УТВЕРЖДЕН
АКСФ.501490.030 90 -ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС АУТЕНТИФИКАЦИИ И ХРАНЕНИЯ ИНФОРМАЦИИ

«GUARDANT ID» версии 2

Руководство администратора

АКСФ.501490.030 90
Версия документа 3.0

Аннотация

Настоящий документ является Руководством администратора 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 чём свидетельствует Таблица 1.

В состав ПАК «Guardant ID» v. 2 не входит модуль администрирования (управления). Возможности администрирования 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 администратора	
На средство должно быть разработано руководство администратора средства с описанием:	
действий по приемке поставленного средства;	3
действий по безопасной установке и настройке средства;	4
действий по реализации функций безопасности среды функционирования средства.	5

[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

СВТ – средства вычислительной техники

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;
- комплект документации.

[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).

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 должен реализовывать следующие факторы аутентификации, необходимые для выполнения многофакторной аутентификации пользователей и/или администраторов в информационных системах (меры ИАФ.1 в части идентификации по уникальному номеру устройства и аутентификации по паролю (PIN-коду), 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-

[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»).

кода (УПД.6 в части ограничения количества неуспешных попыток входа в информационную систему).

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. Функции администратора средства

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 совпадения значения предъявленного PIN-кода администратора и эталонного значения PIN-кода администратора.

Функции средства, доступные роли администратора:

- изменение своего PIN-кода;
- чтение общей информации относительно электронного идентификатора «Guardant ID» из системной области памяти.
- изменение параметров безопасности идентификатора (метрики качества PIN-кодов, количество попыток ввода PIN-кода, время блокировки идентификатора);
- изменение параметров безопасности блока памяти («только чтение»);
- блокировка/разблокировка блока памяти;
- форматирование блока памяти;
- форматирование идентификатора.

3. Приемка поставленного средства

При приемке ПАК «Guardant ID» v. 2 осуществляются следующие действия:

1. Проверка комплектности поставки в соответствии с Формуляром АКСФ.501490.030 30;
2. Проверка соответствия контрольной суммы СПО ПАК «Guardant ID» v. 2, приведенной в Формуляре АКСФ.501490.030 30 и контрольной суммы эталонного СПО ПАК «Guardant ID» v. 2, указанной на сайтах предприятий-изготовителей – www.guardant.ru и www.guardnt.ru;
3. Подключение устройства «Guardant ID» v. 2 к слоту USB СВТ. После подключения на электронном идентификаторе должен включиться светодиод – это признак того, что ПАК «Guardant ID» v. 2 исправен и пригоден к эксплуатации[10].

[10] ПАК «Guardant ID» v. 2:
- представляет собой USB устройство, работа с которым в среде операционных систем семейства Windows и Linux осуществляется посредством стандартных драйверов операционной системы;
- 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.

4. Установка и настройка средства

4.1. Установка средства

Перед началом установки необходимо внимательно ознакомиться с эксплуатационной документацией на изделие, в котором ПАК «Guardant ID» v. 2 будет применяться в качестве идентификатора администратора и пользователей (в части касающейся поддержки электронных идентификаторов «Guardant ID» v. 2).

В ОС семейства Windows устройство «Guardant ID» v.2 работает по протоколу WinUsb и не требует установки проприетарных драйверов, вся работа осуществляется через штатный драйвер WinUsb, входящий с состав операционных систем Windows 7 и выше. В ОС семейства Linux устройство «Guardant ID» v.2 работает через штатный USB-драйвер операционной системы.

Для корректного распознавания операционной системой необходимо идентифицировать устройство.

В операционных системах семейства Windows для этого предназначены:

– файл конфигурации установки - grdid_dev.inf;

– файл каталога - grdid_dev_mnf_winusb.cat.

Для идентификации устройства необходимо в Диспетчере устройств найти устройство «Guardant ID» и обновить драйвер, указав на папку с вышеуказанными файлами.

В операционных системах семейства Linux для этих целей служат:

– файл правил - 95-grdid.rules;

– файл скрипта - install.sh.

Для идентификации устройства необходимо предварительно запустить скрипт установки прав пользователя install.sh.

Для повышения стабильности совместного функционирования электронных идентификаторов «Guardant ID» v.2 и СЗИ Secret Net LSP 1.11 и новее рекомендуется скопировать вспомогательный компонент libgrdidapi.so в папку /lib64 операционной системы и перезагрузить компьютер.

Указанные файлы и вспомогательный компонент доступны для скачивания на сайте разработчика ПАК «Guardant ID» v. 2 по ссылке https://guardnt.ru/gid2.html?3 и/или могут поставляться в составе стороннего программного обеспечения, поддерживающего ПАК «Guardant ID» v. 2.

4.2. 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.

ПАК «Guardant ID» v. 2 поставляется с предустановленным значением PIN-кода администратора «по умолчанию» = '**87654321**'. Для обеспечения безопасной эксплуатации ПАК «Guardant ID» v. 2 на объектах информатизации, обрабатывающих информацию ограниченного доступа, необходимо изменить PIN-код «по умолчанию» после инициализации (форматирования) изделия;

Для настройки доступны следующие параметры:

- параметры сложности PIN-кода;
- максимальное количество попыток ввода неправильного PIN-кода;
- минимальная длина PIN-кода;
- время блокировки идентификатора [11] (при достижении значения параметра «максимальное количество попыток ввода неправильного PIN-кода»).

Значения параметров безопасности приведены в Таблица 3.

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[12], байт	От 1 до 31	Не менее 8	8
Время блокировки идентификатора, мин	От 15 до 60	От 15 до 60	15

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

[12] 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.

5. Требования по 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 сайтах www.guardnt.ru и www.guardant.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 (форматирования);
- 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.