УТВЕРЖДЕН
ПФНА.501410.004 31-ЛУ

# СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА

# Dallas Lock

**(версия изделия 1.0.17)**

## Описание применения

ПФНА.501410.004 31

Листов 23

# АННОТАЦИЯ

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие «Средство доверенной загрузки уровня базовой системы ввода-вывода «Dallas Lock» ПФНА.501410.004 (далее — изделие, СДЗ УБ Dallas Lock).

В настоящем документе содержатся общие сведения о назначении изделия и программного обеспечения изделия, условиях применения, описание задачи, перечень входных и выходных данных.

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Данное руководство предназначено для пользователей (операторов) ТС, на которых установлено изделие «Средство доверенной загрузки уровня базовой системы ввода-вывода «Dallas Lock» ПФНА.501410.004 (далее — изделие, СДЗ УБ, СДЗ УБ Dallas Lock).

В руководстве содержатся сведения, необходимые пользователю для работы на компьютерах, защищённых СДЗ УБ Dallas Lock.

# 1 НАЗНАЧЕНИЕ СДЗ УБ DALLAS LOCK

## 1.1 Наименование и обозначение изделия

Наименование изделия: «Средство доверенной загрузки уровня базовой системы ввода-вывода «Dallas Lock».

Обозначение изделия: ПФНА.501410.004.

## 1.2 Общая информация

Изделие является средством доверенной загрузки уровня базовой системы ввода-вывода и представляет собой программно-техническое средство, которое встраивается в базовую систему ввода-вывода и осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, а также не препятствует доступу к информационным ресурсам в случае успешных контроля целостности своего программного обеспечения и среды функционирования, проверки подлинности пользователя и загружаемой операционной среды.

Изделие обеспечивает невозможность подключения нарушителя в разрыв между базовой системой ввода-вывода и средством доверенной загрузки для несанкционированного доступа.

СДЗ УБ Dallas Lock выполняет свои функции (включая администрирование параметров изделия и просмотр журнала) до начала загрузки штатной операционной системы (далее — ШОС).

СДЗ УБ Dallas Lock предназначено для использования на ТС (персональные и портативные компьютеры, серверы).

Изделие сертифицировано в Системе сертификации средств защиты информации по требованиям безопасности информации ФСТЭК России № РОСС RU.0001.01БИ00 на соответствие требованиям следующих документов:

- «Требования к средствам доверенной загрузки» (утвержден приказом ФСТЭК России № 119 от 27 сентября 2013 г.);
- «Профиль защиты средства доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты» ИТ.СДЗ.УБ2.ПЗ (утвержден ФСТЭК России 30 декабря 2013 г.);
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утвержден приказом ФСТЭК России № 76 от 2 июня 2020 г.) — по 2 уровню доверия.

СДЗ УБ Dallas Lock может использоваться при создании:

- защищенных автоматизированных систем до класса защищенности 2А включительно («Требования по технической защите информации, содержащей сведения, составляющие государственную тайну» (утверждены Приказом ФСТЭК России от 20 октября 2016 г. № 025));
- защищенных автоматизированных систем до класса защищенности 1Б включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- защищенных информационных систем до 1 уровня защищенности персональных данных включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
- защищенных государственных информационных систем до 1 класса защищённости включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);
- защищенных автоматизированных систем 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, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «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»);
- защищенных значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

## 1.3 Основные возможности и функции

СДЗ УБ Dallas Lock предназначено для защиты рабочих ТС от угроз безопасности информации, которые связаны со следующими процессами:

- загрузка нештатной операционной системы (далее — НШОС) и, таким образом, обход правил разграничения доступа ШОС и (или) СЗИ, работающих в среде ШОС;
- несанкционированная загрузка ШОС и получение несанкционированного доступа к информационным ресурсам;
- нарушение целостности программной среды ТС и (или) состава компонентов аппаратного обеспечения ТС в ИС;
- нарушение целостности СДЗ УБ Dallas Lock, обход нарушителем компонентов СДЗ УБ Dallas Lock;
- несанкционированное изменение конфигурации СДЗ УБ Dallas Lock;
- преодоление или обход функций безопасности СДЗ УБ Dallas Lock;
- получение остаточной информации СДЗ УБ Dallas Lock из памяти ТС после завершения работы СДЗ УБ Dallas Lock;
- получение доступа к ресурсам СДЗ УБ Dallas Lock из программной среды ТС после завершения работы СДЗ УБ Dallas Lock;
- сбои и ошибки в процессе функционирования СДЗ УБ Dallas Lock.

Также СДЗ УБ Dallas Lock обеспечивает реализацию следующих функций безопасности:

- разграничение доступа к управлению СДЗ УБ Dallas Lock;
- управление работой СДЗ УБ Dallas Lock;
- управление параметрами СДЗ УБ Dallas Lock;
- аудит безопасности СДЗ УБ Dallas Lock;
- идентификация и аутентификация;
- тестирование СДЗ УБ Dallas Lock, контроль целостности ПО и параметров СДЗ УБ Dallas Lock;
- контроль компонентов ТС;
- блокирование загрузки операционной системы (далее — ОС) средством доверенной загрузки;
- сигнализация СДЗ УБ Dallas Lock;
- обеспечение безопасности после завершения работы СДЗ УБ Dallas Lock.

## 1.4 Состав

СДЗ УБ Dallas Lock состоит из следующих компонентов:

- загрузчик среды исполнения;
- среда исполнения функций безопасности;
- оболочка функций безопасности.

Загрузчик среды исполнения проецируется в область BIOS для обеспечения получения управления над процессом загрузки компьютера. Задача загрузчика среды исполнения — запустить ШОС или выполнить чтение кода среды исполнения функций безопасности с накопителя ПЭВМ и передать ей управление.

Задачи среды исполнения функций безопасности состоят в обеспечении работоспособности оболочки функций безопасности, для чего среда исполнения предоставляет следующие сервисы:

- запуск оболочки функций безопасности;
- обеспечение доступа к файловым системам ШОС;

- обеспечение доступа к USB-устройствам;
- получение сведений о конфигурации ТС, текущего времени;
- вывод графики на экран ТС;
- обеспечение доступа к функции перезагрузки/выключения ТС;
- управление через манипулятор типа «мышь» в процессе администрирования СДЗ УБ Dallas Lock.

Оболочка функций безопасности реализует полезный функционал СДЗ УБ Dallas Lock, связанный с основной задачей, и состоит из следующих подсистем:

- самодиагностики;
- управления доступом;
- администрирования;
- идентификации и аутентификации;
- контроля целостности компонентов ТС;
- регистрации и учёта.

# 2 УСЛОВИЯ ПРИМЕНЕНИЯ

СДЗ УБ Dallas Lock является программно-техническим изделием, его программный код выполняется до загрузки ШОС.

## 2.1 Технические требования

СДЗ УБ Dallas Lock исправно работает на ТС (персональных и портативных компьютерах, серверах). Минимальные аппаратные требования к ТС для установки СДЗ УБ Dallas Lock:

- процессор Intel 3 поколения (Ivy Bridge) с архитектурой Intel 64 или AMD 15 поколения (Excavator) с архитектурой AMD64;
- 4Гб оперативной памяти;
- BIOS платы должен соответствовать спецификации UEFI версии не ниже 2.3.1;
- стиль разделов диска должен быть GPT;
- клавиатура, мышь или совместимое указывающее устройство;
- видеоадаптер и монитор, поддерживающие режим Super VGA с разрешением не менее чем 800x600 точек.

**Примечание.** Работа изделия совместно с некоторыми отдельными видеоадаптерами, материнскими платами или контроллерами накопителей может выполняться некорректно.

Реализована поддержка наиболее распространенных файловых систем, включая: FreeBSD UFS/UFS2, Solaris UFS, FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3.

СДЗ УБ Dallas Lock поддерживает следующие виды аппаратных идентификаторов:

- USB-ключи и смарт-карты Aladdin eToken Pro/Java[1];
- USB-ключи и смарт-карты Рутокен (Рутокен ЭЦП, Рутокен ЭЦП 2.0, Рутокен ЭЦП 3.0, Рутокен Lite);
- электронные ключи Touch Memory (iButton);
- USB-ключи и смарт-карты ESMART (ESMART Token, ESMART Token ГОСТ);
- USB-ключи и смарт-карты JaCarta (JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta PKI);
- USB-ключи Guardant ID 2.0.

## 2.2 Пользователи СДЗ УБ Dallas Lock

В зависимости от предоставленных полномочий, каждая учётная запись пользователя может быть отнесена к одной из трех категорий:

- «Администратор» — пользователь, ответственный за управление СДЗ УБ Dallas Lock. Входит в группу пользователей «Администраторы». Эту функцию могут выполнять и несколько сотрудников подразделения информационной безопасности предприятия;
- «Аудитор» — пользователь, имеющий права на просмотр всех установленных параметров безопасности СДЗ УБ Dallas Lock без возможности их редактирования. Входит в группу пользователей «Аудиторы»;
- «Пользователь» — пользователь защищенного персонального компьютера, не имеющий полномочий на администрирование системы защиты, осуществляющий ввод и обработку информации любыми программными средствами. Входит в группу «Пользователи».

[1] Кроме eToken с 32-мя килобайтами памяти.

# 3 ОПИСАНИЕ ЗАДАЧИ

## 3.1 Подсистема самодиагностики

При включении ТС изделие выполняет функцию самодиагностики для определения возможности выполнять свои функции.

Если диагностика выполнена успешно, пользователю предоставляется возможность пройти авторизацию в новом окне. В журнал заносится запись об инициализации системы с результатом «ОК».

Если в процессе самодиагностики обнаружены неисправности и сбои, ТС выводит соответствующее сообщение и выключается.

Также имеется возможность проверки работоспособности памяти аппаратного идентификатора.

Изделие позволяет администратору проводить самотестирование работоспособности ФБО СДЗ УБ Dallas Lock по требованию. Для этого в оболочке администратора во вкладке «Сервис» предусмотрен пункт меню «Тестирование функций СДЗ». В действие функции самотестирования включены следующие процедуры:

- получение информации о СДЗ УБ Dallas Lock;
- создание ресурсов с назначенным контролем целостности;
- тестирование подсистемы контроля целостности;
- удаление временных ресурсов для тестирования;
- тестирование работы подсистемы создания пользователя;
- тестирование подсистемы идентификации и аутентификации;
- удаление пользователя;
- тестирование подсистемы аудита событий.

Результаты самотестирования отражаются в окне «Автоматическое тестирование функций СДЗ» в виде отчета, который можно сохранить в формате *.txt. Также результат самотестирования фиксируется в журналах «Администрирование», «Все».

## 3.2 Подсистема управления доступом

Изделие позволяет блокировать загрузку операционной системы при следующих событиях:

- выявлении попыток загрузки нештатной операционной системы;
- превышении числа неудачных попыток аутентификации пользователя;
- нарушении целостности средства доверенной загрузки, загружаемой программной среды, состава аппаратных компонентов;
- критичных типах сбоев и ошибок, для которых требуется аварийная поддержка и восстановление и которые затрагивают функции безопасности и не могут быть устранены.

При превышении числа разрешенных неудачных попыток аутентификации пользователя, учётная запись пользователя блокируется автоматически.

Изделие совершает очистку оперативной памяти и обеспечивает недоступность ресурсов средства доверенной загрузки из программной среды ТС, информационного содержания ресурсов ТС при перезагрузке ТС с целью исключения возможности доступа к ресурсам СДЗ УБ Dallas Lock и памяти ТС после завершения работы СДЗ УБ Dallas Lock.

## 3.3 Подсистема администрирования

Локальное администрирование СДЗ УБ Dallas Lock осуществляется из окна программы администрирования — оболочки администратора, в оболочке функциональной безопасности СДЗ УБ Dallas Lock.

Также возможно администрирование СДЗ УБ Dallas Lock на удаленной рабочей станции в составе Домена безопасности в качестве клиента ЕЦУ Dallas Lock при помощи Консоли ЕЦУ. Подробнее см. «Руководство по эксплуатации» ПФНА.501410.004 РЭ.

### 3.3.1 Интерфейс программы

Оболочка администратора СДЗ УБ Dallas Lock функционирует в разрешении от 800x600 или выше, в зависимости от используемого видеоадаптера.

В главном окне оболочки администратора (рисунок 1) расположены вкладки, обеспечивающие доступ к соответствующим настройкам:

- «Сервис» — дополнительные функции СДЗ УБ Dallas Lock;
- «Пользователи» — управление учётными записями пользователей;
- «Контролируемые объекты» — контроль целостности компонентов ТС;
- «Политики безопасности» — настройка авторизации в СДЗ УБ Dallas Lock;
- «Журнал» — регистрация и аудит;
- «Параметры» — управление параметрами платы.

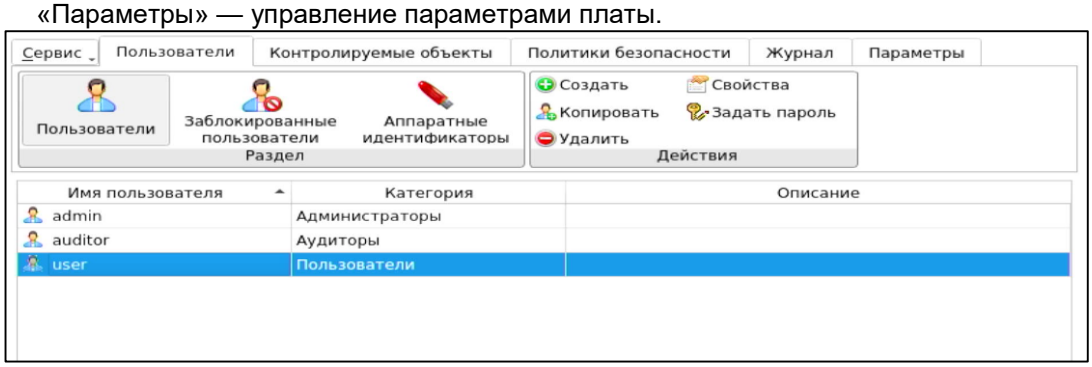


Рисунок 1 — Главное окно оболочки администратора. Пользователи

При выборе вкладки отображается соответствующий список категорийных и функциональных кнопок.

### 3.3.2 Сохранение/применение конфигурации и вывод отчетов

В оболочке администратора СДЗ УБ Dallas Lock предусмотрена функция сохранения всех параметров конфигурации СДЗ УБ Dallas Lock с данными об учетных записях пользователей, контролируемых объектах и политиках безопасности на различные носители информации, с возможностью применения сохраненной конфигурации. Данный функционал доступен только администратору СДЗ УБ Dallas Lock через меню «Сервис» в оболочке администратора.

Возможны следующие действия для пункта «Конфигурация»:

- «Сохранить» — данные об учётных записях пользователей, контролируемых объектах и политиках безопасности сохраняются в специальном файле конфигурации в формате *.xml на различные носители информации;
- «Применить» — применение сохраненных параметров конфигурации. Функция применения файлов конфигурации может использоваться в том случае, когда необходимо перенести текущие настройки основных параметров СДЗ УБ Dallas Lock на несколько автономных ТС, так как настройка параметров безопасности на каждом отдельном ТС может занимать много времени. В этом случае администратору необходимо настроить параметры СДЗ УБ Dallas Lock на одном ТС и сохранить полную конфигурацию настроек СДЗ УБ Dallas Lock, затем перенести настройки на остальные компьютеры, использовав, например, USB-накопитель с сохраненным файлом конфигурации. В случае подтверждения применения новых настроек конфигурационный файл будет применен, текущие параметры безопасности будут сброшены, параметры безопасности изменятся согласно файлу конфигурации. Система выведет уведомление об успешном применении конфигурационного файла.
- «По умолчанию» — восстановление конфигурации СДЗ УБ Dallas Lock по умолчанию. Возврат к настройкам СДЗ УБ Dallas Lock по умолчанию предполагает восстановление первоначальных значений политик безопасности, параметров контроля целостности и атрибутов учётных записей. Учётные записи, созданные при установленном СДЗ УБ Dallas Lock, после восстановления первоначальных настроек будут удалены. Применение настроек по умолчанию носит необратимый характер и эквивалентно переустановке СДЗ УБ Dallas Lock.

«Тестирование функций СДЗ» — самотестирование функций СДЗ УБ Dallas Lock. Данный пункт меню «Сервис» доступен только администраторам. При запуске самотестирования результат самотестирования отображается в окне «Тестирование основных функций СДЗ». При нажатии кнопки «Сохранить» в окне тестирования основных функций СДЗ происходит формирование отчета о тестировании в формате .txt. Результат тестирования фиксируется в журнале в категориях

«Администрирование», «Все».

«Отчет» — сохранение отчета в формате *.txt на различные носители информации. Возможно формирование отчётов «Права и конфигурация» и «Аппаратная часть». Данный функционал доступен пользователям, наделенным полномочиями администратора или аудитора.

В отчете «Права и конфигурации» указываются следующие данные:

- имя пользователя, который создал отчет;
- способ создания отчета;
- дата и время формирования отчета;
- номер сборки СДЗ УБ Dallas Lock;
- параметры конфигурации СДЗ УБ Dallas Lock в соответствии с настройками отчета.

В отчете «Аппаратная часть» указываются следующие данные:

- имя пользователя, который создал отчет;
- дата и время формирования отчета;
- номер сборки СДЗ УБ Dallas Lock;
- характеристики аппаратной конфигурации ТС (система, оперативная память, PCI-устройства, накопители, USB-устройства).

Функция сохранения отчета о конфигурации СДЗ УБ Dallas Lock может использоваться для дальнейшей проверки соответствия текущих настроек эталонным значениям.

«О СДЗ Dallas Lock» — вывод информации о версии СДЗ УБ Dallas Lock, указанного кода технической поддержки и контактов производителя. Здесь возможно сменить код технической поддержки. Возможность выводить информацию о установленном СДЗ УБ Dallas Lock доступна пользователям, которые наделены полномочиями администратора или аудитора.

### 3.3.3 Обновление СДЗ УБ Dallas Lock

Обновление изделия доступно через меню инсталлятора и производится следующим образом:

- предприятие-изготовитель доводит до потребителя информацию о выпуске обновлений изделия и устраненных в новых версиях недостатках по электронной почте письмом с вложенным документом, подписанным ЭП;
- потребитель при получении указанной информации выполняет загрузку обновления с сайта предприятия-изготовителя в виде дистрибутива, информация о контрольной сумме которого содержится на сайте предприятия-изготовителя, а также файл электронной подписи;
- перед установкой обновления потребитель выполняет проверку подлинности электронной подписи (согласно инструкции, представленной на сайте предприятия-изготовителя), расчет[1] и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте предприятия-изготовителя;
- в случае успешной проверки электронной подписи и совпадения контрольных сумм, потребитель выполняет установку обновлений. Если проверка электронной подписи и контрольных сумм не пройдена, потребитель не выполняет установку обновлений и обращается к предприятию-изготовителю изделия;
- для установки обновления необходимо записать файл обновления на USB-flash накопитель, установить подготовленный USB-flash накопитель с изделием в USB-порт ТС и запустить ТС;
- в меню инсталлятора выбрать пункт обновления и следовать указаниям инсталлятора (подробная информация описана в документе «Руководство по эксплуатации» ПФНА.501410.004 РЭ).

## 3.4 Подсистема идентификации и аутентификации

Администратор через оболочку администратора СДЗ УБ Dallas Lock имеет возможность формировать и управлять списком учётных записей пользователей СДЗ УБ Dallas Lock, а также производить необходимые настройки политик безопасности, а именно политики авторизации и политики паролей.

[1] Расчет контрольных сумм должен выполняться сертифицированными средствами с функцией расчета контрольной суммы.

### 3.4.1 Управление учётными записями пользователей

Администратор имеет возможность создавать, редактировать, копировать, удалять и задавать пароль учётным записям пользователей. Все операции по управлению учётными записями пользователей фиксируются в журнале.

Для создания или редактирования учётной записи пользователя администратор задает параметры в соответствующем разделе в окне редактирования или создания учётной записи пользователя.

В окне «Редактирование параметров пользователя» на вкладке «Общие» допустимо редактирование следующих параметров учётной записи пользователя:

- «Категория пользователя» — выбирается из выпадающего списка;
- Примечание. Штатные пользователи, допущенные к работе на защищенной рабочей станции, не должны иметь категорию «Администраторы» или «Аудиторы».
- «Описание» — предназначено для текстового описания учётной записи пользователя (не более 95 символов);
- «Расписание» — установка разрешенного времени входа пользователя в системе (подробное описание установки разрешенного времени описано в документе «Руководство по эксплуатации» ПФНА.501410.004 РЭ, п. 3.3.1 «Управление учетными записями пользователей»).

Допустимо присвоение следующих атрибутов учётной записи пользователя:

- «Отключен» — учётная запись пользователя отключается, вход в систему невозможен до снятия атрибута администратором;
- «Потребовать смену пароля при следующем входе» — при входе пользователя в систему принудительно запускается диалоговое окно смены текущего пароля;

**Примечание.** Чекбокс данного атрибута отсутствует в окне редактирования доменной учётной записи пользователя.

- «Запретить смену пароля пользователем» — запрет для пользователя на смену своего пароля, в том числе и по истечении срока действия;

**Примечание.** Присвоить два атрибута «Потребовать смену пароля при следующем входе» и «Запретить смену пароля пользователем» одновременно невозможно.

- «Бессрочный пароль» — на пользователя не распространяется действие политики безопасности, которая устанавливает максимальный срок действия пароля. Установка данного атрибута не запрещает смену пароля пользователем в любое время;

**Примечание.** Чекбокс данного атрибута отсутствует в окне редактирования доменной учётной записи пользователя.

- «Запретить работу при нарушенной целостности» — вход в систему пользователем при неуспешном прохождении процедуры контроля целостности объектов и компонентов ТС запрещается;
- «Запретить загрузку нештатной ОС» — запрет на загрузку ОС с носителя, отличного от указанного в поле «Загрузочное устройство» вкладки «Параметры» оболочки администратора.

На вкладке «Аппаратная идентификация» возможно назначение аппаратного идентификатора в следующем порядке:

- предъявить аппаратный идентификатор и выбрать его из списка;
- далее автоматически заполняются поля «Серийный номер» (серийный номер АИ), «Имя пользователя», чекбоксы «Хранить пароль» и «Пароль защищен ПИН» (в соответствии с данными, ранее записанными в память АИ);
- при необходимости нажать кнопку «Очистить» — произойдет очистка поля «Имя пользователя»;
- после нажатия кнопки «ОК» данный аппаратный идентификатор будет присвоен

редактируемой учётной записи пользователя.

В дальнейшем авторизация данного пользователя в СДЗ УБ Dallas Lock без предъявления данного АИ будет невозможна.

**Примечание.** Вкладка «Аппаратная идентификация» отсутствует в окне редактирования параметров доменной учётной записи пользователя, заданного по маске.

При необходимости возможно задать дополнительные параметры аппаратной идентификации:

- «Записать» — данная кнопка позволяет записывать в незащищенную и защищенную память АИ идентификационную и аутентификационную информацию (имя пользователя, пароль). В этом случае в окне авторизации в соответствующие поля будет подставлена записанная информация, поля будут недоступны для редактирования;

**Примечание.** Запись только идентификационной информации (имя пользователя) осуществляется по нажатию кнопки без присвоения остальных возможных атрибутов. При успешной записи в поле «Имя пользователя» отобразится имя текущей учётной записи пользователя, поле будет недоступно для редактирования.

**Примечание.** Следует учитывать, что запись информации осуществляется не на все модели аппаратных идентификаторов.

- «Хранить пароль» — данный атрибут позволяет хранить пароль в незащищённой памяти АИ. В этом случае в окне авторизации в поля «Пользователь» и «Пароль» будет подставлена хранящаяся в памяти АИ информация, поля будут недоступны для редактирования;

**Примечание.** Следует обратить внимание, что хранение пароля в незащищенной памяти АИ с точки зрения информационной безопасности нежелательно.

- «Пароль защищен ПИН» — данный атрибут позволяет хранить пароль в защищенной ПИН-кодом памяти. В этом случае в окне авторизации в поле «Пользователь» будет подставлена хранящаяся в памяти АИ идентификационная информация, а пароль будет получен из защищенной памяти АИ, если введен верный ПИН;

**Примечание.** Обязательный атрибут при использовании электронных ключей iButton в качестве АИ.

- «Сменить ПИН» — данная кнопка позволяет сменить ранее назначенный ПИН учётной записи пользователя для аппаратных идентификаторов. В окне «Изменение ПИН-кода» ввести старый, новый ПИН и повторить ввод нового ПИН;

**Примечание.** Требования к ПИН-коду АИ определяются в документации на данный АИ.

- «Форматировать» — данная кнопка позволяет провести форматирование АИ и очистить всю ранее записанную идентификационную и аутентификационную информацию.

Сохранение свойств и атрибутов учётной записи пользователя производится при нажатии кнопки «ОК».

Учётные записи пользователей, которые зарегистрированы в СДЗ УБ Dallas Lock, отображаются в виде таблицы.

Разблокировка заблокированной учётной записи пользователя осуществляется автоматически по истечении установленного времени блокировки или принудительно администратором СДЗ УБ Dallas Lock в разделе «Заблокированные пользователи».

### 3.4.2 Настройка политик безопасности

Администратор имеет возможность настроить политики безопасности для авторизации (Таблица 1) и паролей (Таблица 2) в соответствующих категориях на вкладке «Политики безопасности» оболочки администратора.

Таблица 1 — Список параметров категории «Политики авторизации»

| Параметр политики | Описание |
|---|---|
| «Отображать имя последнего вошедшего пользователя» | Возможное значение параметра: «Да/Нет». В значении «Да» в окне авторизации поле «Имя пользователя» заполняется именем учетной записи пользователя, осуществившего последний успешный вход. При значении «Нет» поле остается пустым.<br>Значение по умолчанию — «Да». |
| «Максимальное количество ошибок ввода пароля» | Установленное значение регламентирует количество попыток ввода значений пароля. В случае ввода неверного пароля появляется предупреждение. По достижении установленного значения учетная запись пользователя блокируется на определенное время, устанавливаемое параметром «Время блокировки учетной записи в случае ввода неправильных паролей».<br>Возможное значение параметра: от 1 до 10 и «Не используется» — количество попыток ввода пароля не ограничено.<br>Значение по умолчанию — «8». |
| «Время блокировки учетной записи в случае ввода неправильных паролей» | Установленное значение регламентирует время блокировки учетной записи после ввода неверного пароля более допустимого числа раз (определяется параметром «Максимальное количество ошибок ввода пароля»). В данный интервал времени вход невозможен даже при верном вводе пароля.<br>Возможное значение параметра: от 1 мин до 5 ч и «Не используется» — в таком случае разблокировка возможна только администратором.<br>Значение по умолчанию — «10 мин.». |
| «Отображать время последнего успешного входа» | Возможное значение параметра: «Да/Нет». В значении «Да» при очередном входе пользователя во время выполнения процедуры контроля целостности объектов отображается дата и время последнего успешного входа данного пользователя. В значении «Нет» — не отображается.<br>Значение по умолчанию — «Да». |
| «Время ожидания авторизации пользователя» | Время, отводимое на ввод пользователем авторизационных данных (от начала набора данных, до нажатия кнопки «ОК»). Если пользователь не успел завершить ввод авторизационных данных, то уже введенные данные очищаются.<br>Возможное значение параметра: от 1 мин до 10 мин и «Не используется» — время ожидания ввода авторизационных данных не ограничено.<br>Значение по умолчанию — «2 мин». |
| «Считывать авторизационную информацию с аппаратного ключа» | Возможное значение параметра: «Да/Нет». В значении «Нет» авторизационная информация вводится пользователем с клавиатуры. В значении «Да» |

| Параметр политики | Описание |
|---|---|
| | авторизационная информация считывается с памяти АИ в соответствии с настройками учетной записи пользователя, указанными на вкладке «Аппаратная идентификация».<br>Значение по умолчанию — «Да». |
| «Фиксировать в журнале неправильные пароли» | Возможное значение параметра: «Да/Нет». В значении «Да» неверный пароль, введенный пользователем, отображается в журнале в столбце «Описание». В значении «Нет» — не отображается.<br>Значение по умолчанию — «Нет». |
| «Автоматический выбор аппаратного идентификатора при авторизации» | Возможное значение параметра: «Да/Нет». В значении «Да» во время авторизации информация автоматически считывается с АИ. В значении «Нет» этого не происходит.<br>Значение по умолчанию — «Нет». |
| «Запретить выход из спящего режима» | Возможное значение параметра: «Да/Нет». При включении параметра в значение «Да» вместо нормального выхода из спящего режима будет произведена перезагрузка компьютера.<br>Значение по умолчанию — «Нет». |

Таблица 2 — Список параметров категории «Политики паролей»

| Параметр политики | Описание |
|---|---|
| «Максимальный срок действия пароля» | Параметр устанавливает максимальный срок действия пароля пользователей. По истечении срока действия пользователю автоматически будет предложено сменить пароль. Не распространяется на учетные записи пользователей с установленным атрибутом «Бессрочный пароль».<br>Возможное значение параметра: от 1 дня до 25 недель и «Не используется» — максимальный срок действия пароля не установлен.<br>Значение по умолчанию — «6 нед.». |
| «Минимальный срок действия пароля» | Параметр определяет минимальный срок действия пароля. Если этот срок еще не истек, смена пароля пользователем запрещена.<br>Возможное значение параметра: от 1 дня до 4 недель и «Не используется» — минимальный срок действия не установлен.<br>Значение по умолчанию — «Не используется». |
| «Напоминать о смене пароля за» | Параметр задает период до установленного максимального срока действия пароля, в который пользователю будет выводиться сообщение о необходимости смены пароля.<br>Возможное значение параметра: от 1 дня до 2 недель и «Не используется» — сообщение выводиться не будет.<br>Значение по умолчанию — «3 дн.». |
| «Минимальная длина» | Параметр устанавливает ограничение на минимальную длину пароля.<br>Возможное значение параметра: от 1 до 14 и «Не используется» — устанавливаемый пароль может иметь пустое значение.<br>Значение по умолчанию — «8 симв.». |

| Параметр политики | Описание |
|---|---|
| «Необходимо наличие цифр» | Если данный параметр включен, то при создании пароля в нем должны присутствовать цифры.<br>Возможное значение параметра: «Да/Нет».<br>Значение по умолчанию — «Нет». |
| «Необходимо наличие спецсимволов» | Если данный параметр включен, то при создании пароля в него должны быть включены специальные символы, такие как "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "\|", ":", ";", "'", "", "<", ">", ",", ".", "?", "/", "=" и прочие.<br>Возможное значение параметра: «Да/Нет».<br>Значение по умолчанию — «Нет». |
| «Необходимо наличие строчных и прописных букв» | Если данный параметр включен, то при создании пароля в него должны быть включены как строчные, так и прописные буквы.<br>Возможное значение параметра: «Да/Нет»<br>Значение по умолчанию — «Нет». |
| «Необходимо отсутствие цифры в первом и последнем символах» | Если данный параметр включен, то при создании пароля его первый и последний символ не должны являться цифрами.<br>Возможное значение параметра: «Да/Нет».<br>Значение по умолчанию — «Нет». |
| «Необходимо изменение пароля не меньше, чем в» | Если данный параметр включен, то при смене пароля новый пароль должен отличаться от старого не менее, чем на указанное количество символов. Сверка старого и нового пароля осуществляется посимвольно.<br>Возможное значение параметра: от 1 до 10 символов и «Не используется» — проверки на отличие старого пароля от нового не происходит.<br>Значение по умолчанию — «Не используется». |
| «Разрешена генерация пароля» | Возможное значение параметра: «Да/Нет». В значении «Да» пользователю дается возможность генерации паролей. В значении «Нет» у пользователя нет возможности воспользоваться генерацией пароля.<br>Значение по умолчанию — «Да». |

Следует обратить внимание, что при использовании СДЗ УБ Dallas Lock в составе ТС, предназначенного для обеспечения безопасности защищаемой информации, необходимо устанавливать параметры политик безопасности, соответствующие требованиям, предъявляемым к классам защищенности автоматизированных систем.

## 3.5 Подсистема контроля целостности компонентов ТС

СДЗ УБ Dallas Lock позволяет осуществлять контроль целостности следующих типов объектов:

- «Файловая система»;
- «Реестр»;
- «Области диска»;
- «CMOS»;
- «Таблицы SMBIOS»;
- «Таблицы BIOS»;
- «Аппаратная конфигурация»;
- «Программное обеспечение СДЗ УБ».

Просмотр контролируемых объектов конкретной категории осуществляется через соответствующие

кнопки на панели «Категория» вкладки «Контролируемые объекты».

Для контроля целостности используется метод сравнения расчётной контрольной суммы (далее — КС), полученной в момент проверки целостности, с эталонной контрольной суммой, рассчитанной в момент назначения целостности.

Для подсчёта контрольных сумм используются алгоритмы CRC32, хэш MD5, хэш ГОСТ Р 34.11-94.

### 3.5.1 Параметры контролируемых объектов файловой системы, реестра Windows и областей жесткого диска

Параметры контролируемых объектов файловой системы (далее — ФС), реестра Windows и областей жесткого диска представлены в таблице (см. таблица 3).

Таблица 3 — Параметры контролируемых объектов

| Наименование параметра | Описание |
|---|---|
| **Объекты файловой системы** | |
| «Путь» | Путь к файлу или каталогу (директорию) контролируемого объекта. Задается при добавлении объекта ФС, в дальнейшем не может быть изменен |
| «Описание» | Текстовое описание контролируемого объекта |
| «Алгоритм расчета» | Алгоритм расчета контрольной суммы объекта файловой системы |
| «Учитывать наличие» | При контроле целостности объекта файловой системы будет проверяться наличие указанного объекта. Устанавливается автоматически при установке атрибутов «Учитывать содержимое» и «Учитывать атрибуты» |
| «Учитывать содержимое» | При контроле целостности объекта файловой системы будет проверяться содержимое указанного объекта |
| «Учитывать атрибуты» | При контроле целостности объекта файловой системы будет проверяться неизменность атрибутов указанного объекта. |
| **Объекты реестра Windows** | |
| «Файл ветки реестра» | Путь к файлу реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен |
| «Путь реестра» | Путь к контролируемому объекту в указанном выше файле реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен |
| «Описание» | Текстовое описание контролируемого объекта |
| «Алгоритм расчета» | Алгоритм расчета контрольной суммы объекта реестра |
| «Рекурсивно» | При контроле целостности объекта реестра типа «Ключ» будут также контролироваться все подключи реестра. Не применимо для объектов реестра типа «Значение» |
| **Области жесткого диска** | |
| «Диск» | Наименование жесткого диска, подключенного к ТС. Задается при добавлении объекта, в дальнейшем не может быть изменен |
| «Описание» | Текстовое описание контролируемого объекта |
| «Начальный сектор» | Начальный сектор области жесткого диска |
| «Количество секторов» | Количество секторов жесткого диска, подлежащих контролю целостности |

| Наименование параметра | Описание |
|---|---|
| «Алгоритм» | Алгоритм расчета контрольных сумм при контроле целостности области жесткого диска |

Администратор имеет возможность задавать списки контролируемых объектов и производить их редактирование. Под редактированием понимается удаление элементов из списка, изменение параметров элементов списка.

Каждая запись в списке объектов состоит из следующих столбцов:

- «Идентификатор»;
- «Описание»;
- «Алгоритм»;
- «Параметры»;
- «Эталонная КС»;
- «Расчётная КС».

Механизм контроля целостности ФС позволяет осуществлять контроль объектов следующих файловых систем: FreeBSD UFS/UFS2, Solaris UFS, FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3. В СДЗ УБ Dallas Lock реализована возможность задавать контроль целостности для таких объектов файловой системы, как файл и папка.

**Примечание.** Назначать контроль целостности ФС можно только для объектов ФС, находящихся на локальных дисках, и областям локальных дисков.

### 3.5.2 Настройка контроля целостности BIOS/CMOS, таблицы SMBIOS

Кнопки в блоке «Действия» для категории «BIOS CMOS»:

- «Обновить CMOS»;
- «Сохранить».

Для категории «BIOS CMOS» форма просмотра разделена на три блока «SMBIOS», «BIOS» и «CMOS» (рисунок 2).

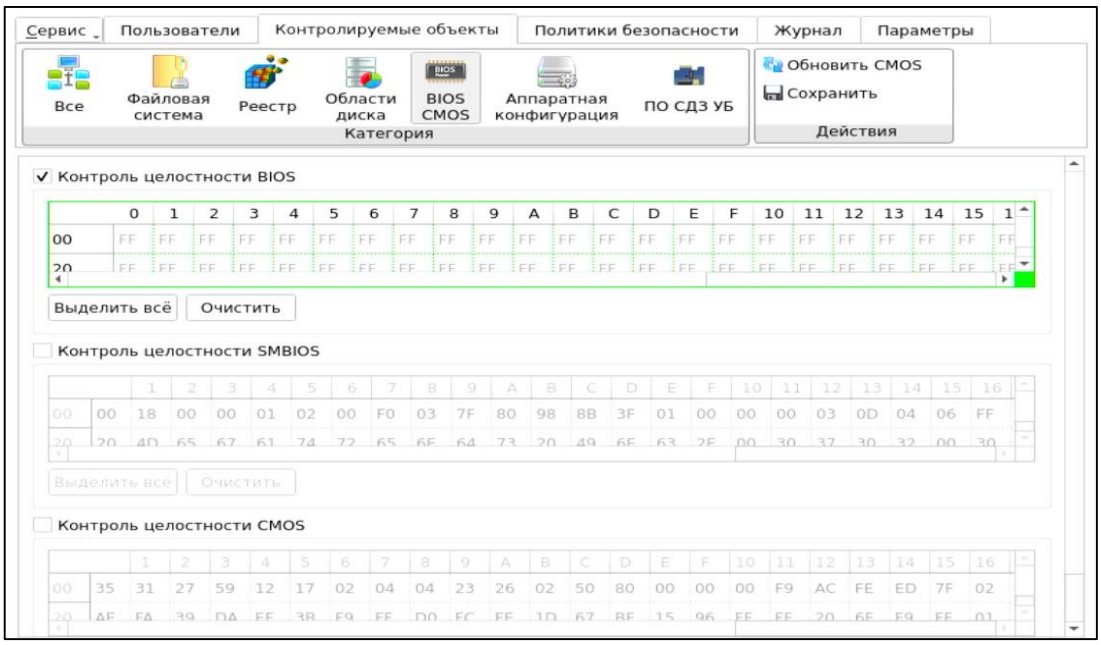


Рисунок 2 — Контроль BIOS, CMOS, «SMBIOS»

Блоки «SMBIOS», «BIOS» и «CMOS» представляют из себя три таблицы значений, в которых цветом можно выделять ячейки, для которых нужно назначить контроль, при этом установив чекбоксы «Контроль целостности SMBIOS», «Контроль целостности BIOS» и «Контроль целостности CMOS».

В блоках «SMBIOS» и «BIOS» для удобного использования предусмотрены кнопки «Выделить все» и «Очистить». В блоке «CMOS» это кнопки «Инверсия», которая заменяет назначение целостности для каждой ячейки на обратное значение, «Очистить» и «По умолчанию». На выделенные цветом ячейки назначен контроль целостности. Если ячейки красного цвета — контроль целостности для них не пройден.

### 3.5.3 Настройка контроля целостности аппаратной конфигурации

Настройка параметров контроля целостности аппаратной конфигурации осуществляется при выборе категории «Аппаратная конфигурация» на вкладке «Контролируемые объекты».

Для категории «Аппаратная конфигурация» доступны следующие функциональные кнопки:

- «Контролировать все группы» — при нажатии осуществляется инициирование контроля всех групп контролируемых объектов аппаратной конфигурации;
- «Снять контроль со всех групп» — при нажатии осуществляется прекращение контроля всех групп контролируемых объектов аппаратной конфигурации;
- «Обновить конфигурацию» — при нажатии осуществляется обновление списка устройств аппаратной конфигурации ТС;
- «Пересчитать» — при нажатии осуществляется пересчет значений целостности объектов аппаратной конфигурации;
- «Сохранить» — при нажатии осуществляется сохранение списка контролируемых объектов аппаратной конфигурации.

Для настройки контроля аппаратной конфигурации в основной области доступны соответствующие группам чекбоксы «контролировать группу» и напротив конкретного идентификатора в группе «исключить из контроля»/«включить контроль».

Для категории «Аппаратная конфигурация» выводятся списки групп аппаратной конфигурации (Таблица 4).

Таблица 4 — Пример списка групп аппаратной конфигурации

| Группа | Описание |
|---|---|
| **Объекты файловой системы** | |
| Система | Отображается информация о материнской плате, BIOS и ЦП |
| Оперативная память | Отображаются установленные модули оперативной памяти |
| PCI-Устройства | Отображаются подключённые PCI-устройства |
| Накопители | Отображаются установленные накопители |
| USB-Устройства | Отображаются различные устройства, подключённые через USB-порт, например: аппаратные идентификаторы, USB-преобразователи, USB-HID устройства |
| «Учитывать атрибуты» | При контроле целостности объекта файловой системы будет проверяться неизменность атрибутов указанного объекта. |

Каждая группа содержит свой список относящихся к ней устройств, которые подключены к ТС, если группа не содержит устройства, она также выводится.

Список устройств, входящих в ту или другую группу, содержит поля:

- «Идентификатор» — аппаратная конфигурация устройства;
- «Тип» — тип оборудования;
- «Производитель» — производитель оборудования;
- «Статус» — отображает состояние устройства. Поле заполняется при нарушении контроля целостности и может принимать два значения: «Добавлено» или «Удалено».

### 3.5.4 Настройка контроля целостности ПО СДЗ УБ Dallas Lock

Для категории «ПО СДЗ УБ» доступны следующие функциональные кнопки:

- «Проверить» — при нажатии осуществляется проверка контрольных сумм ПО СДЗ УБ Dallas Lock;
- «Сохранить» — при нажатии осуществляется сохранение выбранного алгоритма и расчет контрольных сумм ПО СДЗ УБ Dallas Lock.

Для установки контроля целостности ПО СДЗ УБ Dallas Lock необходимо установить флаг в поле «Включить контроль ПО».

Допустима установка атрибута «Алгоритм» — из выпадающего списка выбирается алгоритм расчета контрольной суммы прошивки ПО СДЗ УБ Dallas Lock.

## 3.6 Подсистема регистрации и учёта

События по администрированию СДЗ УБ Dallas Lock, события входов пользователей, события проверки целостности и редактирования учётных записей пользователей фиксируются в журнале.

Сортировка записей журнала по порядковому номеру, времени события, пользователям, в течение работы которых произошло событие, наименованию события, результату и описанию (по возрастанию/убыванию) осуществляется нажатием на заголовки соответствующих столбцов левой кнопкой мыши.

В ходе выполнения процедуры контроля целостности объектов отображается количество занятой памяти журналом (в процентах).

В журнале выделяются следующие категории событий:

- «Входы»;
- «Администрирование»;
- «Учётные записи»;
- «Целостность».

Просмотр событий конкретной категории осуществляется через соответствующие кнопки в панели «Категория».

Каждая запись журнала хранится в энергонезависимой памяти платы в преобразованном виде. При чтении записи журнала производится обратное преобразование с проверкой контрольной суммы. В случае несовпадения контрольной суммы записи выводится соответствующее предупреждение, а запись считается повреждённой.

Возможны следующие действия с журналом:

- «Фильтр» — возможность гибкой фильтрации записей журнала;
- «Очистить» — выводится диалоговое окно с предложением очистки журнала. После очистки журнала порядковая нумерация новых событий продолжается далее, а не начинается заново;
- «Экспорт» — экспортирование журнала в требуемом формате;
- «Информация» — выводится информационное окно для выбранного события.

**Примечание.** Подробное описание работы данных действий описаны в документе «Руководство по эксплуатации» ПФНА.501410.004 РЭ.

Размер журнала предусмотрен таким образом, чтобы не происходило его переполнение за время эксплуатации СДЗ УБ Dallas Lock (например, на интервал периодического контроля защищенности информации на объекте информатизации). При переполнении журнала более чем на 85% при входе в СДЗ УБ Dallas Lock выдается соответствующее предупреждение. При заполнении журнала более чем на 95% вход в систему разрешен только для администрирования СДЗ УБ Dallas Lock.

В категории «Входы» фиксируются события, связанные с процессом аутентификации в СДЗ УБ Dallas Lock:

- проверка пользователя;
- инициализация системы;
- старт ОС;

- запуск оболочки администратора;
- выход пользователя из системы;
- перезагрузка/выключение ТС;
- смена пароля.

В категории «Администрирование» фиксируются события, связанные с управлением конфигурацией и обновлением СДЗ УБ Dallas Lock:

- ввод в домен/вывод из домена безопасности ЕЦУ;
- синхронизация с ЕЦУ;
- применение конфигурации СДЗ УБ Dallas Lock/по умолчанию;
- обновление ПО СДЗ УБ Dallas Lock;
- изменение политики безопасности;
- сохранение конфигурации в файл;
- очистка журнала;
- экспорт журнала;
- установка даты-времени;
- задание загрузочного устройства;
- добавление/изменение/удаление объекта контроля целостности файловой системы;
- добавление/изменение/удаление объекта контроля целостности реестра;
- добавление/изменение/удаление объекта контроля целостности области диска;
- добавление/изменение/удаление объекта контроля целостности аппаратной конфигурации;
- добавление/изменение/удаление объекта контроля целостности программного обеспечения СДЗ УБ Dallas Lock;
- добавление/изменение/удаление объекта контроля целостности образа BIOS;
- добавление/изменение/удаление объекта контроля целостности таблицы SMBIOS;
- добавление/изменение/удаление объекта контроля целостности CMOS;
- запуск/завершение самотестирования СДЗ УБ Dallas Lock.

В категории «Учётные записи» фиксируются события, связанные с изменениями учётных записей пользователей в СДЗ УБ Dallas Lock:

- первичная регистрация учётной записи;
- повторная регистрация учётной записи;
- создание учётной записи;
- изменение учётной записи;
- задание пароля учётной записи;
- удаление учётной записи.

В категории «Целостность» фиксируются события, связанные с проверкой целостности контролируемых объектов:

- запуск/завершение контроля целостности объектов;
- контроль целостности объекта;
- пересчет целостности объекта;
- удаление объекта целостности.

В случае возникновения события, не попадающего ни под одну из категорий, в журнал заносится событие «Неизвестное событие».

# 4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными в СДЗ УБ Dallas Lock являются:

- файлы конфигураций модулей системы, используемые при установке или в процессе администрирования;
- уникальные для каждой учётной записи имя пользователя, пароль и серийный номер аппаратного идентификатора;
- ПИН-код аппаратного идентификатора;
- формализованные правила политик безопасности, реализуемые с помощью механизмов СДЗ УБ Dallas Lock и преобразованные в значения атрибутов и полномочий.

Имя учётной записи пользователя не может быть пустым и может содержать не более 31 символа. Возможные параметры пароля задаются в разделе «Политики паролей». Требования к ПИН-коду аппаратного идентификатора определяются в документации на данный аппаратный идентификатор.

В качестве выходных данных в СДЗ УБ Dallas Lock выступают:

- сообщения СДЗ УБ Dallas Lock на действия пользователей;
- журнал, создаваемый СДЗ УБ Dallas Lock в процессе работы;
- значения контрольных сумм объектов, на которых установлен контроль целостности;
- сохраненные параметры конфигурации СДЗ УБ Dallas Lock, сформированные в процессе администрирования;
- паспорт аппаратной части ТС;
- отчеты результатов самодиагностики СДЗ УБ Dallas Lock.

# ТЕРМИНЫ И СОКРАЩЕНИЯ

Некоторые термины, содержащиеся в тексте руководства, уникальны для СДЗ УБ Dallas Lock, другие используются для удобства, третьи выбраны из соображений краткости.

| | |
|---|---|
| **АИ** | аппаратный идентификатор |
| **ЕЦУ** | Единый центр управления |
| **КС** | контрольная сумма |
| **НШОС** | нештатная операционная система |
| **ОС** | операционная система |
| **ПИН (ПИН-код)** | пароль, предоставляющий доступ к защищенной памяти АИ |
| **ПО** | программное обеспечение |
| **СВТ** | средство вычислительной техники |
| **СДЗ УБ** | средство доверенной загрузки уровня базовой системы ввода-вывода |
| **ТС** | техническое средство |
| **ЦП** | центральный процессор |
| **ШОС** | штатная операционная система |
| **ФБО** | функция безопасности объекта оценки |
| **ФС** | файловая система |
| **ФСТЭК России** | Федеральная служба по техническому и экспортному контролю |