СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ
«Dallas Lock»

Описание применения

ПФНА.501410.003 31

АННОТАЦИЯ

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие «Средство доверенной загрузки «Dallas Lock» ПФНА.501410.003 (далее по тексту – изделие, СДЗ Dallas Lock).

В настоящем документе содержатся общие сведения о назначении изделия, условиях применения, а также описаны основные задачи программной части изделия.

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

АИ	аппаратный идентификатор
АС	автоматизированная система
ДСЧ	датчик случайных чисел
ДВК	датчик вскрытия корпуса
НШОС	нештатная операционная система
ОС	операционная система
ПИН (ПИН-код)	пароль, предоставляющий доступ к защищенной памяти АИ
ПО	программное обеспечение
СВТ	средства вычислительной техники
СДЗ	средство доверенной загрузки
СЗИ НСД	средство защиты информации от несанкционированного доступа
ЦП	центральный процессор
ШОС	штатная операционная система
ЭВМ	электронная вычислительная машина

1 НАЗНАЧЕНИЕ

1.1 Наименование и обозначение изделия

Наименование изделия: «Средство доверенной загрузки «Dallas Lock».

Обозначение изделия: ПФНА.501410.003.

1.2 Общая информация

Изделие является средством доверенной загрузки уровня платы расширения и представляет собой программно-техническое средство, которое осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы (НШОС), а также предоставляет доступ к информационным ресурсам в случае успешной проверки подлинности загружаемой операционной системы.

СДЗ Dallas Lock выполняет свои функции (включая администрирование параметров изделия и просмотр журнала) до начала загрузки ШОС.

СДЗ Dallas Lock предназначено для использования на персональных компьютерах (в т. ч. на ноутбуках) и серверах, работающих под управлением ОС архитектуры x86-32 и x86-64.

1.3 Основные возможности и функции

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

– загрузка 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 СВТ и (или) состава компонентов аппаратного обеспечения СВТ;

– нарушение целостности ПО СДЗ Dallas Lock, обход нарушителем компонентов СДЗ Dallas Lock;

– несанкционированное изменение конфигурации СДЗ Dallas Lock;

– преодоление или обход функций идентификации/аутентификации СДЗ Dallas Lock за счет недостаточного качества аутентификационной информации и (или) недоверенного маршрута между средством доверенной загрузки и пользователями;

– получение остаточной информации СДЗ Dallas Lock из памяти СВТ после завершения работы СДЗ Dallas Lock;

– получение доступа к ресурсам СДЗ Dallas Lock из программной среды СВТ после завершения работы СДЗ Dallas Lock;

– сбои и ошибки в процессе функционирования СДЗ Dallas Lock.

Также СДЗ Dallas Lock обеспечивает реализацию следующих функций безопасности:

- блокирование загрузки НШОС;
- разграничение доступа к управлению СДЗ Dallas Lock;
- управление работой СДЗ Dallas Lock;
- регистрация событий, связанных с безопасностью, в журнале событий;
- идентификация и аутентификация пользователей;
- самодиагностика изделия;
- контроль целостности ПО и компонентов СВТ;
- обеспечение безопасности при возникновении сбоев и ошибок в процессе работы;
- обеспечение безопасности после завершения работы СДЗ Dallas Lock;
- обеспечение доверенного маршрута при взаимодействии с уполномоченными субъектами.

1.4 Состав

СДЗ Dallas Lock состоит из:

- аппаратной части;
- прошивки (программной части).

Аппаратная часть СДЗ Dallas Lock представляет собой печатную плату (плата PCIe «КТ-500» ПФНА.501410.003-01, плата miniPCIe-HS «КТ-521» ПФНА.501410.003-02 или плата M.2 «КТ-550» ПФНА.501410.003-04).

Прошивка (программная часть) СДЗ Dallas Lock состоит из следующих компонентов:

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

1.4.1 Загрузчик среды исполнения

Загрузчик среды исполнения проецируется в область BIOS для обеспечения получения управления над процессом загрузки компьютера. Его задача – выполнить чтение кода среды исполнения функции безопасности из памяти платы и передать ей управление.

1.4.2 Среда исполнения функций безопасности

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 ЭВМ, текущего времени;

– вывод графики на экран ЭВМ;

– обеспечение доступа к энергонезависимой памяти платы для чтения/сохранения параметров и журнала;

– обеспечение доступа к функции перезагрузки/выключения ЭВМ;

– управление через манипулятор типа «мышь» в процессе администрирования СДЗ Dallas Lock;

– поддержка системных плат BIOS и UEFI;

– загрузка ШОС.

1.4.3 Оболочка функций безопасности

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

– самодиагностики;

– управления доступом;

– администрирования параметров СДЗ Dallas Lock;

– идентификации и аутентификации пользователей;

– контроля целостности компонентов СВТ;

– регистрации и учёта.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

Прошивка СДЗ Dallas Lock является программным компонентом изделия, ее программный код выполняется до загрузки ШОС. Основные условия применения в целом соответствуют условиям применения платы СДЗ Dallas Lock.

2.1 Технические требования

СДЗ Dallas Lock исправно работает на ЭВМ архитектуры Intel x86-32 и x86-64. Минимальные аппаратные требования к ЭВМ для установки СДЗ Dallas Lock:

– процессор Pentium с частотой 300 МГц;

– не менее 512 МБ оперативной памяти;

– разъем на материнской плате для подключения СДЗ Dallas Lock: PCI-express / Mini PCI-express / M.2;

– наличие свободных портов USB, если изделие используется совместно с аппаратными идентификаторами (за исключением случаев, когда в качестве аппаратных идентификаторов используются электронные ключи Touch Memory, а считыватель Touch Memory подключен непосредственно к плате формата PCIe «КТ-500»);

– клавиатура, мышь Microsoft Mouse 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: FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3, VMFS5.

СДЗ Dallas Lock поддерживает следующие виды аппаратных идентификаторов:

– USB-ключи и смарт-карты Aladdin eToken Pro/Java[1];

– USB-ключи и смарт-карты Рутокен (Рутокен S[2], Рутокен ЭЦП);

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

[2] Рутокен S можно только назначить пользователю, записать данные учетной записи пользователя на него нельзя. Для совместного использования с СДЗ Dallas Lock аппаратный идентификатор Рутокен S необходимо предварительно отформатировать с помощью набора библиотек и утилит OpenSC версий 0.12 - 0.17, используя команды:

$ pkcs15-init --erase-card

$ pkcs15-init --create-pkcs15 --so-pin "<ПИН администратора>" --so-puk "" --pin "<ПИН пользователя>"

$ pkcs15-init --store-pin --label "<имя АИ>" --auth-id 02 --pin "<ПИН пользователя >" --puk ""

– электронные ключи Touch Memory (iButton)[3];

– USB-ключи и смарт-карты eSmart (eSmart Token, eSmart GOST);

– USB-ключи и смарт- карты JaCarta (JaCarta ГОСТ, JaCarta PKI).

Примечание. При использовании СДЗ Dallas Lock аппаратная идентификация не является обязательной.

Примечание. Для защиты информации, содержащей сведения, составляющие государственную тайну со степенью секретности до «совершенно секретно» включительно, используются электронные ключи iButton. Также электронные ключи iButton могут использоваться для защиты конфиденциальной информации.

2.2 Входные и выходные данные

Входными данными в СДЗ Dallas Lock являются:

– файлы конфигураций модулей системы, используемые при установке или в процессе администрирования;

– уникальные для каждой учетной записи имя пользователя, пароль и серийный номер аппаратного идентификатора;

– ПИН-код аппаратного идентификатора;

– формализованные правила политик безопасности, реализуемые с помощью механизмов СДЗ Dallas Lock и преобразованные в значения атрибутов и полномочий.

Имя учетной 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 Dallas Lock выступают:

– сообщения СДЗ Dallas Lock на действия пользователей;

– журнал, создаваемый СДЗ Dallas Lock в процессе работы;

– значения контрольных сумм объектов, на которых установлен контроль целостности;

– сохраненные параметры конфигурации СДЗ Dallas Lock, сформированные в процессе администрирования;

– отчеты результатов самодиагностики СДЗ Dallas Lock.

[3] При подключении считывателя Touch Memory непосредственно к СДЗ Dallas Lock (только для платы формата PCIe «КТ-500») есть возможность работы с памятью электронных ключей iButton (DS-1992, DS-1993, DS-1995, DS-1996) для хранения идентификационной и аутентификационной информации учетной записи пользователя и его авторизации на ее основе.

Следует иметь в виду, что действия с памятью электронных ключей iButton не будут доступны с момента обнаружения СДЗ Dallas Lock подключенного к ЭВМ USB-считывателя Touch Memory и до перезагрузки ЭВМ.

2.3 Пользователи СДЗ Dallas Lock

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

– «Администраторы» – пользователь, ответственный за управление СДЗ Dallas Lock. Эту функцию могут выполнять и несколько сотрудников подразделения информационной безопасности предприятия;

– «Аудиторы» – пользователь, имеющий права на просмотр всех установленных параметров безопасности СДЗ Dallas Lock без возможности их редактирования;

– «Пользователи» – пользователь защищенного персонального компьютера, не имеющий полномочий на администрирование системы защиты, осуществляющий ввод и обработку информации любыми программными средствами.

3 ОПИСАНИЕ ЗАДАЧИ

3.1 Подсистема самодиагностики

При включении ПЭВМ СДЗ 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, ПЭВМ выводит сообщение и выключается.

3.2 Подсистема управления доступом

СДЗ позволяет блокировать загрузку операционной системы:

- при превышении числа неудачных попыток аутентификации пользователя;
- при нарушении целостности программной среды или аппаратных компонентов;
- при обходе нарушителем компонентов СДЗ Dallas Lock;
- при попытке загрузки НШОС;
- при критичных сбоях и ошибках.

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

СДЗ совершает очистку оперативной памяти и обеспечивает недоступность ресурсов средства доверенной загрузки из программной среды СВТ, информационного содержания ресурсов СВТ после завершения работы средства доверенной загрузки.

СДЗ обладает возможностью осуществлять перезагрузку СВТ в случае, если в течение определенного времени после включения питания управление загрузкой не было передано на СДЗ, размещенном на системной плате.

3.3 Подсистема администрирования СДЗ Dallas Lock

Администрирование СДЗ Dallas Lock осуществляется из окна программы администрирования – оболочки администратора, в оболочке функциональной безопасности СДЗ Dallas Lock.

3.3.1 Интерфейс программы

Оболочка администратора СДЗ 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:

- «Пользователи» – управление учетными записями пользователей;

– «Контролируемые объекты» – контроль целостности компонентов СВТ;

– «Политики безопасности» – настройка авторизации в СДЗ Dallas Lock;

– «Журнал» – регистрация и аудит;

– «Параметры» – управление параметрами платы;

– «Сервис» – дополнительные функции СДЗ Dallas Lock.

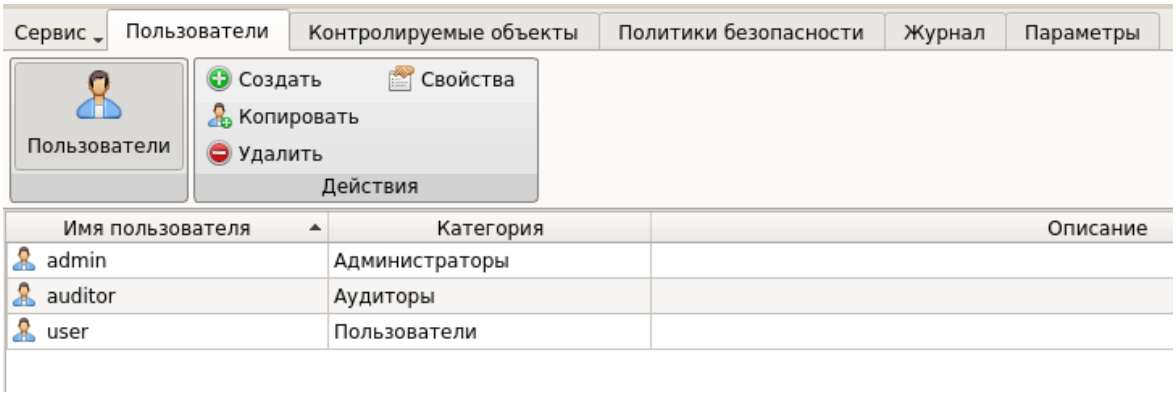

Рисунок 1 – Главное окно оболочки администратора. Пользователи

При выборе вкладки отображается соответствующий список категорийных и функциональных кнопок.

3.3.2 Сохранение/применение конфигурации и вывод отчетов в СДЗ Dallas Lock

В оболочке администратора СДЗ Dallas Lock предусмотрена функция сохранения всех параметров конфигурации СДЗ Dallas Lock на различные носители информации, с возможностью применения сохраненной конфигурации. Данный функционал доступен только администратору СДЗ Dallas Lock через меню «Сервис» в оболочке администратора.

Возможны следующие действия для пункта «Конфигурация»:

– «Сохранить» - данные об учетных 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 Dallas Lock на несколько автономных ЭВМ, т.к. настройка параметров безопасности на каждом отдельном ЭВМ может занимать много времени. В этом случае администратору необходимо настроить параметры СДЗ Dallas Lock на одном ЭВМ и сохранить полную конфигурацию настроек СДЗ 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 Dallas Lock по умолчанию. Возврат к настройкам СДЗ Dallas Lock по умолчанию предполагает восстановление первоначальных значений политик безопасности, параметров контроля целостности и атрибутов учетных записей. Учетные записи, созданные при установленном СДЗ Dallas Lock, после восстановления первоначальных настроек будут удалены. Применение настроек по умолчанию носит необратимый характер и эквивалентно переустановке СДЗ Dallas Lock.

«Отчет…» - сохранение отчета о конфигурации СДЗ Dallas Lock в формате *.txt на различные носители информации. Данный функционал доступен пользователям, наделенным полномочиями администратора или аудитора.

В отчете указываются следующие данные:

– дата и время формирования отчета;

– имя пользователя, который создал отчет;

– версия прошивки СДЗ Dallas Lock;

– параметры конфигурации СДЗ Dallas Lock в соответствии с настройками отчета.

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

«О СДЗ Dallas Lock» - вывод необходимых контактов производителя.

Дополнительные функции СДЗ Dallas Lock доступны пользователям, наделенным полномочиями администратора. Возможность сохранять отчет о конфигурации СДЗ Dallas Lock и выводить информацию о ЭВМ и установленном СДЗ Dallas Lock доступна также аудиторам.

3.3.3 Обновление прошивки СДЗ Dallas Lock

Порядок обновления изделия производится следующим образом:

– компания-разработчик доводит до потребителя информацию о выпуске обновлений изделия и устраненных в новых версиях недостатках по электронной почте (с подтверждением полученной информации);

– потребитель при получении указанной информации выполняет загрузку обновления с сайта предприятия-изготовителя в виде файла, информация о контрольной сумме которого содержится на сайте предприятия-изготовителя;

– для верификации установочного пакета необходимо выполнить расчет[4] и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте предприятия-изготовителя;

– перед применением необходимо разрешить запись в системную область энергонезависимой памяти СДЗ. Более подробное описание содержится в документе «Руководство по эксплуатации» ПФНА.501410.003 РЭ;

– для установки обновления необходимо из оболочки администратора СДЗ перейти на вкладку «Параметры», выбрать действие «Обновить», после чего выбрать файл с новой прошивкой.

3.4 Подсистема идентификации и аутентификации

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

3.4.1 Управление учетными записями пользователей

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

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

На вкладке **«Общие»** допустимо редактирование следующих параметров учетной 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 учетной 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.501410.003 РЭ).

Допустимо присвоение следующих атрибутов учетной записи пользователя:

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

– «Отключен» – учетная 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 учетной записи пользователя.

– «Запретить смену пароля пользователем» – запрет для пользователя на смену своего пароля, в т. ч. 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 учетной записи пользователя.

– «Запретить работу при нарушенной целостности» – вход в систему пользователем при неуспешном прохождении процедуры контроля целостности объектов и компонентов СВТ запрещается;

– «Запретить работу при событиях от ДВК» – вход в систему блокируется при срабатывании датчика вскрытия корпуса. На экране приглашения в систему отображается соответствующее сообщение.

Примечание. Данный атрибут применим только для варианта исполнения изделия ПФНА. 501410.003-01 (плата формата PCIe «КТ-500»).

– «Запретить загрузку нештатной ОС» – запрет на загрузку ОС с носителя, отличного от указанного в поле «Загрузочное устройство» вкладки «Параметры» оболочки администратора.

– «Запретить работу при неисправности часов» – вход в систему блокируется при неисправности часов. На экране приглашения в систему отображается соответствующее сообщение;

Примечание. Данный атрибут применим только для варианта исполнения изделия ПФНА. 501410.003-01 (плата формата PCIe «КТ-500»).

– «Запретить работу при неисправности ДСЧ» – вход в систему блокируется при неисправности ДСЧ. На экране приглашения в систему отображается соответствующее сообщение.

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 идентификатор будет присвоен редактируемой учетной записи пользователя.

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

Примечание. Вкладка «Аппаратная идентификация» отсутствует в окне редактирования параметров доменной учетной 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 советующие 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 учетной 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 аппаратных идентификаторов.

– «Сменить ПИН» – данная кнопка позволяет сменить ранее назначенный ПИН учетной записи пользователя для идентификатора. В окне «Изменение ПИН» ввести старый, новый ПИН и повторить ввод нового ПИН;

Примечание. Требования к ПИН-коду аппаратного идентификатора определяются в документации на данный аппаратный идентификатор.

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

На вкладке **«Вход в СЗИ НСД»** дополнительно можно настроить автовход в СЗИ НЗД Dallas Lock, установив соответствующий атрибут. При этом можно выбрать опцию:

– «Авторизационные данные введенные пользователем при входе» - чтобы использовать данные учетные записи пользователя, которые были введены при входе;

– «Предопределенные данные» - чтобы внести данные учетной записи пользователя вручную.

После загрузки ШОС осуществится автоматический вход в СЗИ НСД с указанными параметрами:

– «Имя пользователя»;

– «Пароль пользователя»;

– «Домен пользователя».

Допустимо присвоение следующих атрибутов СЗИ:

– «Передавать аппаратный идентификатор в СЗИ НСД»;

– «Передавать пароль в СЗИ НСД».

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

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

Автоматическая разблокировка заблокированной учетной записи пользователя осуществляется по истечении установленного времени или принудительно администратором СДЗ Dallas Lock.

3.4.2 Настройка политик безопасности

Администратор имеет возможность настроить политики безопасности для авторизации (Таблица 1), паролей (Таблица 2) и ДСЧ (Таблица 3 – Список параметров категории

«Политики ДСЧ») 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 «Пользователь» заполняется именем учетной записи пользователя, осуществившего последний успешный вход. При значении «Нет» поле остается пустым
«Максимальное количество ошибок ввода пароля»	Установленное значение регламентирует количество попыток ввода значений пароля. В случае ввода неверного пароля появляется предупреждение. По достижении установленного значения - учётная запись пользователя блокируется на определённое время, устанавливаемое параметром «Время блокировки учетной записи в случае ввода неправильных паролей». Возможное значение параметра: от 1 до 15 и «Не используется» - количество попыток ввода пароля неограниченно
«Время блокировки учетной записи в случае ввода неправильных паролей»	Установленное значение регламентирует время блокировки учётной 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. Возможное значение параметра: от 1 мин до 5 ч и «Не используется» - в таком случае разблокировка возможна только администратором
«Отображать время последнего успешного входа»	Возможное значение параметра: «Да/Нет». В значении «Да» при очередном входе пользователя во вовремя выполнения процедуры контроля целостности объектов отображается дата и время последнего успешного входа данного пользователя. В значении «Нет» - не отображается
«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, уже введённые данные очищаются. Возможное значение параметра: от 1 мин до 10 мин и «Не используется» - время ожидания ввода авторизационных данных неограниченно
«Использовать авторизационную информацию из аппаратного ключа»	Возможное значение параметра: «Да/Нет». В значении «Нет» авторизационная информация вводится

Параметр политики	Описание
	пользователем с клавиатуры. В значении «Да» авторизационная информация считывается с памяти аппаратного идентификатора в соответствии с настройками учетной записи пользователя, указанными на вкладке «Аппаратная идентификация»
«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
«Использовать аппаратный идентификатор по умолчанию»	Возможное значение параметра: «Да/Нет». В значении «Нет» аппаратный идентификатор должен быть выбран из предъявленных пользователем самостоятельно. В значении «Да» обнаруженный аппаратный идентификатор используется автоматически. Если аппаратных идентификаторов предъявлено несколько, то используется первый обнаруженный

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». Возможное значение параметра: от 1 дня до 25 недель и «Не используется» - максимальный срок действия пароля не установлен
«Минимальный срок действия пароля»	Параметр определяет минимальный срок действия пароля. Если этот срок ещё не истёк, смена пароля пользователем запрещена. Возможное значение параметра: от 1 дня до 4 недель, «Не используется» - минимальный срок действия не установлен
«Напоминать о смене пароля за»	Параметр задаёт период до установленного максимального срока действия пароля, в который пользователю будет выводиться сообщение о необходимости смены пароля. Возможное значение параметра: от 1 дня до 2 недель и «Не используется» - сообщение выводиться не будет

Параметр политики	Описание
«Минимальная длина»	Параметр устанавливает ограничение на минимальную длину пароля. Возможное значение параметра: от 1 до 14 и «Не используется» - устанавливаемый пароль может иметь пустое значение
«Необходимо наличие цифр»	Если данный параметр включен, то при создании пароля в нём должны присутствовать цифры. Возможное значение параметра: «Да/Нет»
«Необходимо наличие спецсимволов»	Если данный параметр включен, то при создании пароля в него должны быть включены специальные символы, такие как "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/", "=" и т. д. Возможное значение параметра: «Да/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. Возможное значение параметра: «Да/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. Возможное значение параметра: «Да/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. Возможное значение параметра: от 1 до 10 и «Не используется» - проверки на отличие старого пароля от нового не происходит

Таблица 3 – Список параметров категории «Политики ДСЧ»

Параметр политики	Описание
«Тестирование ДСЧ при входе»	Возможное значение параметра: «Да/Нет». В значении «Да» осуществляется тестирование ДСЧ при входе. При значении «Нет» тестирование ДСЧ при входе отключено
«Число попыток самотестирования ДСЧ»	Установленное значение регламентирует число попыток самотестирования ДСЧ. Возможное значение параметра: от 1 до 3

Параметр политики	Описание
«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.

Следует обратить внимание, что при использовании СДЗ Dallas Lock в составе СВТ, 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 СВТ

СДЗ Dallas Lock позволяет осуществлять контроль целостности следующих типов объектов:

- «Файловая система» (ФС);
- «Реестр»;
- «Области диска»;
- «BIOS CMOS»;
- «Аппаратная конфигурация».

Просмотр контролируемых объектов конкретной категории осуществляется через соответствующие кнопки на панели «Категория».

Для контроля целостности используется метод сравнения расчётной контрольной суммы (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 ФС, реестра Windows и областей жесткого диска (Таблица 4).

Таблица 4 – 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

Наименование параметра	Описание
«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»	Путь к файлу реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен
«Путь»	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 ЭВМ. 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
«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: FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3, VMFS5. В СДЗ 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

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

– «Обновить CMOS»;

– «Сохранить».

Для категории «BIOS CMOS» форма просмотра разделена на два блока «BIOS» и «CMOS» (Рисунок 2).

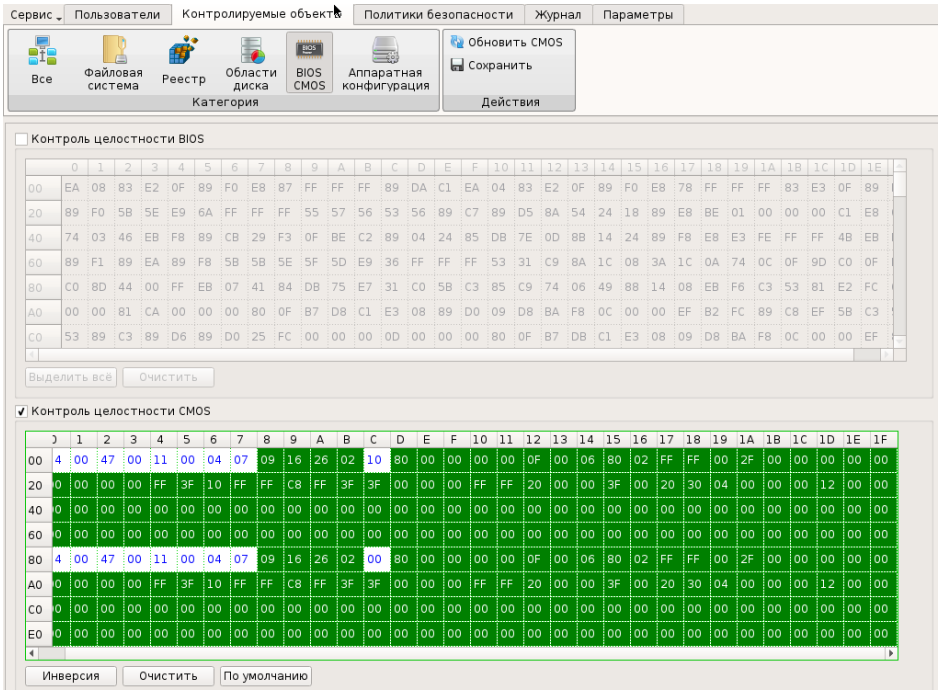

Рисунок 2 – Контроль BIOS CMOS

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

В блоке «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, и «Очистить». 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 ЭВМ;

– «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».

Для категории «Аппаратная конфигурация» выводятся списки групп аппаратной конфигурации (Таблица 5).

Таблица 5 – Пример списка групп аппаратной конфигурации

Группа	Описание
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

Каждая группа содержит свой список относящихся к ней устройств, которые подключены к ЭВМ, 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».

3.6 Подсистема регистрации и аудита

События по администрированию СДЗ Dallas Lock, события входов пользователей, события проверки целостности и редактирования учетных 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»;

– «Учетные 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.

Примечание. Подробное описание работы данных действий описаны в документе

«Руководство по эксплуатации» ПФНА.501410.003 РЭ.

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

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

- проверка пользователя;
- инициализация системы;
- старт ОС;
- запуск оболочки администратора;
- выход пользователя;
- перезагрузка;
- выключение;
- смена пароля.

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

- применение конфигурации СДЗ Dallas Lock;
- сохранение отчета о конфигурации СДЗ Dallas Lock;
- обновление прошивки СДЗ Dallas Lock;
- изменение политики безопасности;
- чистка журнала;
- экспорт журнала;
- установка даты-времени;
- установка времени срабатывания сторожевого таймера;
- срабатывание сторожевого таймера;
- генерация псевдослучайной последовательности;
- обнуление датчиков вскрытия корпуса;
- задание загрузочного устройства;
- добавление объекта контроля целостности файловой системы / реестра / области диска / аппаратной конфигурации / BIOS / CMOS;
- изменение объекта контроля целостности файловой системы / реестра / области

диска /аппаратной конфигурации / BIOS / CMOS;

– удаление объекта контроля целостности файловой системы / реестра / области диска /аппаратной конфигурации / BIOS / CMOS.

В категории «Учетные записи» фиксируются события, связанные с изменениями учетных записей пользователей в СДЗ Dallas Lock:

– удаление учетной записи;

– создание учетной записи;

– изменение учетной записи;

– задание пароля учетной записи.

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

– завершение контроля целостности объектов;

– контроль целостности объекта;

– пересчет целостности объекта;

– удаление объекта целостности;

– завершение пересчета целостности списка объекта.

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