реализации многофакторной аутентификации в информационной системе (обеспечивается фактор «владения»).

[9] PIN-код пользователя применяется для подтверждения факта того, что используемая в процессе аутентификации аутентификационная информация, принадлежит пользователю или администратору информационной системы, который обладает этой информацией (фактор «знания»).

1.2.4 ПАК «Guardant ID» v. 2 обеспечивает управление доступом пользователей и администраторов информационной системы, а также программных средств информационной системы к аутентификационной информации в памяти электронного идентификатора «Guardant ID» и средствам управления ПАК «Guardant ID» v. 2 на основе специальных наборов символов - PIN-кода пользователя и PIN-кода администратора (мера защиты УПД.2 в части реализации управления доступом на основе ролей).

2 Режимы работы и функции средства

2.1 Режимы работы средства

ПАК «Guardant ID» v. 2 может функционировать в следующих режимах:

- режим «Администратор», требующий предъявления PIN-кода администратора;
- режим «Пользователь», требующий предъявления PIN-кода пользователя;
- режим «Неавторизованный пользователь», не требующий предъявления PIN-кода.

2.2 Функции средства, требующие предъявление PIN-кода

ПАК «Guardant ID» v. 2 требует предъявление PIN-кода Пользователя в следующих случаях:

- изменение своего PIN-кода;
- чтение информации из блока памяти, если для блока памяти установлен PIN-код и параметры безопасности блока требуют предъявления PIN-кода;
- запись информации в блок памяти, если для блока памяти установлен PIN-код и параметры безопасности блока требуют предъявления PIN-кода;
- изменение идентификатора блока памяти, если для блока памяти установлен PIN-код и параметры безопасности блока требуют предъявления PIN-кода;
- форматирование блока памяти, если для блока памяти установлен PIN-код и параметры безопасности блока требуют предъявления PIN-кода.

ПАК «Guardant ID» v. 2 проверяет соответствие значения предъявленного PIN-кода пользователя установленному эталонному значению PIN-кода пользователя. Выполнение вышеперечисленных операций пользователя может быть осуществлено только в случае совпадения значения предъявленного PIN-кода пользователя и эталонного значения PIN-кода пользователя.

ПАК «Guardant ID» v. 2 требует предъявление PIN-кода Администратора в следующих случаях:

- изменение своего PIN-кода;
- изменение параметров безопасности идентификатора;
- изменение параметров безопасности блока памяти;
- блокировка/разблокировка блока памяти;

- форматирование блока памяти;
- форматирование электронного идентификатора «Guardant ID».

ПАК «Guardant ID» v. 2 проверяет соответствие значения предъявленного PIN-кода администратора установленному эталонному значению PIN-кода администратора. Выполнение вышеперечисленных операций администратора может быть осуществлено только в случае только в случае совпадения значения предъявленного PIN-кода администратора и эталонного значения PIN-кода администратора.

2.3 Функции средства, доступные каждой роли пользователей

Роль	**Функция**
Пользователь	1. Изменение своего PIN-кода; 2. Чтение общей информации относительно электронного идентификатора «Guardant ID» из системной области памяти; 3. Чтение информации из блока памяти; 4. Запись информации в блок памяти; 5. Изменение идентификатора блока памяти; 6. Форматирование блока памяти.
Администратор	1. Изменение своего PIN-кода; 2. Чтение общей информации относительно электронного идентификатора «Guardant ID» из системной области памяти. 3. Изменение параметров безопасности идентификатора (метрики качества PIN-кодов, количество попыток ввода PIN-кода, время блокировки идентификатора); 4. Изменение параметров безопасности блока памяти («только чтение», «запрет записи параметров безопасности блока»); 5. Блокировка/разблокировка блока памяти; 6. Форматирование блока памяти; 7. Форматирование идентификатора.

3 Принципы безопасной работы средства

3.1 Требования и ограничения для обеспечения безопасной эксплуатации средства

Для обеспечения безопасной эксплуатации ПАК «Guardant ID» v. 2 на объектах информатизации, обрабатывающих информацию ограниченного доступа, необходимо выполнение следующих требований и ограничений:

- ПАК «Guardant ID» v. 2» может применяться в качестве идентификатора администратора и пользователей изделий, совместимость с которыми подтверждена предприятием-разработчиком ПАК «Guardant ID» v. 2». Информация о совместимых с ПАК «Guardant ID» v. 2» изделиях размещается на сайте предприятий-разработчиков www.guardant.ru и www.guardnt.ru. При невозможности публикации информации о совместимом изделии в открытом доступе она может быть предоставлена заинтересованной стороне по запросу.
- ПАК «Guardant ID» v. 2» может функционировать в среде операционных систем, BIOS (базовой системы ввода-вывода), программ начальной загрузки, и других программных средств, поддерживающих спецификацию протокола обмена данными USB 1.1 и новее.
- ПАК «Guardant ID» v. 2 должен подключаться к средствам вычислительной техники, имеющим в своем составе контроллер USB, поддерживающий работу устройств по интерфейсу USB стандарта 1.1 и новее, а также свободный USB порт.
- наличие администратора безопасности, отвечающего за правильную эксплуатацию ПАК «Guardant ID» v. 2;
- обеспечение физической сохранности средств вычислительной техники с установленным ПАК «Guardant ID» v. 2 и исключение возможности доступа к ним посторонних лиц;
- обязательная смена PIN-кода «по умолчанию» электронных идентификаторов после их инициализации;
- сохранение в секрете идентификаторов, PIN-кодов и паролей администраторов и пользователей ПАК «Guardant ID» v. 2, периодическая смена PIN-кодов и паролей;
- проведение периодической проверки на наличие актуальных уязвимостей (недостатков) в среде функционирования ПАК «Guardant ID» v. 2 с использованием средств анализа защищенности (не реже одного раза в месяц);

- отсутствие средств разработки и отладки ПО в среде функционирования ПАК «Guardant ID» v. 2;
- проведение периодической проверки среды функционирования ПАК «Guardant ID» v. 2 на наличие вредоносного ПО (не реже одного раза в месяц).

Для всех компонентов среды функционирования ПАК «Guardant ID» v. 2 должны быть установлены все актуальные обновления программного обеспечения, а также выполнены рекомендации разработчиков по безопасному конфигурированию, либо приняты меры по защите информации, нейтрализующие уязвимости.

Перед эксплуатацией ПАК «Guardant ID» v. 2 необходимо внимательно ознакомиться с содержанием эксплуатационной документации на ПАК «Guardant ID» v. 2 и изделия, совместно с которыми планируется применять ПАК «Guardant ID» v. 2.

ВНИМАНИЕ!

Утрата PIN-кода администратора приводит к невозможности выполнения с электронным идентификатором операций, требующих предъявления указанного PIN-кода.

3.2 Настройка параметров безопасности средства

Настройка параметров безопасности выполняется через интерфейс изделия, в котором ПАК «Guardant ID» v. 2 применяется в качестве идентификатора администратора и пользователей.

Выполнение настройки параметров безопасности ПАК «Guardant ID» v. 2 может быть осуществлено только Администратором при совпадении значения предъявленного PIN-кода администратора и эталонного значения PIN-кода администратора.

Для настройки доступны следующие параметры:

- параметры сложности PIN-кода;
- максимальное количество попыток ввода неправильного PIN-кода;
- минимальная длина PIN-кода;
- время блокировки идентификатора [10] (при достижении значения параметра «максимальное количество попыток ввода неправильного PIN-кода»).

Допустимые и рекомендованные значения параметров безопасности приведены в Таблица 3.

[10] Обратный отсчёт времени блокировки идентификатора осуществляется только в тот период времени, когда заблокированный идентификатор подключен к работающему USB-порту компьютера.

Таблица 3 – Значения параметров безопасности

Наименование параметра	Значения параметров безопасности		
	Допустимые	**Рекомендованные**	**По умолчанию**
Параметры сложности PIN-кода	Использовать хотя бы 1: - цифру; - строчную букву; - заглавную букву; - специальный символ.	Использовать хотя бы 1: - цифру: Да; - строчную букву: Да; - заглавную букву: Да; - специальный символ: Да. При данных значениях сложности алфавит PIN-кода составит не менее 70 символов.	Не установлены
Максимальное количество попыток ввода неправильного PIN-кода	От 1 до 10	От 3 до 4	4
Длина PIN-кода[11], байт	От 1 до 31	Не менее 8	8
Время блокировки идентификатора, мин	От 15 до 60	15 до 60	15

3.3 Типы событий безопасности, связанные с доступными пользователю функциями средства

3.3.1 Функция возврата общей информации о ПАК «Guardant ID»

Назначение	Получение информации о номере аппаратной версии, номере протокола, номере микропрограммы, объёме памяти и номере идентификатора.
Описание функций по безопасности	ИАФ.2 Идентификация устройства ПАК Guardant ID. Возвращает уникальный идентификатор устройства ПАК «Guardant ID».
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.2 Функция инициализации ПАК «Guardant ID»

Назначение	Инициализация памяти ключа Guardant ID, установка нового PIN-код.
Описание функций по безопасности	ИАФ.1, ИАФ.2, УПД.2, ЗСВ.1 Предназначена для удаления аутентификационной, а также остальной информации, установленной пользователями и администраторами.

[11] Код одного символа ASCII определяется одним байтом, поэтому при использовании в качестве PIN-кода символьных строк в кодировке ASCII справедливо утверждение, что длина PIN-кода может составлять от 1 до 31 символа.

Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.3 Функция изменения PIN-код пользователя

Назначение	Изменяет/устанавливает новое значение PIN-кода.
Описание функций по безопасности	ИАФ.1, ИАФ.4, ИАФ.6, ЗСВ.1 Предназначена для установки нового значения PIN-кода администратора или PIN-кода пользователя (блока).
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.4 Функция записи атрибутов безопасности ПАК «Guardant ID»

Назначение	Устанавливает параметры сложности PIN-кода, значение максимального количества попыток ввода неправильного PIN-кода, время блокировки ПАК «Guardant ID».
Описание функций по безопасности	ИАФ.1, ИАФ.4, ИАФ.6, УПД.6, ЗСВ.1 Предназначена для управления параметрами безопасности ПАК «Guardant ID».
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.5 Функция чтения данных из памяти ПАК «Guardant ID»

Назначение	Считывает значение идентификационной (аутентификационной) информации из памяти ПАК «Guardant ID».
Описание функций по безопасности	ИАФ.1, ИАФ.4, ЗСВ.1 Предназначена для считывания идентификационной (аутентификационной) информации из памяти ПАК «Guardant ID».
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.6 Функция записи данных в память ПАК «Guardant ID»

Назначение	Записывает значение идентификационной (аутентификационной) информации в память ПАК «Guardant ID».
Описание функций по безопасности	ИАФ.1, ИАФ.4, ЗСВ.1 Предназначена для записи идентификационной (аутентификационной) информации в память ПАК

	«Guardant ID».
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.7 Функция записи идентификатора вендора блока памяти

Назначение	Записывает значение идентификатора вендора блока памяти ПАК «Guardant ID».
Описание функций по безопасности	ИАФ.1, ЗСВ.1 Предназначена для записи идентификатора вендора, с помощью которого происходит разграничение области памяти ПАК «Guardant ID».
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.8 Функция записи атрибутов безопасности блока памяти

Назначение	Изменяет значение атрибутов безопасности блока памяти ПАК «Guardant ID».
Описание функций по безопасности	ИАФ.1, ИАФ.4, УПД.2, ЗСВ.1 Предназначена для записи атрибутов безопасности отдельного блока памяти ПАК «Guardant ID».
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.9 Функция блокировки/разблокировки блока памяти

Назначение	Управляет доступностью отдельного блока памяти.
Описание функций по безопасности	ИАФ.1, ИАФ.4, УПД.2, ЗСВ.1 Предназначена для управления доступом к блоку памяти, а соответственно и идентификационной (аутентификационной) информации содержащейся в нём.
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.10 Функция установки признака проверки PIN-кода для блока памяти

Назначение	Устанавливает/снимает признак проверки PIN-кода для блока памяти.
Описание функций по безопасности	ИАФ.1, ИАФ.4, УПД.2, ЗСВ.1 Предназначена для установки признака проверки PIN-кода при доступе к блоку памяти.

Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

3.3.11 Функция инициализации блока памяти

Назначение	Инициализирует блок памяти ключа, сбрасывает значение PIN-кода блока и флагов управления доступом к блоку памяти.
Описание функций по безопасности	ИАФ.1, ЗСВ.1 Предназначена для удаления идентификационных (аутентификационных) данных их памяти блока.
Сообщения об ошибках	Сообщения об ошибках приведены в Приложении 1.

4 Действия после сбоев и ошибок эксплуатации средства

В случае возникновения сбоев и ошибок эксплуатации средства необходимо:

1. В эксплуатационной документации на изделие, в котором ПАК «Guardant ID» v. 2 применяется в качестве идентификатора администратора и пользователей (далее-совместимого изделия), найти описание возникшей нештатной ситуации и действий по ее устранению. При необходимости – обратиться в службу технической поддержки предприятия-изготовителя совместимого изделия.
2. В случае, если служба технической поддержки предприятия-изготовителя совместимого изделия определила, что нештатная ситуация вызвана сбоем (ошибкой) функционирования ПАК «Guardant ID» v. 2 - необходимо обратиться в техническую поддержку предприятия-изготовителя ПАК «Guardant ID» v. 2:
   115088, г. Москва, ул. Шарикоподшипниковская, дом 1, этаж 4, пом. IX, комн. 11
   Телефон: 8 (495) 925-7790
   E-mail: info@guardant.ru.

Предприятие-изготовитель оказывает базовую техническую поддержку ПАК «Guardant ID» v. 2. В рамках базовой технической поддержки предприятие-изготовитель обеспечивает поиск, анализ и устранение недостатков ПАК «Guardant ID» v. 2 на протяжении срока действия базовой технической поддержки.

Базовая техническая поддержка входит в стоимость поставляемого ПАК «Guardant ID» v. 2 и обеспечивается предприятием-изготовителем. Срок базовой технической поддержки определяется сроком действия сертификата соответствия ФСТЭК России и может быть продлен по окончании срока действия сертификата соответствия.

Иные виды технической поддержки (расширения сервисов технической поддержки) предоставляются предприятием-изготовителем на возмездной основе, в соответствии с действующими политиками и правилами оказания технической поддержки продуктов предприятия-изготовителя.

Об окончании производства и базовой технической поддержки ПАК «Guardant ID» v. 2 предприятие-изготовитель информирует потребителей не позднее, чем за 1 год до окончания производства и поддержки следующими способами:

- публикацией соответствующей информации на сайте предприятия-изготовителя;
- направлением электронных писем на электронные почтовые адреса потребителей.

Приложение 1

Сообщения об ошибках функций безопасности средства приведены в Таблица 4.

Таблица 4 – Сообщения об ошибках функций безопасности

Код ошибки	**Описание ошибки**
1	Guardant ID с указанным PIN не найден
4	Ошибка записи / верификации при записи
10	PIN-код не соответствует установленным метрикам
11	Ключ заблокирован из-за неправильных попыток ввода PIN-кода
12	Блок заблокирован из-за неправильных попыток ввода PIN-кода
13	Запись в блок запрещена
14	Прямая запись в дескриптор блока запрещена
17	Блок заблокирован администратором