СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ
«Dallas Lock»

Руководство по эксплуатации

ПФНА.501410.003 РЭ

Настоящее руководство по эксплуатации распространяется на изделие «Средство доверенной загрузки «Dallas Lock» (далее по тексту - СДЗ Dallas Lock).

Документ предназначен для специалистов по информационным технологиям, служб и подразделений обеспечения безопасности информации, осуществляющих администрирование изделия.

Руководство состоит из 5 разделов и включает в себя:

– раздел 1: общее описание назначения, технические характеристики и возможности СДЗ Dallas Lock, состав изделия, а также устройство и работу механизмов СДЗ Dallas Lock;

– раздел 2: сведения, необходимые для установки и эксплуатации изделия, подготовки его к работе, описание задач по администрированию изделия, описание пользовательского интерфейса оболочки администратора СДЗ Dallas Lock и функционал, доступный администратору изделия;

– разделы 3–5: сведения о техническом обслуживании, ремонте, хранении, транспортировании и утилизации изделия.

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

АИ	аппаратный идентификатор
АС	автоматизированная система
ДСЧ	датчик случайных чисел
ДВК	датчик вскрытия корпуса
КСБ	консоль сервера безопасности
НШОС	нештатная операционная система
ОС	операционная система
ПИН (ПИН-код)	пароль, предоставляющий доступ к защищенной памяти АИ
ПО	программное обеспечение
СБ	сервер безопасности
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 ОПИСАНИЕ И РАБОТА

1.1 Назначение изделия

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

Обозначение изделия: ПФНА.501410.003.

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

1.2 Технические характеристики

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);
- 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»

---

[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 ""

[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.

включительно, используются электронные ключи iButton. Также электронные ключи iButton могут использоваться для защиты конфиденциальной информации.

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

СДЗ Dallas Lock позволяет контролировать целостность реестра ОС Windows.

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.

СДЗ Dallas Lock реализует следующие функции 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.

1.3 Состав изделия

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) (Рисунок 1), плата miniPCIe-HS «КТ-521» (ПФНА.501410.003-02) (Рисунок 2) или плата M.2 «КТ-550» (ПФНА.501410.003-04) (Рисунок 3).

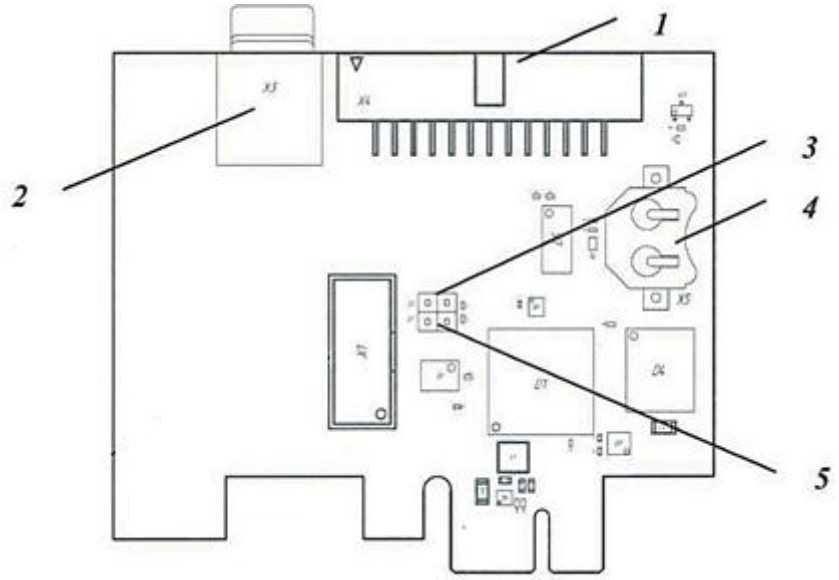

Рисунок 1 – Расположение основных элементов **«КТ-500»**

(1 – Группа штыревых разъемов для подключения датчиков вскрытия корпуса, цепи системного сброса, считывателя Touch Memory (или кабеля для подключения считывателя Touch Memory через разъем RJ11 ПФНА.501410.003-08);
2 – Слот для карты microSD;
3 – Контакты под джампер для блокировки загрузки кода из области Option ROM. Передача управления ROM СДЗ Dallas Lock не осуществляется при установленном джампере;
4 – Разъем для литиевой батареи CR1220/ CR1225 часов реального времени и блока контроля вскрытия корпуса;
5 – Контакты под джампер для входа в сервисный режим СДЗ (для обновления прошивки платы). При установленном джампере разрешается запись в системную область памяти СДЗ)

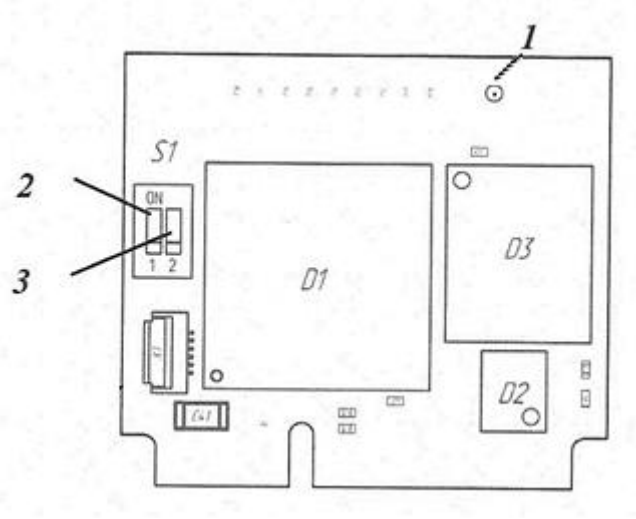

Рисунок 2 – Расположение основных элементов **«КТ-521»**

(1 – Коаксиальный разъем для подключения «сторожевого таймера»;
2 – Микропереключатель для блокировки загрузки кода из области Option ROM. Передача управления ROM СДЗ Dallas Lock не осуществляется в положении переключателя «ON»;
3 – Микропереключатель для входа в сервисный режим СДЗ (для обновления прошивки платы). В положении переключателя «ON» разрешается запись в системную область памяти СДЗ)

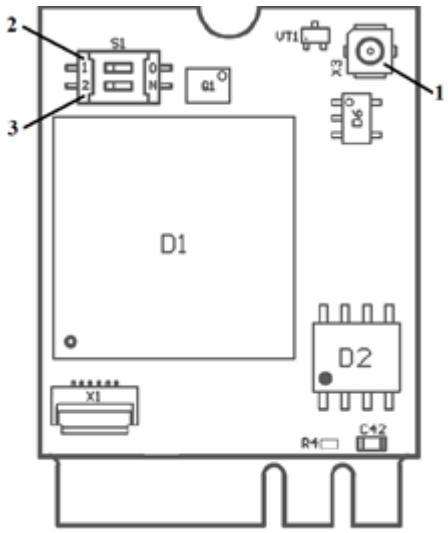

Рисунок 3 – Расположение основных элементов **«КТ-550»**

(1 – Коаксиальный разъем для подключения «сторожевого таймера»;
2 – Микропереключатель для блокировки загрузки кода из области Option ROM. Передача управления ROM СДЗ Dallas Lock не осуществляется в положении переключателя «ON»;
3 – Микропереключатель для входа в сервисный режим СДЗ (для обновления прошивки платы). В положении переключателя «ON» разрешается запись в системную область памяти СДЗ)

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

– загрузчик среды исполнения;

– среда исполнения функций безопасности;

– оболочка функций безопасности.

1.4 Устройство и работа

При включении/перезагрузке ЭВМ BIOS системной платы передает управление исполняемой ROM СДЗ Dallas Lock, в которой записан загрузчик среды исполнения. Таким образом, загрузчик получает управление и производит загрузку среды исполнения функций безопасности.

Среда исполнения функций безопасности запускает оболочку функций безопасности.

Оболочка функций безопасности после получения управления производит самодиагностику СДЗ Dallas Lock. При выявлении критических сбоев выводится соответствующее сообщение и СДЗ Dallas Lock выключает ЭВМ.

Далее, оболочка функций безопасности СДЗ Dallas Lock отображает окно авторизации.

После успешной авторизации и выборе действия «Загрузка» оболочка функций безопасности СДЗ Dallas Lock завершает работу, происходит дальнейшая загрузка СВТ.

1.5 Маркировка и упаковка

Маркировка СДЗ Dallas Lock содержит:

– товарный знак предприятия-изготовителя;

– заводской (учетный) порядковый номер изделия;

– год, месяц, число упаковки (в разделе 5 «Свидетельство об упаковывании и приемке»);

– знак соответствия сертифицированной продукции (наносится на поверхность печатной копии формуляра (ПФНА.501410.003 ФО), поставляемого в составе комплекта СДЗ Dallas Lock, в разделе 5 «Свидетельство об упаковывании и приемке» в поле «Номер знака соответствия»).

Маркировка наносится на печатную плату СДЗ Dallas Lock, упаковку изделия и в формуляр.

Надписи при маркировке выполняются одним из следующих способов:

– рукописным – основным чертежным шрифтом, высотой не менее 1,6 мм, по ГОСТ 2.304, черным цветом;

– с применением печатающих устройств вывода ЭВМ, высота шрифта не менее 1,6 мм;

– комбинированием перечисленных способов.

Упаковка изделия осуществляется в тару, обеспечивающую защиту и сохранность при транспортировании и хранении изделия согласно требованиям раздела 6 Технических условий (ПФНА.501410.003 ТУ).

2 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

2.1 Эксплуатационные ограничения

2.1.1 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.

2.2 Подготовка изделия к использованию

Установка и эксплуатация СДЗ Dallas Lock должны соответствовать требованиям прилагаемой документации в полном объеме.

Перед установкой платы СДЗ Dallas Lock необходимо сконфигурировать настройки Setup BIOS в зависимости от того, какая используется материнская плата и в каком режиме загружается ШОС:

– для UEFI-режима (материнская плата UEFI-совместима и используется ШОС, установленная в режиме UEFI-загрузки):

- включить режим UEFI Boot (Enabled);
- отключить режим CSM (Disabled);
- отключить режим FastBoot (Disabled);
- в Setup BIOS удалить установленные ключи для SecureBoot и затем

установить ключи, расположенные на диске, идущем в комплекте с изделием, в следующем порядке: db.auth, KEK.auth, PK.auth.

Примечание. Для замены ключей для SecureBoot можно воспользоваться утилитой KeyTool.efi, расположенной на диске, идущем в комплекте с изделием.

– для Combo-режима (если материнская плата UEFI-совместима и используется ШОС, установленная в режиме Legacy-загрузки):

- проверить, что режим CSM включен (Enabled);
- отключить режим FastBoot (Disabled).

– для Legacy-режима (если материнская плата не UEFI-совместима и используется ШОС, установленная в режиме Legacy-загрузки):

- отключить режим FastBoot (Disabled).

Примечание. Плата СДЗ Dallas Lock по умолчанию загружается в режиме «Только UEFI». Поменять режим загрузки платы СДЗ Dallas Lock можно с помощью сервисной утилиты KtService (см. п.п. 2.3.6.1)

Примечание. Для корректной работы СДЗ Dallas Lock с ОС Windows 8, 8.1, 10 также необходимо отключить быструю загрузку (быстрый запуск) ОС и режим гибернации.

Также в настройках Setup BIOS необходимо установить загрузку с жесткого диска (загрузчика) с ШОС.

При эксплуатации изделия на доступ к настройкам BIOS должен быть установлен пароль.

Установка платы СДЗ Dallas Lock в системную плату ЭВМ осуществляется в свободный слот PCI-express / mini PCI-express / M.2.

В СДЗ Dallas Lock реализован беспроводной (программный) «сторожевой таймер». При наличии разъемов «Reset» или «Power» рекомендуется подключать «сторожевой таймер» изделия к ЭВМ с помощью поставляемого Кабеля ПФНА.501410.003-05 (для платы «КТ-500») или ПФНА.501410.003-06 (для плат «КТ-521» и «КТ-550»).

– на плате формата PCIe «КТ-500» кабель подключается к штыревым разъемам «R» и «G» (см. Рисунок 4), на ЭВМ - к разъёму «Reset» («Power»);

– на платах формата miniPCIe-HS «КТ-521» и M.2 «КТ-550» кабель подключается к коаксиальному разъему (см. Рисунок 2 и 3), на ЭВМ - к разъёму «Reset» («Power»).

Примечание. Если ЭВМ при включении уходит в перезагрузку или выключается (в зависимости от того, к какому разъему кабель «сторожевого таймера» подключен со

стороны ЭВМ), то кабель подключен неверно. Полярность подключения двухконтактного разъема кабеля не соблюдена.

На плате формата PCIe «КТ-500» также для подключения датчиков вскрытия корпуса (ДВК) используются штыревые разъемы «V+», «S1» и «S2», для подключения считывателя Touch Memory (в том числе через Кабель ПФНА.501410.003-08) – штыревые разъемы «C1», «C2» и «G» (Рисунок 5).

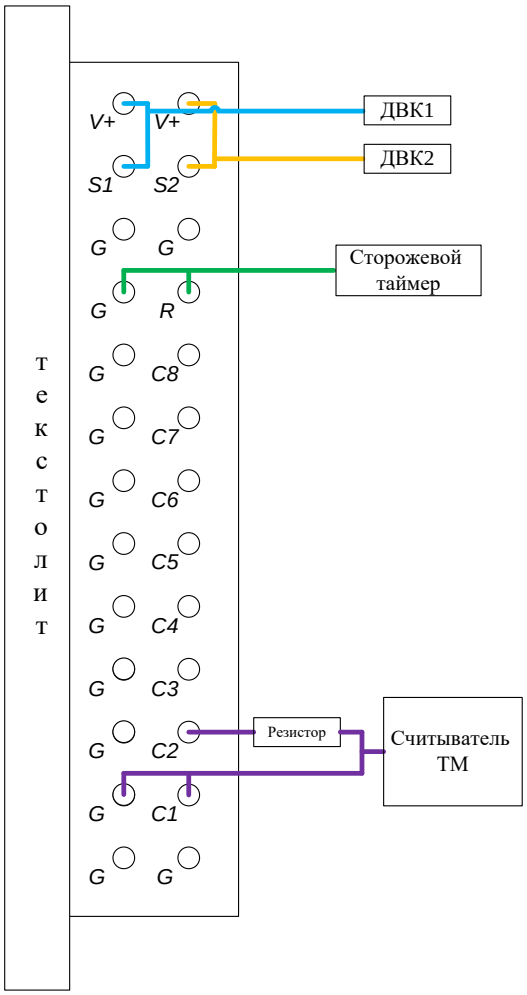

Рисунок 6 – Схема подключения ДВК, сторожевого таймера и считывателя ТМ к штыревым разъемам на плате «КТ-500»

Установка дополнительных программных компонент (драйверов) для обеспечения функционирования СДЗ Dallas Lock на жесткий диск ЭВМ не требуется.

Примечание. Для работы функции автовхода по авторизационным данным из СДЗ Dallas Lock в ШОС, защищенную СЗИ Dallas Lock 8.0, а также для использования часов платы «КТ-500» при регистрации времени событий в журналах СЗИ Dallas Lock 8.0, необходима установка драйвера платы КТ, расположенном на диске, идущем в комплекте с СДЗ Dallas Lock.

2.2.1 Меры безопасности при подготовке изделия

Установку изделия должен осуществлять специалист, имеющий базовые знания в области компьютерной техники и навыки системного администрирования.

Установку СДЗ Dallas Lock в системную плату осуществлять только при выключенном питании ЭВМ.

При установке СДЗ Dallas Lock избегать возможных повреждений элементов, выступающих над поверхностью печатной платы изделия.

2.2.2 Внешний осмотр изделия

Перед установкой изделия необходимо осмотреть печатную плату изделия на предмет видимых повреждений. При их наличии изделие к эксплуатации не допускается.

2.3 Использование изделия

В настоящем руководстве по эксплуатации рассматриваются возможные действия пользователей СДЗ Dallas Lock с правами аудитора и администратора. Возможные действия оператора СДЗ Dallas Lock изложены в документе «Руководство оператора» (ПФНА.501410.003 34).

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

Аудитор – пользователь, имеющий права на просмотр всех установленных параметров безопасности СДЗ Dallas Lock без возможности их редактирования.

2.3.1 Вход на защищенную ЭВМ

При загрузке компьютера с установленной платой СДЗ Dallas Lock появляется экран приглашения на вход в систему (Рисунок 7).

> **Примечание.** При первом входе пароль пользователя «admin» равен пустому значению.

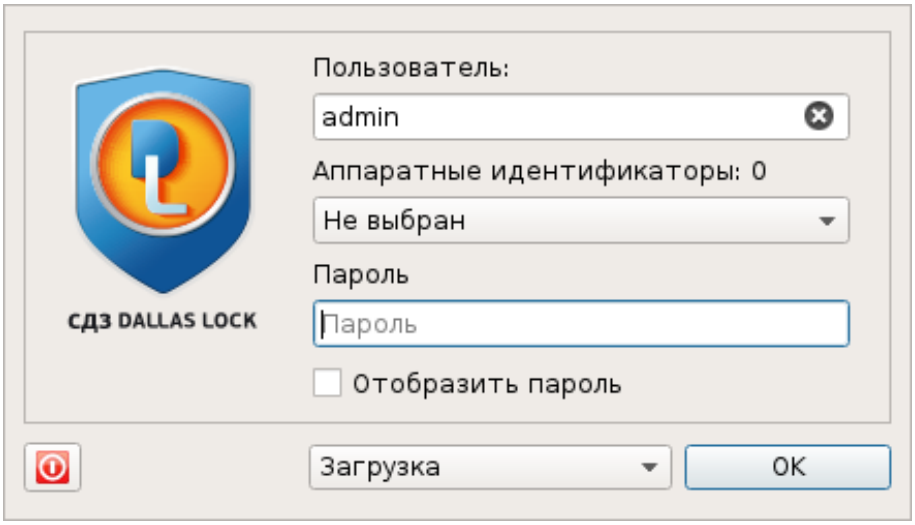

Рисунок 7 – Экран приглашения на вход в систему

Примечание. Если защищенный СДЗ Dallas Lock компьютер введен в Домен безопасности, в левом нижнем углу экрана приглашения на вход будет отображен соответствующий значок: - при наличии связи с СБ, - при отсутствии связи с СБ.

Для входа на защищенный СДЗ Dallas Lock компьютер необходимо:

– предъявить АИ, если он назначен учетной записи пользователя (подробное описание авторизации с использованием АИ см. в п.п. 2.3.1.1);

– используя клавиатуру, ввести в поле «Пользователь» имя учетной записи, под которой пользователь зарегистрирован в СДЗ Dallas Lock. В зависимости от настроек политики авторизации СДЗ Dallas Lock в этом поле может оставаться имя учетной записи пользователя, выполнившего вход последним;

Примечание. Ввод имени доменной учетной записи пользователя должен производиться в одном из следующих форматов:
– [dom]\[name], где [dom] – полное или короткое имя домена, [name] – имя учетной записи;
– [name]@[dom], где в качестве значения [dom] используется только полное имя домена.
Доменная учетная запись пользователя должна быть предварительно зарегистрирована в СДЗ Dallas Lock.

Примечание. Для корректной работы доменной авторизации необходима настройка обратной зоны DNS, обслуживающего СДЗ Dallas Lock, чтобы полученные СДЗ Dallas Lock от DHCP-сервера IP-адреса DNS-серверов могли быть преобразованы в полное DNS-имя, из которого можно взять полный доменный суффикс для учетной записи.

Например, СДЗ получает IP-адрес 192.168.0.100 и IP-адрес DNS-сервера 192.168.0.1. DNS-сервер должен быть настроен таким образом, что результатом запроса преобразования адреса "192.168.0.1" в имя будет "dns.dl.local". Таким образом, будет создана возможность авторизовываться пользователям по короткому суффиксу (user@dl) в полном доменном имени (user@dl.local).

– ввести пароль. При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка). Также следует помнить, что строчные и прописные буквы в пароле различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля;

– выбрать в выпадающем списке допустимую для учетной записи пользователя операцию по работе с системой:

- «Загрузка» – переход к загрузке ШОС;
- «Смена пароля» – переход к смене пароля текущей учетной записи пользователя;
- «Администрирование» – запуск оболочки администратора СДЗ Dallas Lock (действие доступно только для пользователей категорий «Администратор» и «Аудитор»);

– нажать клавишу «Enter» или кнопку «ОК» на экранной форме.

Примечание. При первичной настройке СДЗ необходимо явным образом задать загрузочное устройство из раскрывающегося списка в поле «Загрузочное устройство» на вкладке «Параметры» оболочки администратора (см. п.п. 2.3.3.5 настоящего руководства).

В СДЗ Dallas Lock сначала проверяется возможность входа пользователя с данным именем. В случае отсутствия в СДЗ Dallas Lock учетной записи пользователя с указанным именем выводится соответствующее сообщение, осуществляется возврат к окну авторизации (Рисунок 8).

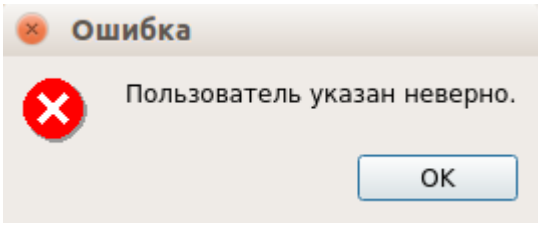

Рисунок 8 – Окно сообщения при неверном имени пользователя

Далее проверяется правильность указанного пользователем пароля. В случае успеха разрешается вход в систему, иначе осуществляется возврат к этапу авторизации. (Рисунок 9).

При использовании аппаратного идентификатора проверяется правильность введенных данных в соответствии с настройками использования АИ для данной учетной записи.

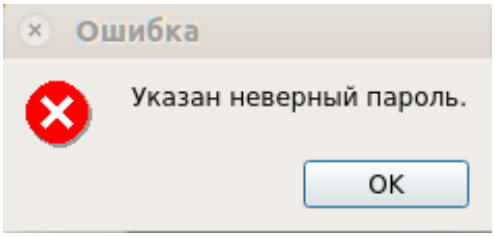

Рисунок 9 – Окно сообщения при неверном вводе пароля учетной записи пользователя

При превышении количества попыток ввода пароля, предусмотренных политикой авторизации СДЗ Dallas Lock, происходит автоматическая блокировка учетной записи пользователя на определенное время (задается политикой авторизации) или навсегда (до явной разблокировки администратором), если политике «Время блокировки учетной записи в случае ввода неправильных паролей» (см. п.п. 2.3.3.3) присвоено значение «Не используется». Выводится соответствующее сообщение (Рисунок 10).

Разблокировка учетной записи пользователя осуществляется автоматически по истечении указанного времени блокировки или после явной разблокировки администратором в окне «Редактирование параметров пользователя» (Рисунок 11). В таком случае у пользователя появляется возможность осуществить вход в систему снова.

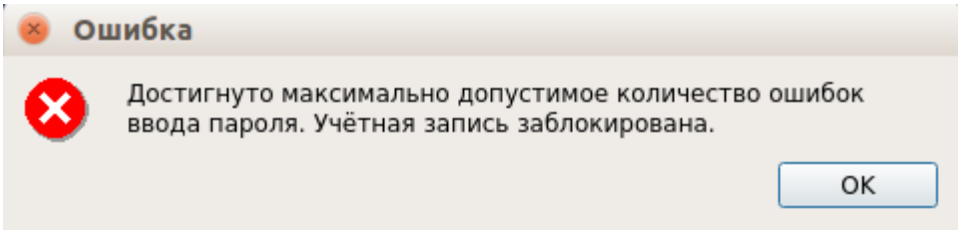

Рисунок 10 – Окно сообщения блокировки учетной записи пользователя

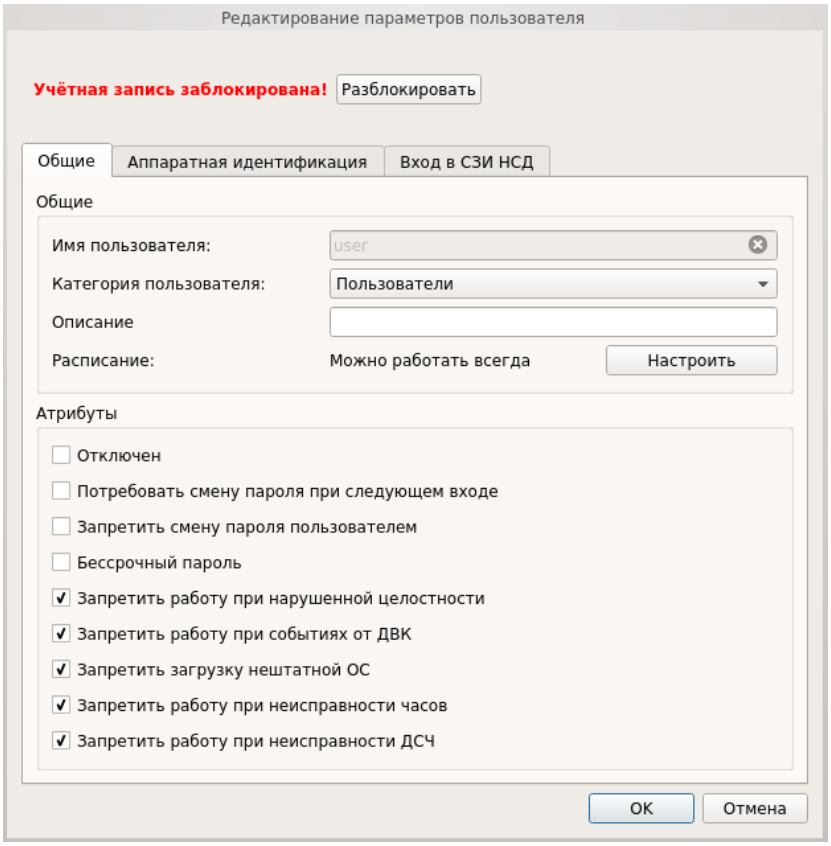

Рисунок 11 – Окно «Редактирование параметров пользователя» при блокировке

При успешной проверке пароля, если в свойствах учетной записи пользователя администратор установил атрибут «Отключен», выводится соответствующее сообщение о неактивности учетной записи пользователя (Рисунок 12). В этом случае включение осуществляется только администратором.

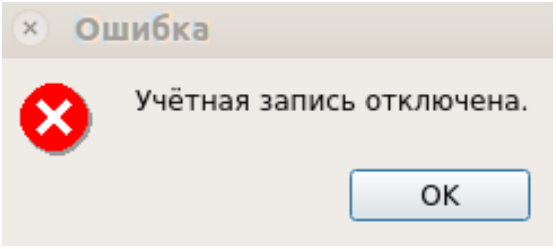

Рисунок 12 – Окно сообщения при попытке входа отключенного пользователя

Далее осуществляется проверка допустимого времени работы согласно установленному для учетной записи пользователя расписанию. В случае, если осуществляется попытка авторизации пользователя в неустановленное для него время работы, выводится соответствующее сообщение (Рисунок 13), осуществляется возврат к этапу авторизации.

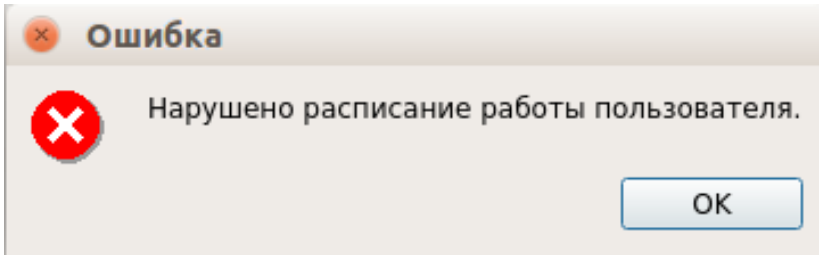

Рисунок 13 – Окно сообщения при попытке входа в неразрешенное время работы

Примечание. Проверка допустимого времени работы осуществляется только в момент авторизации пользователя. При наступлении запрещенного времени работы авторизация в СДЗ Dallas Lock становится невозможной, но изделие не запрещает продолжать ранее инициализированный сеанс.

После успешной авторизации происходит переход к процедуре контроля целостности объектов, указанных в СДЗ Dallas Lock. При успешном прохождении данной процедуры выводится соответствующее сообщение. При входе пользователей с полномочиями аудитора или администратора в окне контроля целостности помимо результата отображается ход выполнения процедуры контроля целостности объектов (Рисунок 14).

После нажатия кнопки «Enter» или «Далее» выполняется выбранное в окне авторизации действие («Загрузка», «Смена пароля» или «Администрирование»).

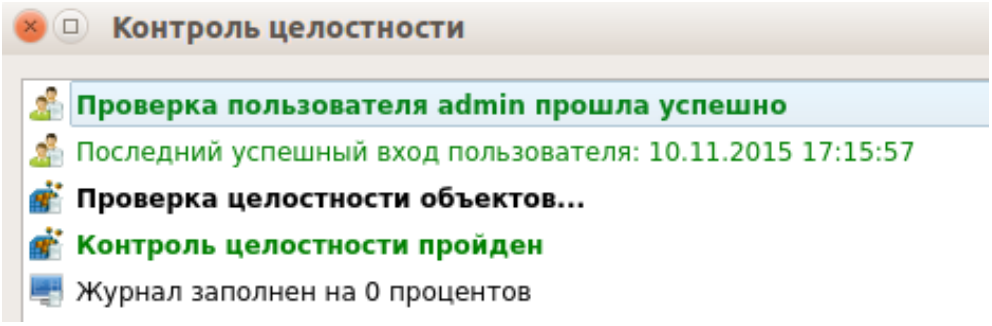

Рисунок 14 – Пример окна сообщения при успешном прохождении контроля целостности

В случае неуспешного прохождения процедуры контроля целостности при входе пользователя, учетной записи которого установлен атрибут «Запретить работу при нарушении целостности» (см. п.п. 2.3.3.1), выводится соответствующее сообщение (Рисунок 15). В окне доступны следующие действия:

«Выход» - возвращает в окно авторизации;

«Выключить» - осуществляется выключение ЭВМ;

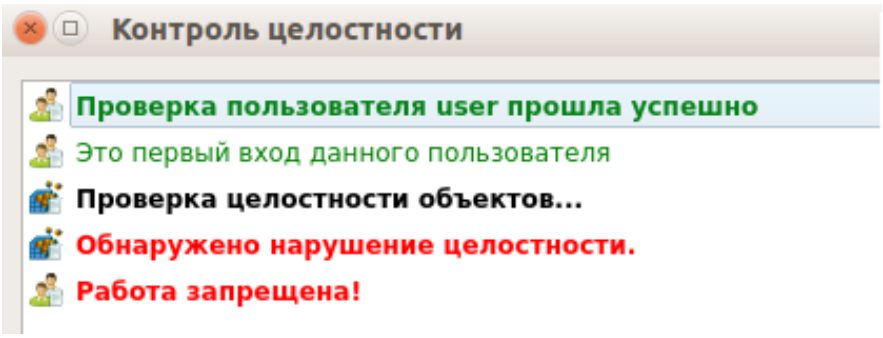

Рисунок 15 – Пример окна сообщения при неуспешном прохождении контроля целостности при входе непривилегированного пользователя

Если пользователю разрешено работать в системе с нарушенной целостностью контролируемых объектов, осуществляется вывод соответствующего сообщения (Рисунок 16) и вход в систему продолжается при нажатии кнопки «Далее». Осуществляется работа в соответствии с выбранным действием («Загрузка», «Смена пароля» или «Администрирование»).

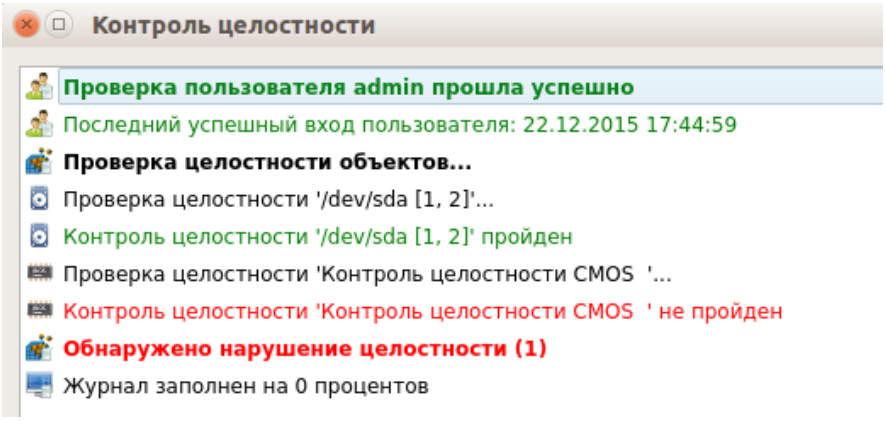

Рисунок 16 – Пример окна сообщения при неуспешном прохождении контроля целостности при входе администратора аудитора

При успешном выполнении процесса контроля целостности производится переход к этапу проверки срока действия пароля для учетной записи пользователя. Загрузка ШОС и администрирование не доступны для учетной записи с истекшим сроком действия пароля. В случае истечения срока действия пароля проверяется разрешение для пользователя на смену своего пароля в соответствии с установленным атрибутом в настройках учетной записи пользователя «Запретить смену пароля пользователем». Если атрибут не установлен, происходит переход к процедуре смены пароля (подробное описание см. п. 2.3.2).

В случае отсутствия разрешения на смену пароля выводится сообщение: «Истёк срок действия пароля. Пароль не может быть изменен». Производится возврат к этапу авторизации.

2.3.1.1 Вход на защищенную ЭВМ с использованием аппаратного идентификатора

Если учетной записи пользователя назначен аппаратный идентификатор, то его необходимо предъявить, а именно:

– вставить его в usb-порт или прикоснуться к считывателю (в зависимости от типа устройства);

– выбрать наименование идентификатора, которое появится в выпадающем меню «аппаратные идентификаторы».

Процедура авторизации с использованием аппаратного идентификатора возможна одним из следующих способов:

– когда АИ сопоставлен учетной записи пользователя – для авторизации необходимо предъявить АИ, ввести имя пользователя и пароль. В таком случае происходит проверка соответствия предъявленного аппаратного идентификатора с введенным именем учетной записи пользователя;

Примечание. В случае предъявления не сопоставленного данной учетной записи пользователя АИ при попытке авторизации будет выведено соответствующее сообщение (Рисунок 17).

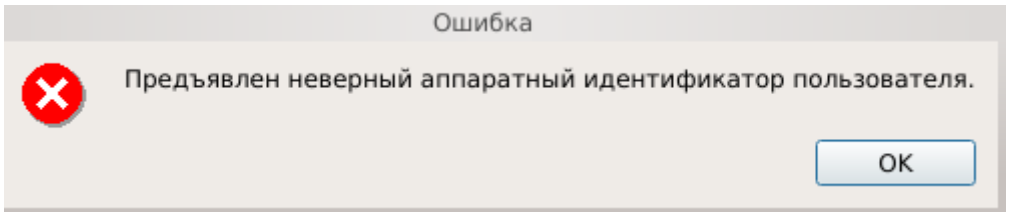

Рисунок 17 – Окно сообщения при предъявлении неверного АИ

– когда АИ сопоставлен учетной записи пользователя и в незащищенной памяти АИ хранится идентификационная информация – для авторизации необходимо предъявить АИ (при этом в поле «Пользователь» будет подставлена хранящаяся в памяти АИ идентификационная информация, поле будет недоступно для редактирования) и ввести пароль учетной записи пользователя;

– когда АИ сопоставлен учетной записи пользователя и в незащищенной памяти АИ хранится идентификационная и аутентификационная информация – для авторизации необходимо предъявить АИ (при этом в поля «Пользователь» и «Пароль» будет подставлена хранящаяся в памяти АИ идентификационная и аутентификационная информация, поля будут недоступны для редактирования);

– когда АИ сопоставлен учетной записи пользователя и в защищенной ПИН-кодом памяти АИ хранится аутентификационная информация – для авторизации

необходимо предъявить АИ (при этом в поле «Пользователь» будет подставлена хранящаяся в памяти АИ идентификационная информация, поле будет недоступно для редактирования) и ввести ПИН АИ, при этом пароль будет получен из защищенной памяти АИ, если введен верный ПИН.

2.3.2 Смена пароля

При выборе действия «Смена пароля» осуществляется переход к диалоговому окну процедуры смены пароля учетной записи пользователя (Рисунок 18).

Если администратором установлен атрибут в свойствах учетной записи пользователя «Потребовать смену пароля при следующем входе» или истек срок действия пароля учетной записи пользователя, предусмотренный политикой авторизации СДЗ Dallas Lock, осуществляется автоматический переход к диалоговому окну процедуры смены пароля учетной записи пользователя независимо от выбранного действия.

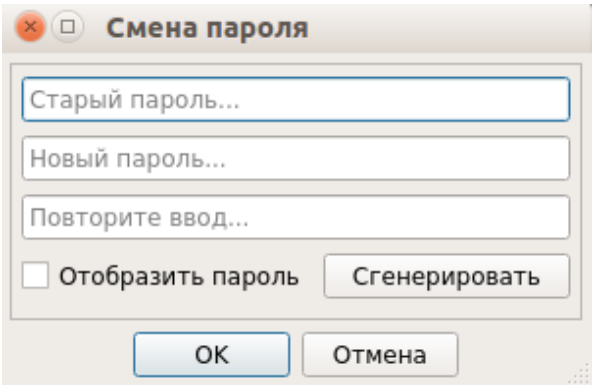

Рисунок 18 – Диалоговое окно смены текущего пароля учетной записи пользователя

Указанное действие недоступно, если администратором установлен атрибут в свойствах учетной записи пользователя «Запретить смену пароля пользователем».

В этом случае при попытке смены пароля пользователем выдается соответствующее сообщение о действующем запрете (Рисунок 19).

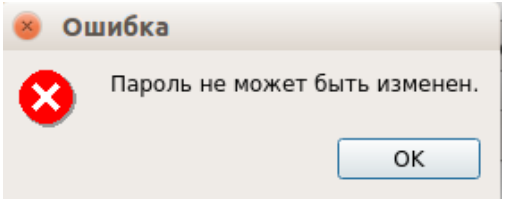

Рисунок 19 – Окно сообщения при запрете смены пароля пользователем

Для смены пароля необходимо корректно ввести:

– текущий пароль;
– новый пароль (должен отвечать установленным политикам сложности паролей);
– подтвердить новый пароль.

Также пользователь имеет возможность воспользоваться генератором паролей.

При вводе пароля следует помнить, что строчные и прописные буквы в пароле различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.

При несоответствии пароля требованиям политики сложности паролей выводится соответствующее сообщение, смена пароля не производится, осуществляется возврат к процедуре смены пароля (Рисунок 20 и 19).

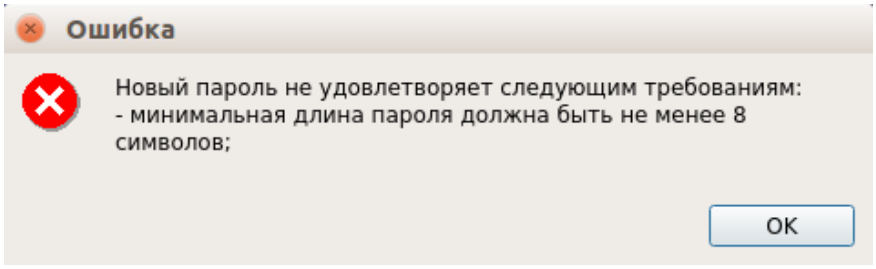

Рисунок 20 – Сообщение при несоответствии длины пароля учетной записи пользователя политике сложности паролей

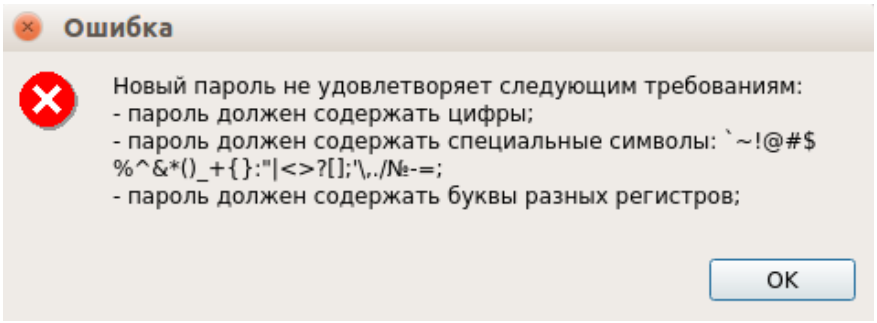

Рисунок 21 – Сообщение при несоответствии сложности пароля учетной записи пользователя политике сложности паролей

При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка). Для контроля правильности ввода значений пароля можно воспользоваться чекбоксом «Отобразить пароль».

Если значения пароля в поле ввода и в поле повтора не совпадают, выводится соответствующее сообщение и осуществляется возврат к окну смены пароля (Рисунок 22).

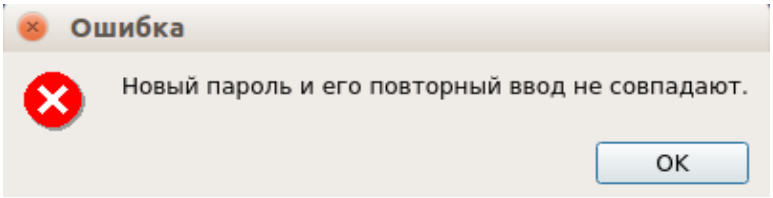

Рисунок 22 – Сообщение при несовпадении паролей

При успешной смене текущего пароля учетной записи пользователя выводится соответствующее сообщение (Рисунок 23) и осуществляется возврат в окно авторизации.

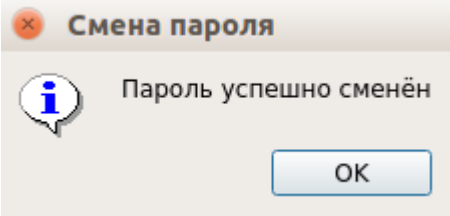

Рисунок 23 – Сообщение при успешной смене текущего пароля учетной записи пользователя

Примечание. При использовании авторизационных данных из аппаратного идентификатора новый пароль записывается в аппаратный идентификатор.

2.3.3 Администрирование СДЗ Dallas Lock

При выборе действия «Администрирование» осуществляется запуск оболочки администратора (действие доступно только для пользователей категорий «Администратор» и «Аудитор»).

В главном окне оболочки администратора (Рисунок 24) расположены вкладки, обеспечивающие доступ к соответствующим разделам:

– «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.

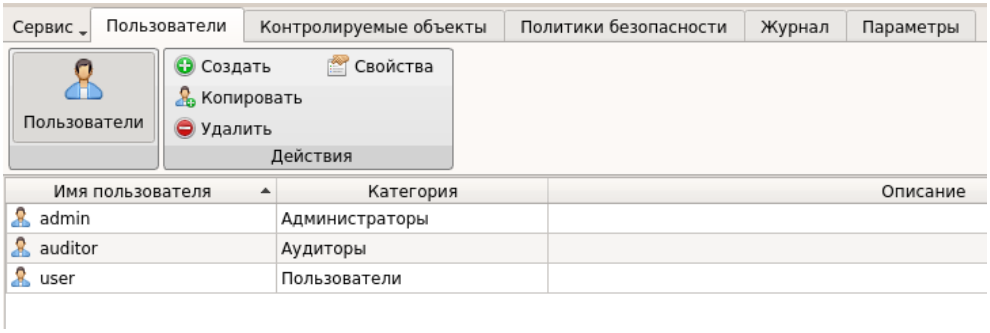

Рисунок 24 – Главное окно. Пользователи

При попытке запуска оболочки администратора пользователем, не входящим в категорию «Аудитор» или «Администратор», выводится соответствующее сообщение (Рисунок 25).

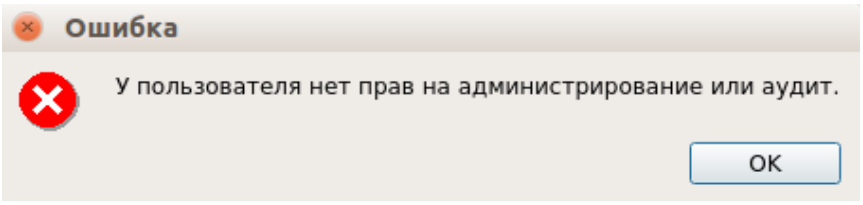

Рисунок 25 – Сообщение при запрете на администрирование СДЗ Dallas Lock

2.3.3.1 Управление учетными записями пользователей

В разделе «Пользователи» в виде таблицы отображаются все учетные записи пользователей, зарегистрированные в СДЗ Dallas Lock. Сортировка пользователей по имени, категории или описанию (по возрастанию/убыванию) осуществляется нажатием на заголовки соответствующих столбцов левой кнопкой мыши.

Возможны следующие действия с учетными записями пользователей:

– «Создать»;

– «Копировать»;

– «Удалить»;

– «Свойства»;

– «Задать пароль».

Реализация перечисленных действий осуществляется через соответствующие функциональные кнопки на панели «Действия» или через контекстное меню при нажатии правой кнопкой мыши на выбранной учетной записи пользователя.

При нажатии кнопки «Свойства» выводится окно редактирования параметров учетной записи выбранного пользователя (Рисунок 26).

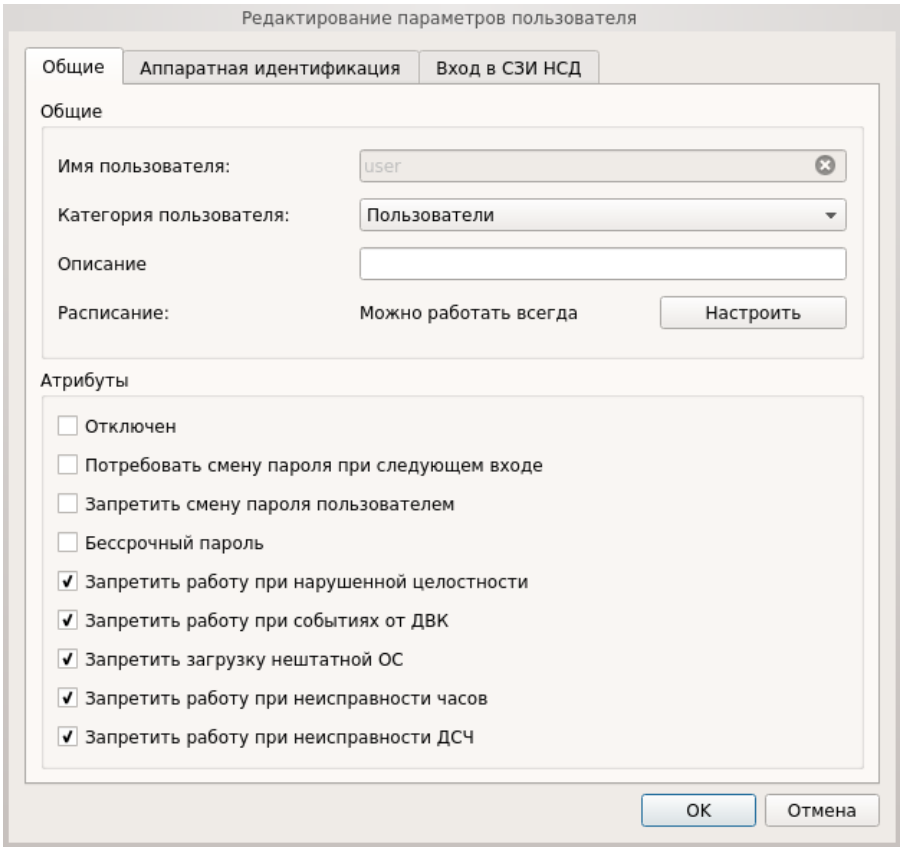

Рисунок 26 – Окно редактирования параметров учетной записи пользователя. Данные пользователя

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 систему (Рисунок 27).

В окне «Расписание» в верхней части окна задается период времени работы, в левой части окна задаются допустимые для работы пользователя дни недели.

Для быстрой настройки предусмотрены дополнительные кнопки:

– «Разрешить все» - разрешено любое время для работы;

– «Запретить все» - запрещено любое время для работы;

– «Рабочее время» - устанавливается стандартный график работы (пн-пт, 09.00 – 18.00).

Также имеется возможность указать период действия учетной записи в соответствующем разделе.

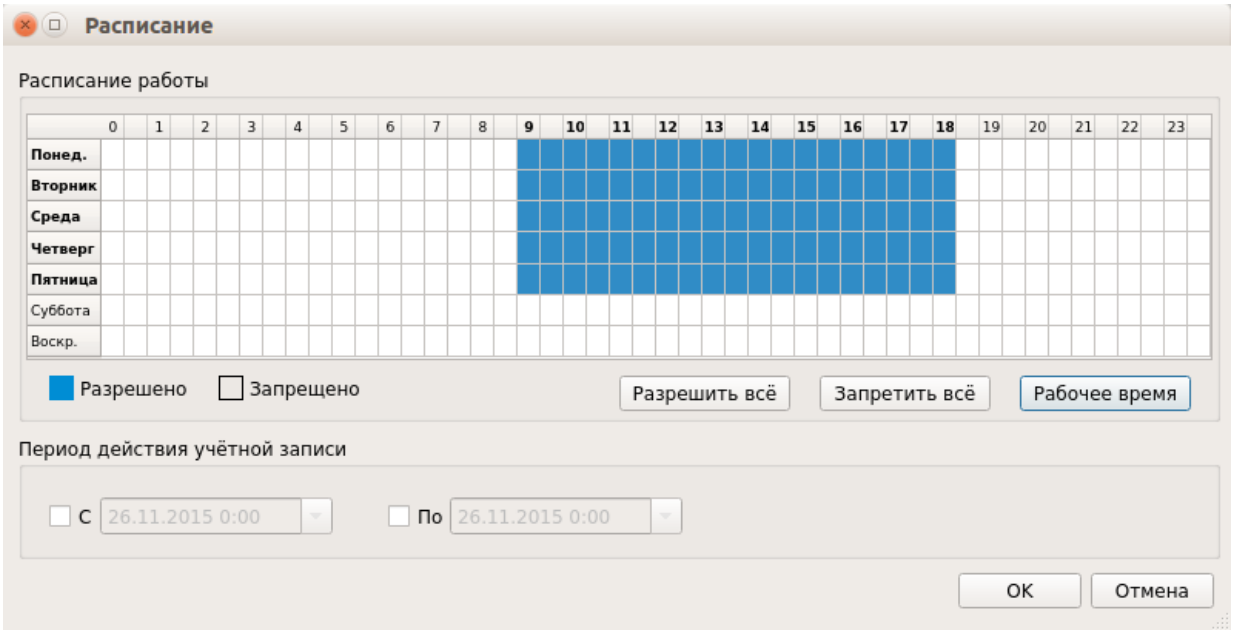

Рисунок 27 – Окно редактирования разрешенного времени работы в системе

Допустимо присвоение следующих атрибутов учетной записи пользователя:

– «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 учетную запись пользователя не распространяется действие политики безопасности, которая устанавливает максимальный срок действия пароля. Установка данного атрибута не запрещает смену пароля учетной записи 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» (Рисунок 28) возможно назначение аппаратного идентификатора в следующем порядке:

– предъявить аппаратный идентификатор и выбрать его из списка;

– 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 можно нажать кнопку «Очистить» – произойдет очистка поля «Имя пользователя»;

– после нажатия кнопки «Ок» данный идентификатор присваивается редактируемому пользователю.

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.

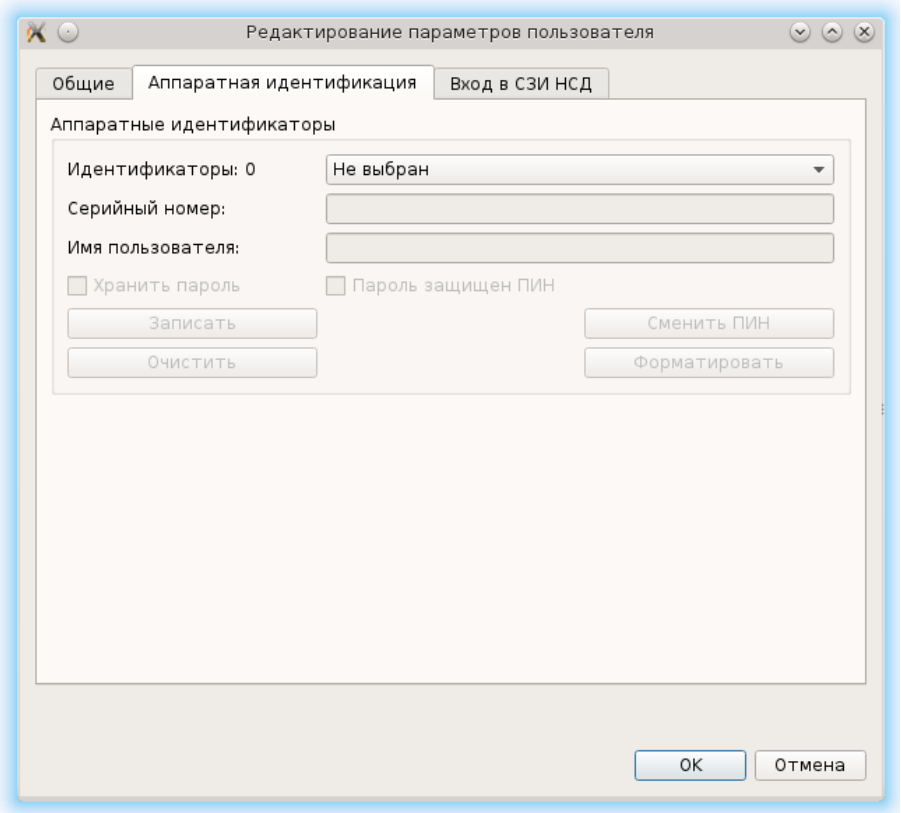

Рисунок 28 – Окно редактирования параметров учетной записи пользователя. Аппаратная идентификация

При необходимости возможно задать дополнительные параметры аппаратной идентификации:

– «Записать» – данная кнопка позволяет записывать в незащищенную и защищенную память АИ идентификационную и аутентификационную информацию (имя учетной записи 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» (Рисунок 29) ввести старый, новый ПИН и повторить ввод нового ПИН;

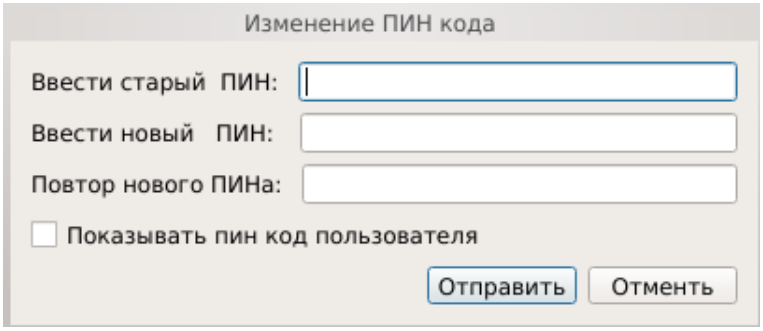

Рисунок 29 – Окно смены ПИН-кода

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 (Рисунок 30).

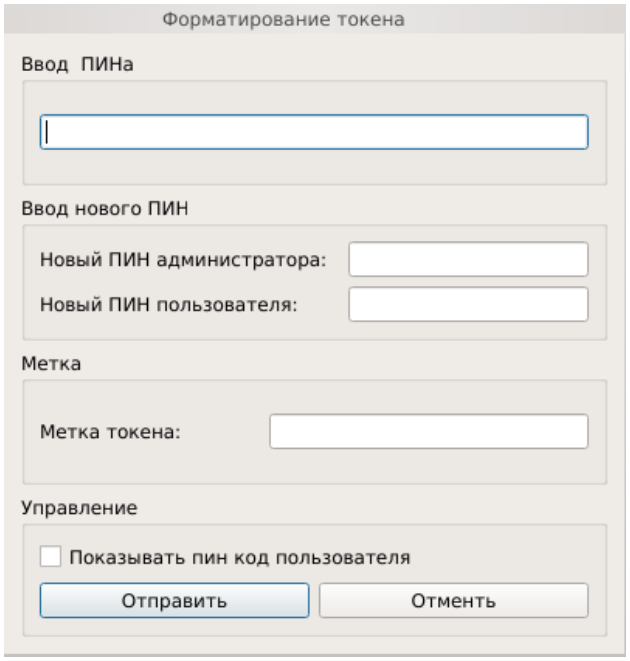

Рисунок 30 – Окно форматирование токена

В окне «Форматирование токена» ввести следующую информацию:

– Старый ПИН администратора;

– Новый ПИН администратора;

– Новый ПИН пользователя;

– Метку токена;

– Нажать кнопку «Отправить».

На вкладке «Вход в СЗИ НСД» (Рисунок 31) 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 НСД:

– «Передавать аппаратный идентификатор в СЗИ НСД»;

– «Передавать пароль в СЗИ НСД».

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

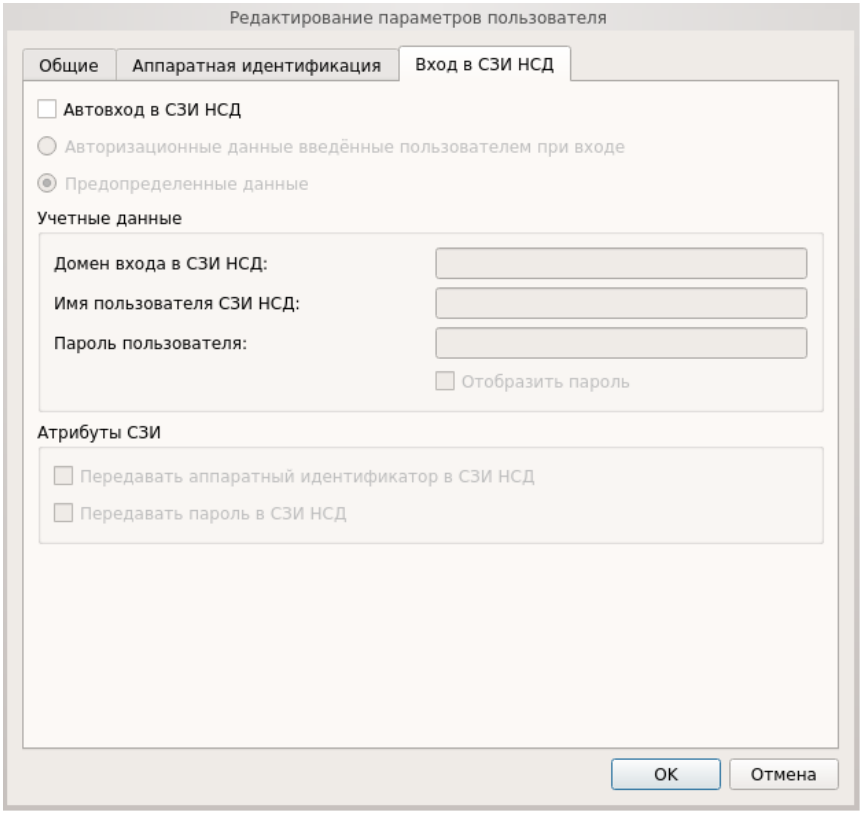

Рисунок 31 – Окно редактирования параметров учетной записи пользователя. Вход в СЗИ НСД

При нажатии кнопки «Создать» выводится окно создания новой учетной записи пользователя. Процедура создания новой учетной записи пользователя аналогична редактированию параметров учетной записи пользователя, но начинается с ввода имени учетной записи пользователя и по окончанию настройки выводится окно «Ввод пароля», в котором необходимо установить пароль для учетной записи пользователя. Имя учетной записи пользователя не может быть пустым и содержать более 31 символа.

Примечание. Доменные учетные записи нельзя создать средствами СДЗ Dallas Lock, можно зарегистрировать уже существующие. В случае необходимости создания новой доменной учетной записи пользователя, следует создать ее средствами администрирования на контроллере домена и после этого зарегистрировать в СДЗ Dallas Lock.

Регистрация доменной учетной записи пользователя в СДЗ Dallas Lock производится в формате «[dom]\[name]», где [dom] – это короткое имя домена, [name] – это имя учетной записи. Также есть возможность регистрации доменной учетной записи пользователя по маске «**» или «[dom]*», где «*» означает «любой».

При регистрации доменной учетной записи пользователя в СДЗ Dallas Lock пароль не запрашивается, также для доменных учетных записей в СДЗ Dallas Lock кнопка «Задать пароль» в окне «Действия» на вкладке «Пользователи» неактивна.

При нажатии кнопки «Копировать» выводится окно создания новой учетной записи пользователя, в котором заполнены свойства и атрибуты, соответствующие эталонной учетной записи пользователя.

При нажатии кнопки «Удалить» осуществляется удаление выбранной учетной записи пользователя без вывода предупреждения.

При выборе действия «Задать пароль» в появившемся окне ввода пароля (Рисунок 32) имеется возможность установить новый пароль учетной записи пользователя.

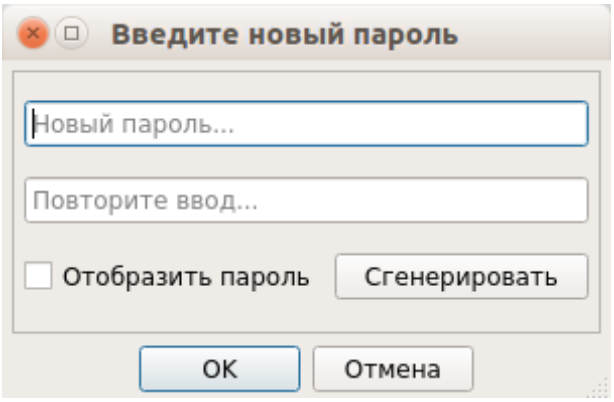

Рисунок 32 – Окно установки пароля для учетной записи пользователю

2.3.3.2 Контроль целостности

В разделе «Контролируемые объекты» в виде таблицы отображаются все контролируемые объекты, зарегистрированные в СДЗ Dallas Lock (Рисунок 33).

Сортировка контролируемых объектов по идентификатору, описанию, алгоритму, параметрам, эталонным или расчетным контрольным суммам (по возрастанию/убыванию) осуществляется нажатием на заголовки соответствующих столбцов левой кнопкой мыши.

Выделяются следующие категории контролируемых объектов:

– «Файловая система»;

– «Реестр»;

– «Области диска»;

– «BIOS CMOS»;

– «Аппаратная конфигурация».

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

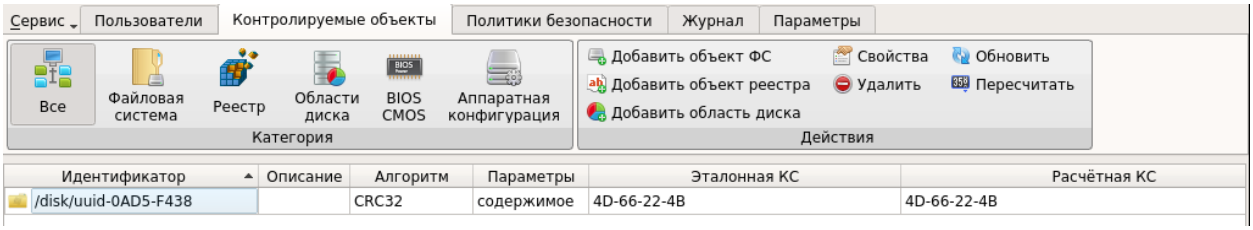

Рисунок 33 – Главное окно. Контролируемые объекты

Возможны следующие действия с контролируемыми файлами:

– «Добавить объект ФС»;

– «Добавить объект реестра»;

– «Добавить область диска»;

– «Свойства»;

– «Удалить»;

– «Обновить»;

– «Пересчитать».

Реализация перечисленных действий осуществляется через соответствующие функциональные кнопки в панели «Действия».

Контроль целостности объектов файловой системы.

При нажатии кнопки «Добавить объект ФС» выполняется вывод диалогового окна «Добавить объект файловой системы» (Рисунок 34), где доступно редактирование следующих параметров:

– «Путь» – путь к файлу или каталогу (директорию) контролируемого объекта. Задается при добавлении объекта ФС, в дальнейшем не может быть изменен;

– «Описание» – поле предназначено для текстового описания контролируемого объекта;

Допустима установка следующих атрибутов:

– «Алгоритм расчета» – из выпадающего списка выбирается алгоритм расчета контрольной суммы объекта файловой системы;

– «Учитывать наличие» – при контроле целостности объекта файловой системы будет проверяться только 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.

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

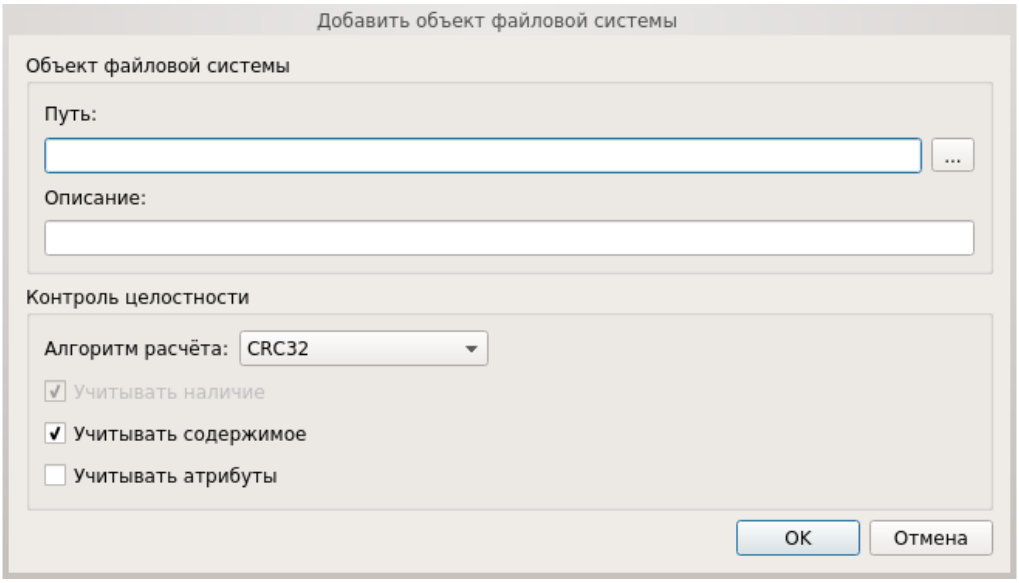

Рисунок 35 – Окно добавления объекта ФС в контролируемые объекты

При нажатии кнопки «Свойства» выводится окно редактирования выбранного объекта ФС аналогичное окну добавления объекта ФС в контролируемые объекты. Путь к объекту ФС в данном окне изменить нельзя.

При нажатии кнопки «Удалить» выполняется удаление выбранных объектов ФС из списка контролируемых объектов.

При нажатии кнопки «Обновить» выполняется обновление расчетных КС списка контролируемых объектов ФС.

При нажатии кнопки «Пересчет» выполняется пересчет эталонных контрольных сумм контролируемых объектов ФС.

Контроль целостности объектов реестра Windows

При нажатии кнопки «Добавить объект реестра» осуществляется вывод диалогового окна «Добавить объект реестра Windows» (Рисунок 36), где доступно редактирование следующих параметров:

– «Файл ветки реестра» – выбирается путь к файлу реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен;

– «Путь реестра» – выбирается путь к контролируемому объекту в указанном выше файле реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен;

– «Описание» – поле предназначено для текстового описания контролируемого объекта.

Допустима установка следующих атрибутов:

– «Алгоритм расчета» – из выпадающего списка выбирается 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».

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

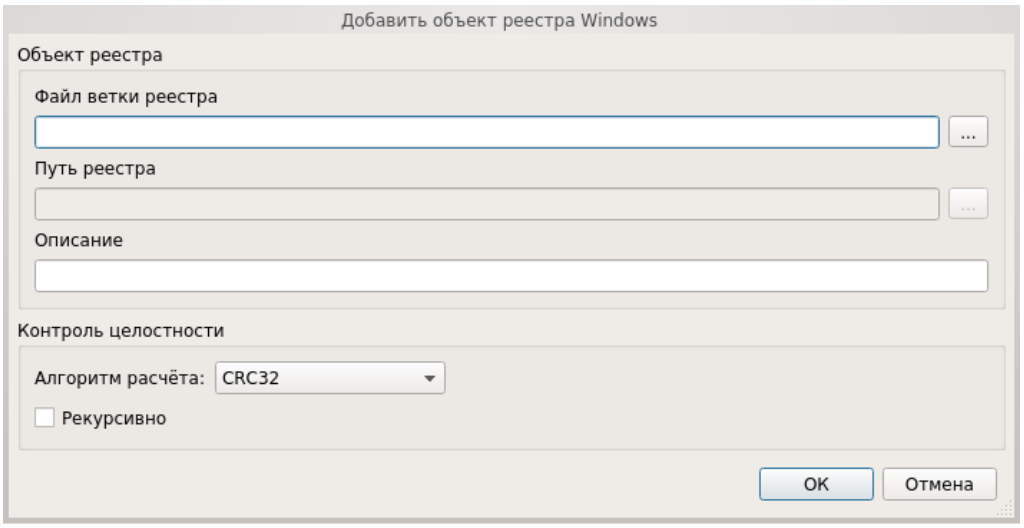

Рисунок 36 – Окно добавления объекта реестра в контролируемые объекты

При нажатии кнопки «Свойства» выводится окно редактирования выбранного объекта реестра аналогичное окну добавления объекта реестра в контролируемые объекты. Путь к контролируемому объекту реестра в данном окне изменить нельзя.

При нажатии кнопки «Удалить» осуществляется удаление выбранных объектов реестра из списка контролируемых объектов без предупреждения.

При нажатии кнопки «Обновить» осуществляется обновление расчетных КС списка контролируемых объектов реестра.

При нажатии кнопки «Пересчет» осуществляется пересчет эталонных контрольных сумм контролируемых объектов реестра.

Контроль целостности областей жесткого диска

Контроль целостности может быть назначен только для локальных дисков.

При нажатии кнопки «Добавить область диска» осуществляется вывод диалогового окна «Добавление области диска» (Рисунок 37), где доступно редактирование следующих параметров:

– «Диск» – из выпадающего списка выбирается жесткий диск, подключенный к ЭВМ. При выборе диска в соответствующих полях автоматически отображается его размер,

размер сектора и количество секторов. Задается при добавлении объекта, в дальнейшем не может быть изменен;

– «Описание» – поле предназначено для текстового описания контролируемого объекта.

Допустима установка следующих атрибутов:

– «Начальный сектор» – задается начальный сектор области жесткого диска;

– «Количество секторов» – задается количество секторов жесткого диска, подлежащих контролю целостности;

– «Алгоритм» – из выпадающего списка выбирается алгоритм расчета контрольных сумм при контроле целостности области жесткого диска.

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

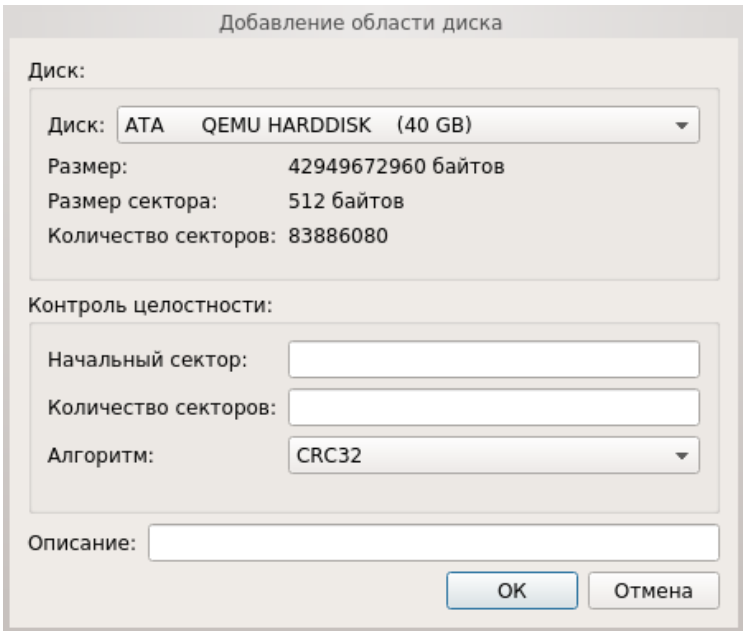

Рисунок 37 – Окно добавления области диска в контролируемые объекты

При нажатии кнопки «Свойства» выводится окно редактирования контролируемых областей диска аналогичное окну добавления области диска в контролируемые объекты. Наименование жесткого диска в данном окне изменить нельзя.

При нажатии кнопки «Удалить» осуществляется удаление выбранных областей жесткого диска из списка контролируемых объектов без предупреждения.

При нажатии кнопки «Обновить» осуществляется обновление списка контролируемых областей жесткого диска.

При нажатии кнопки «Пересчет» осуществляется пересчет эталонных контрольных сумм контролируемых областей жесткого диска.

Контроль 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 38).

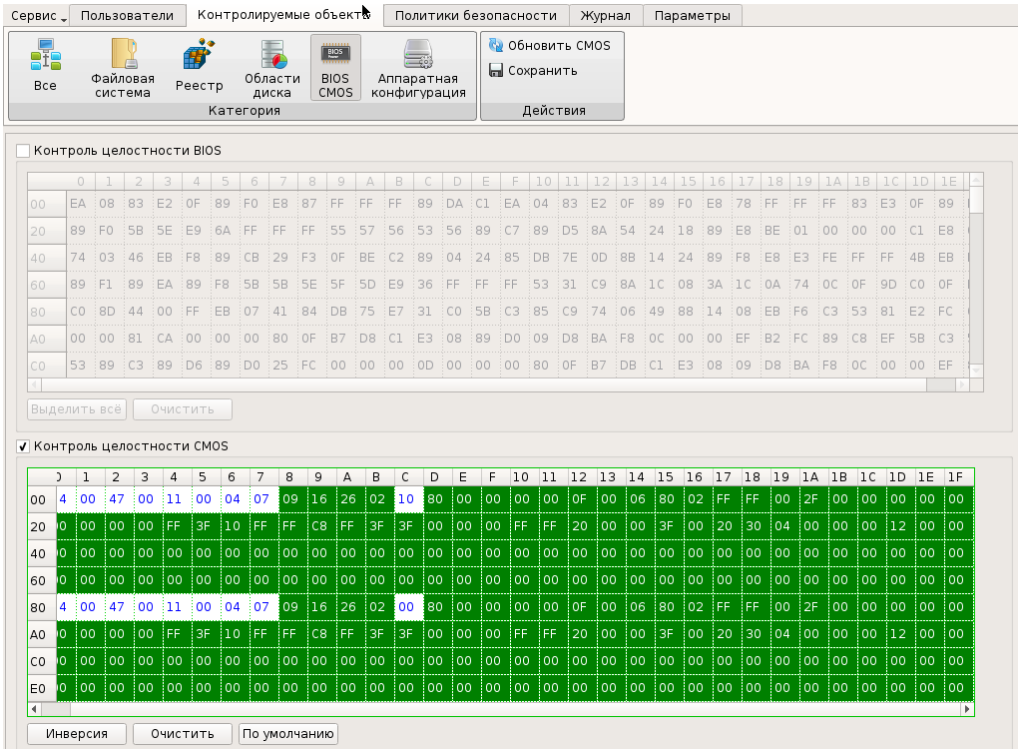

Рисунок 38 – Контроль BIOS CMOS

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.

Контроль целостности объектов аппаратной конфигурации СВТ

В списке объектов аппаратной конфигурации автоматически отображаются все аппаратные устройства, установленные в ЭВМ.

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 (Рисунок 39) «Контролировать группу» и напротив конкретного идентификатора в группе «исключить из контроля».

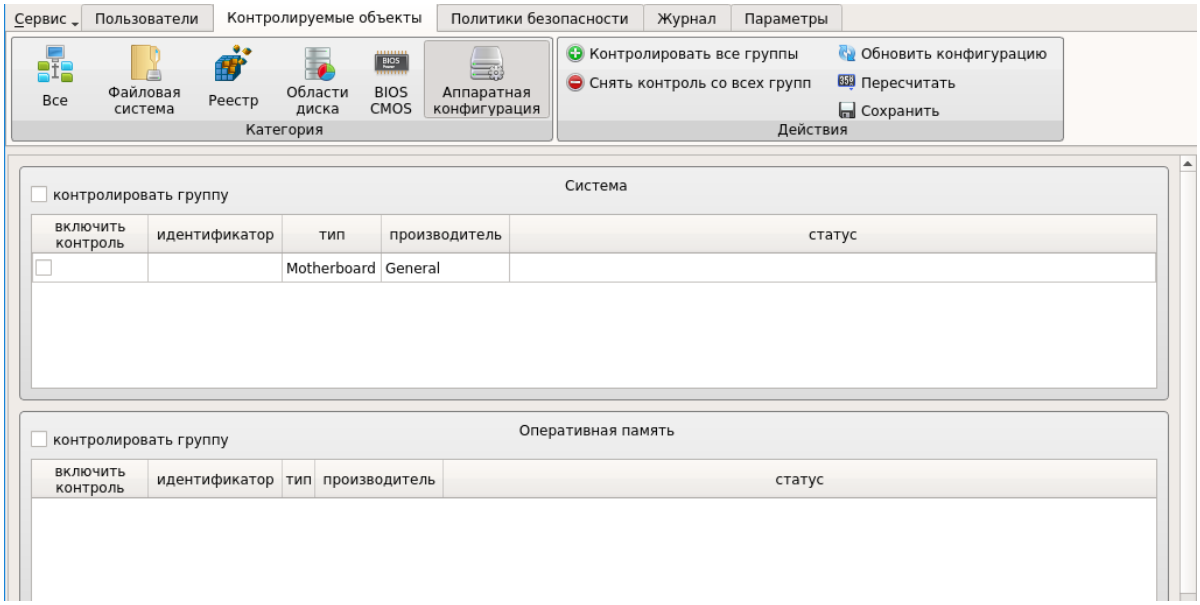

Рисунок 39 – Главное окно. Контролируемые объекты аппаратной конфигурации СВТ

Для категории «Аппаратная конфигурация» выводятся списки групп аппаратной конфигурации (Таблица 1).

Таблица 1 – 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».

2.3.3.3 Настройка авторизации в СДЗ Dallas Lock

В разделе «Политики безопасности» в виде таблицы отображаются параметры и значения политик безопасности.

Выделяются следующие категории политик безопасности:

– «Политики авторизации»;

– «Политики паролей»;

– «Политики ДСЧ».

Просмотр параметров и значений конкретной категории политик осуществляется через соответствующие кнопки в панели «Политики» (Рисунок 41, 37 и 38). Описание и возможные значение политик приведены в таблицах 2, 3 и 4.

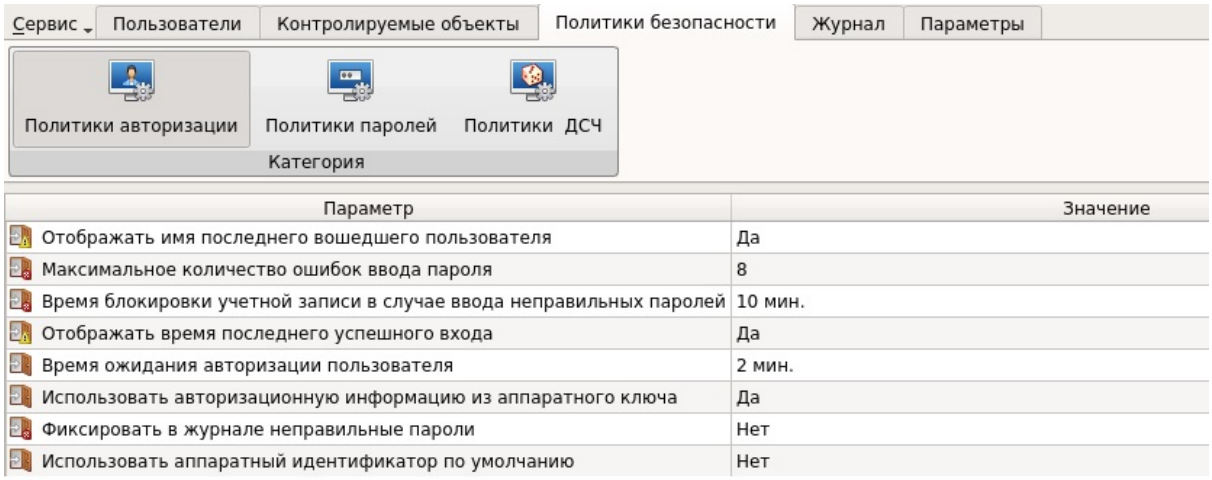

Рисунок 40 – Главное окно. Политики авторизации

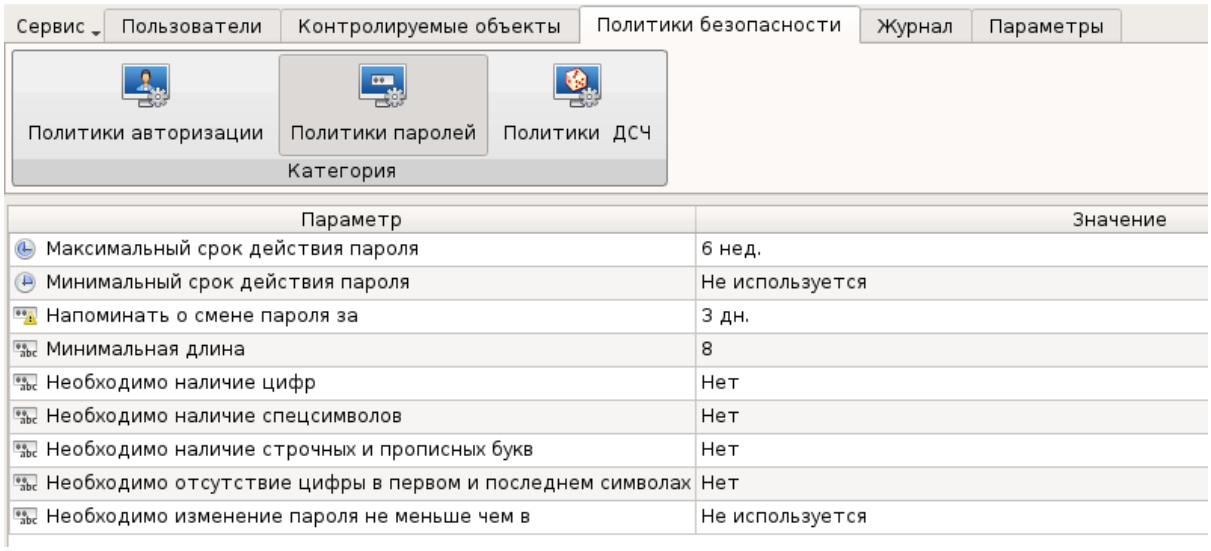

Рисунок 41 – Главное окно. Политики паролей

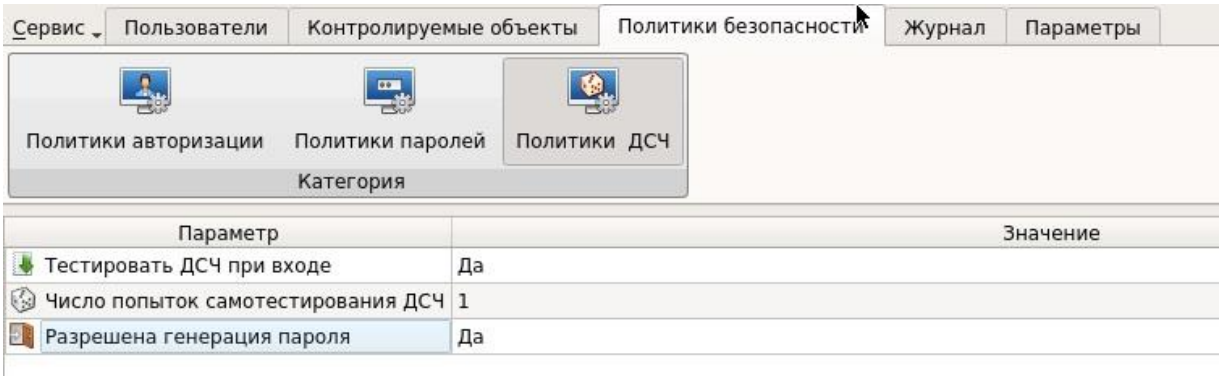

Рисунок 42 – Главное окно. Политики ДСЧ

Редактирование значений параметров политик осуществляется через соответствующие диалоговые окна, вызываемые двойным нажатием левой кнопки мыши на поле таблицы с редактируемой записью. Пример диалогового окна редактирования параметров политики безопасности (Рисунок 43).

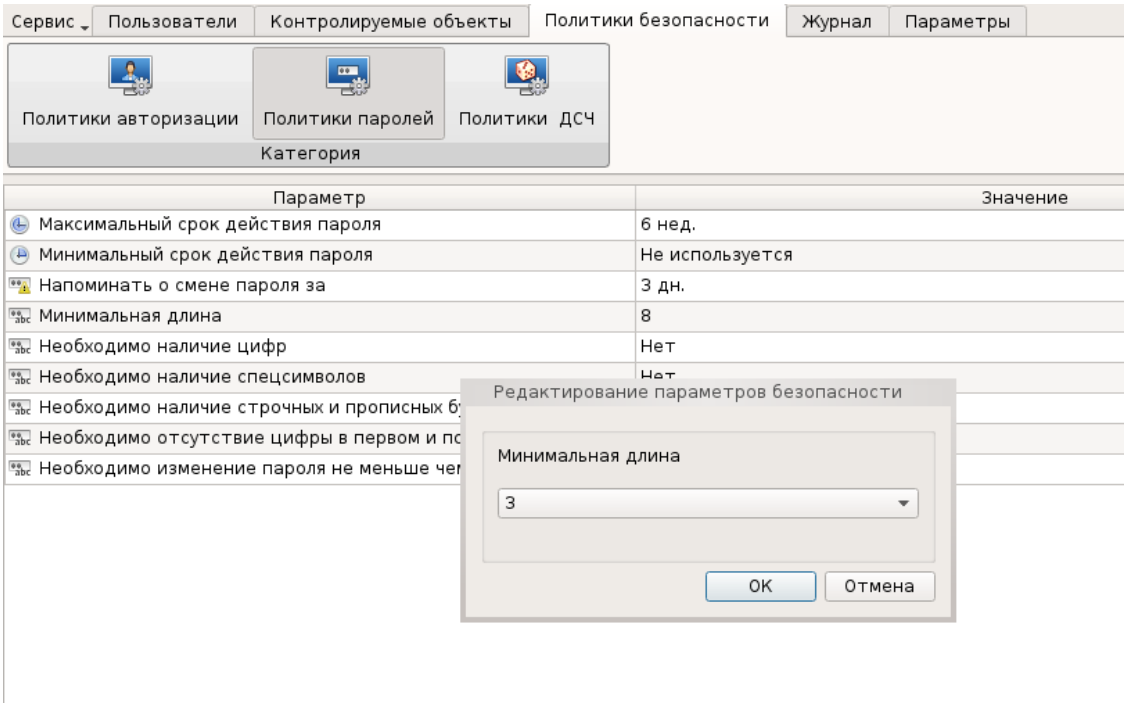

Рисунок 43 – Диалоговое окно редактирования параметров политики безопасности

Таблица 2 – 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.

Параметр политики	Описание
	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 время 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 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 3 – Список параметров категории «Политики паролей»

Параметр политики	Описание
«Максимальный срок действия пароля»	Параметр устанавливает максимальный срок действия пароля пользователей. По истечении срока действия

Параметр политики	Описание
	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
«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»

Параметр политики	Описание
«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 4 – 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
«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.

Перечень вариантов параметров политик безопасности предполагается выбирать из соответствующих выпадающих списков или путем выбора одного из вариантов «Да/Нет».

Сохранение измененных значений параметров политики безопасности осуществляется после нажатия кнопки «ОК» в диалоговом окне редактирования параметров политики безопасности.

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.

2.3.3.4 Регистрация и аудит

В разделе «Журнал» в виде таблицы отображаются все события, зарегистрированные в ходе работы СДЗ Dallas Lock (Рисунок 44).

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).

Выделяются следующие категории событий:

– «Входы»;

– «Администрирование»;

– «Учетные записи»;

– «Целостность».

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

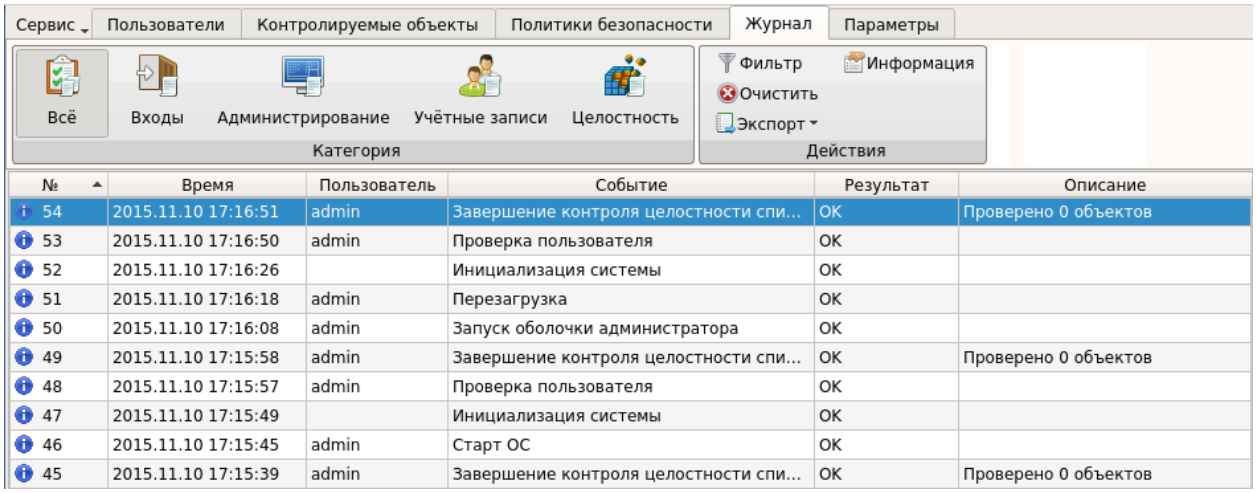

Рисунок 44 – Главное окно. Журнал

Возможны следующие действия с журналом:

– «Фильтр»;

– «Очистить»;

– «Экспорт»;

– «Информация».

Реализация перечисленных действий осуществляется через соответствующие функциональные кнопки на панели «Действия».

При нажатии кнопки «Фильтр» выводится всплывающее меню (Рисунок 45), через которое, по нажатию правой кнопки мыши, допустимо назначение:

– текстового фильтра;

– интервального фильтра;

– фильтра по значению;

– регулярного выражения;

– автофильтра (Рисунок 46).

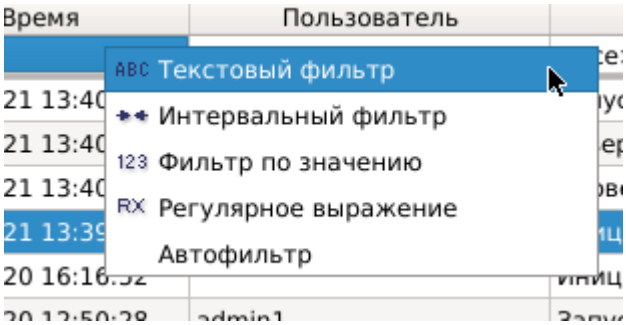

Рисунок 45 – Главное окно. Назначение фильтра

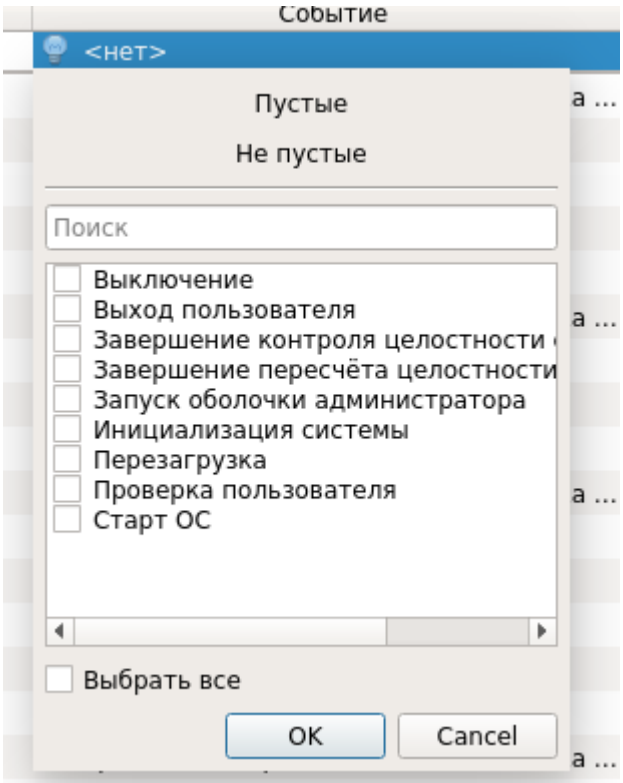

Рисунок 46 – Меню назначения автофильтра журнала

Результат применения фильтра журнала по заданию пользователя «admin» (Рисунок 47).

Время	Пользователь	Событие	Результат
<все>	admin	<все>	<все>
2015.11.10 17:16:51	admin	Завершение контроля целостности списка ...	OK
2015.11.10 17:16:50	admin	Проверка пользователя	OK
2015.11.10 17:16:18	admin	Перезагрузка	OK
2015.11.10 17:16:08	admin	Запуск оболочки администратора	OK
2015.11.10 17:15:58	admin	Завершение контроля целостности списка ...	OK
2015.11.10 17:15:57	admin	Проверка пользователя	OK
2015.11.10 17:15:45	admin	Старт ОС	OK
2015.11.10 17:15:39	admin	Завершение контроля целостности списка ...	OK
2015.11.10 17:15:37	admin	Проверка пользователя	OK
2015.11.10 17:09:56	admin	Старт ОС	OK
2015.11.10 16:30:06	admin	Запуск оболочки администратора	OK
2015.11.10 16:30:00	admin	Завершение контроля целостности списка ...	OK

Рисунок 47 – Результат применения фильтра журнала по значению даты события

Результат применения автофильтра журнала по наименованию события (Старт ОС / Перезагрузка) (Рисунок 48).

Время	Пользователь	Событие	Результат
<все>	admin	2 строк	<все>
2015.11.10 17:16:18	admin	Перезагрузка	OK
2015.11.10 17:15:45	admin	Старт ОС	OK
2015.11.10 17:09:56	admin	Старт ОС	OK

Рисунок 48 – Результат применения автофильтра журнала по наименованию события

Удаление или отключение назначенного фильтра производится через вызов соответствующего меню при нажатии правой клавиши мыши на поле фильтра.

При нажатии кнопки «Очистить» выводится соответствующее предупреждение (Рисунок 49).

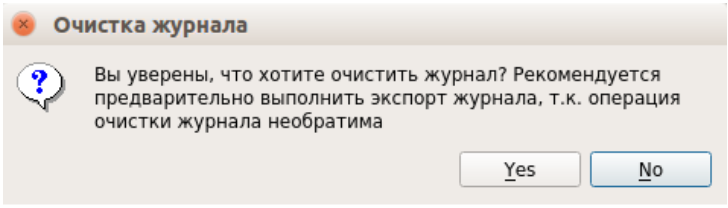

Рисунок 49 – Сообщение «Очитка журнала»

После очистки журнала порядковая нумерация новых событий продолжается далее, а не начинается заново.

Поскольку операция удаления записей журнала необратима, перед очисткой журнала рекомендуется произвести экспорт записей журнала в файл. При нажатии кнопки «Экспорт» из выпадающего списка выбирается формат создаваемого файла (Рисунок 50). Данная функция также доступна пользователям категории «Аудиторы».

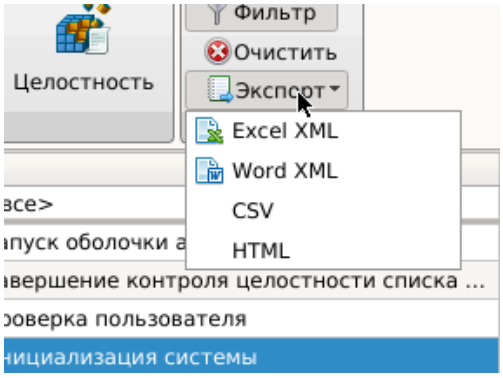

Рисунок 50 – Главное окно. Меню экспорта журнала в файл

При нажатии кнопки «Информация» выводится соответствующее информационное окно для выбранного события (Рисунок 51).

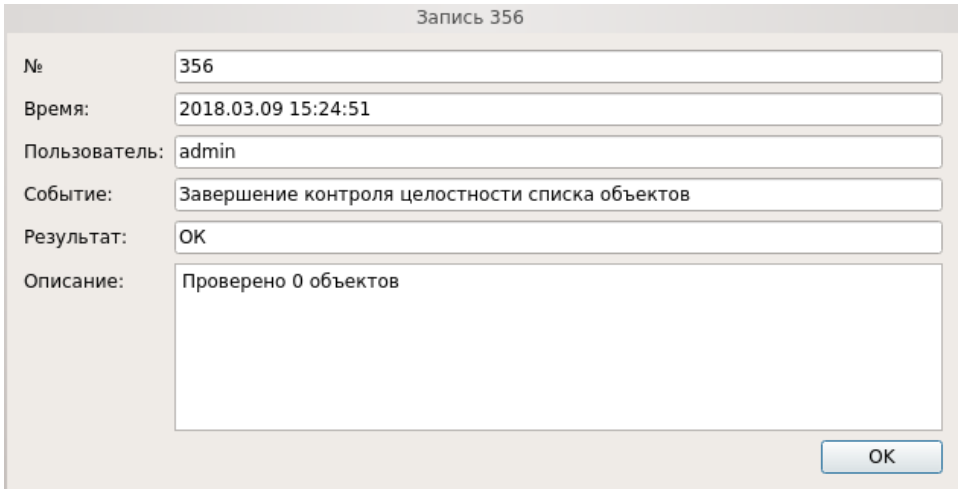

Рисунок 51 – Информационное окно

2.3.3.5 Управление параметрами платы

В разделе «Параметры» отображаются следующие категории:

– «Плата КТ»;

– «Параметры загрузки»;

– «Параметры сети».

Просмотр параметров и значений конкретной категории осуществляется через соответствующие кнопки в панели «Категория» (Рисунок 49, 50 и 51).

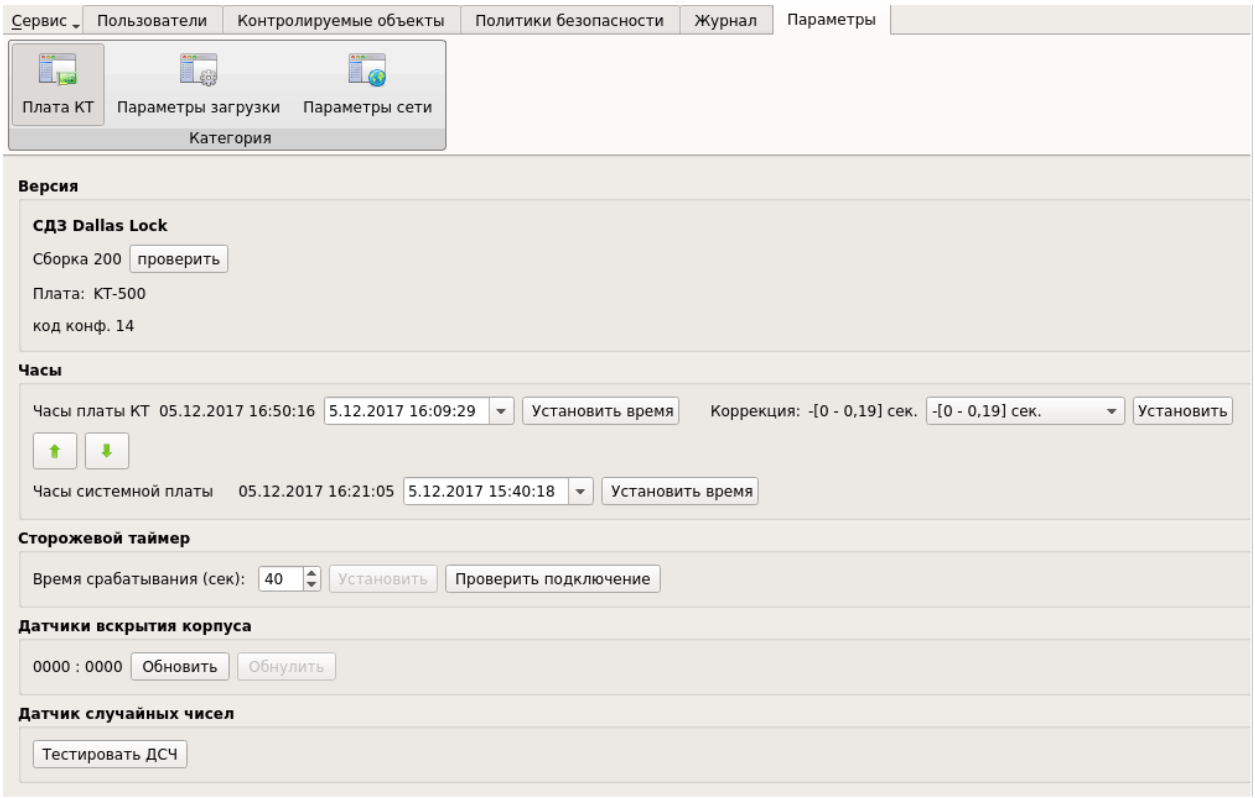

Рисунок 52 – Главное окно. Плата КТ

Категория «Плата КТ»:

– «Версия» – на данной панели отображается техническая информация об изделии.

– «Часы» – на данной панели устанавливаются часы в текстовом поле. Если плата не оснащена часами или часы неисправны, используется время системной платы.

Есть возможность коррекции времени часов платы при нарушении точности их работы с помощью параметра «Коррекция». Используя заданные диапазоны суточных отклонений в секундах с различным знаком «+/-» можно ускорить или замедлить темп хода часов.

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

– «Сторожевой таймер» - для сторожевого таймера возможно установить/изменить время срабатывания в секундах. Проверить подключение сторожевого таймера можно при помощи соответствующей кнопки;

– «Датчик вскрытия корпуса» (ДВК) - если установлено значение «0000:0000» - вскрытие не зафиксировано, в противном случае ДВК сработали и вскрытие зафиксировано. Обновить и обнулить результат можно при помощи соответствующих кнопок;

Примечание. Параметр «Датчик вскрытия корпуса» применим только для варианта исполнения изделия ПФНА.501410.003-01 (плата формата PCIe «КТ-500»).

– «Датчик случайных чисел» (ДСЧ) – возможен запуск тестирования ДСЧ из оболочки администратора при помощи соответствующей кнопки.

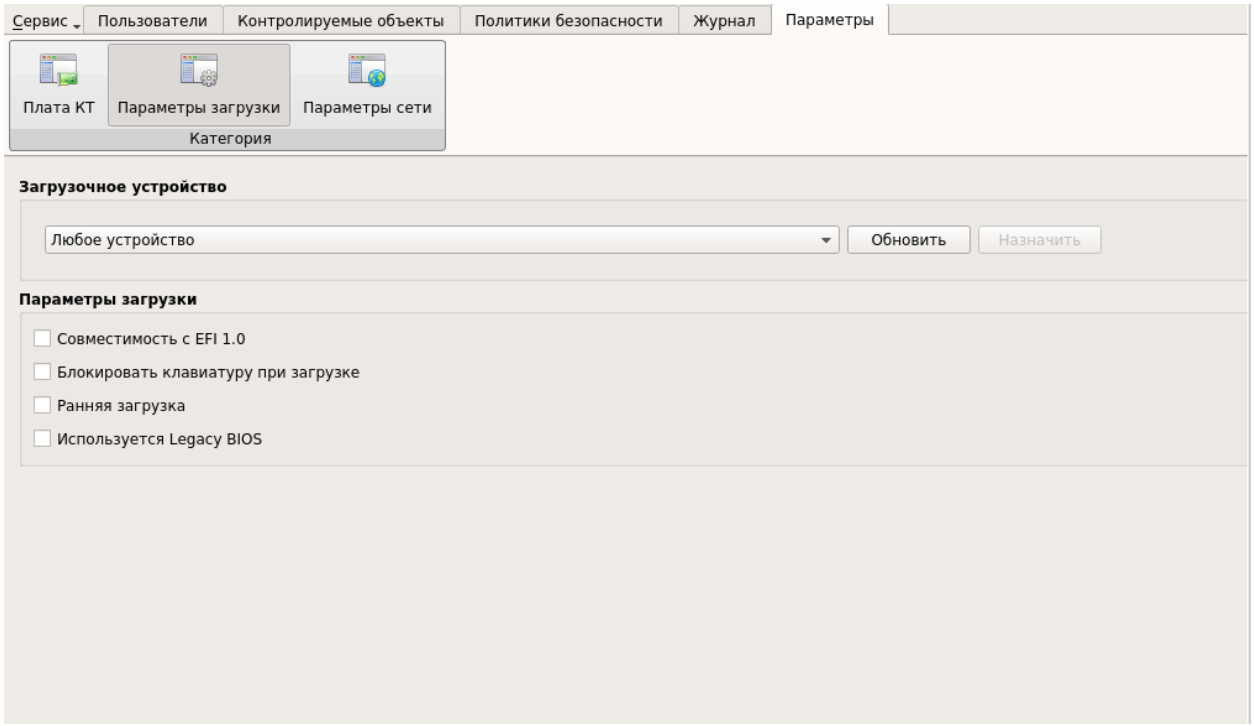

Рисунок 53 – Главное окно. Параметры загрузки

Категория «Параметры загрузки»:

– «Загрузочное устройство» – необходимо выбрать из выпадающего списка конкретное загрузочное устройство, с которого будет возможна загрузка ШОС, после чего нажать кнопку «Назначить». Возможно установить пункт «Любое устройство», в таком случае загрузка ШОС будет возможна с произвольного устройства;

– «Параметры загрузки» – поле настройки параметров загрузки содержит чекбоксы:

- «Совместимость с EFI 1.0» - устанавливается, если СДЗ Dallas Lock некорректно работает с UEFI-совместимой материнской платой и ШОС, установленной в режиме UEFI-загрузки. По умолчанию – отключен.
- «Блокировать клавиатуру при загрузке» - устанавливается для блокировки клавиатуры в EFI-совместимых материнских платах при выборе в Boot Menu (меню загрузки) устройства, с которого требуется загрузить компьютер. По умолчанию – отключен.
- «Ранняя загрузка» - устанавливается, если СДЗ Dallas Lock некорректно работает с UEFI-совместимой материнской платой и ШОС, установленной в режиме UEFI-загрузки. По умолчанию - включен.
- «Используется Legacy BIOS» - устанавливается для работы с включенным CSM режимом (невозможно отключить) в UEFI-совместимых материнских платах с ШОС, установленной в режиме Legacy-загрузки. По умолчанию – отключен.

  Примечание. При режиме загрузки платы «UEFI в режиме совместимости» (см. п.п. 2.3.6.2) чекбокс должен быть выключен.

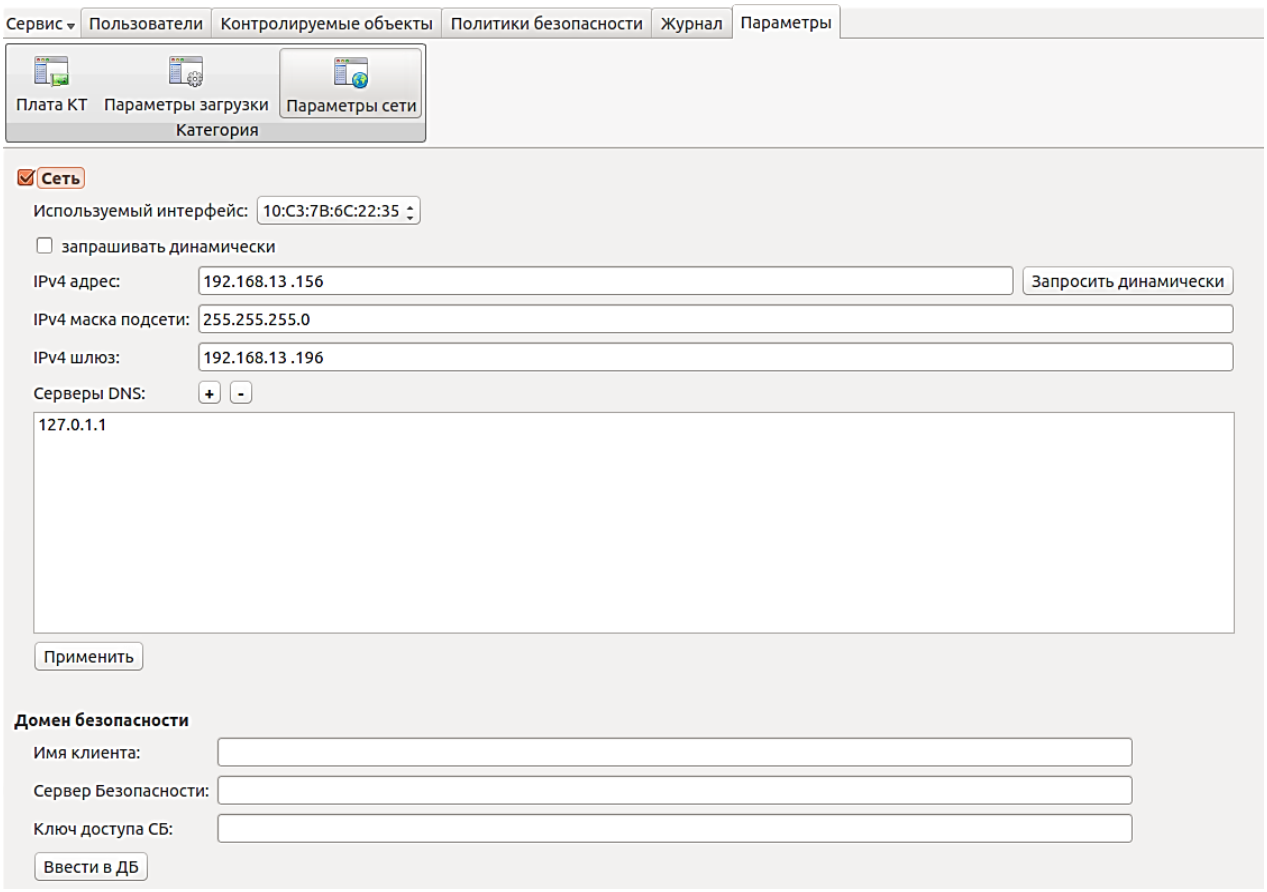

Рисунок 54 – Главное окно. Параметры сети

Категория «Параметры сети»:

– «Сеть» – чекбокс для включения сети. Содержит сетевые параметры необходимые для удаленного администрирования с КСБ. Для настройки требуется заполнить следующие поля:

- «Используемый интерфейс» - из выпадающего списка необходимо выбрать мак-адрес нужного сетевого адаптера;
- чекбокс «запрашивать динамически» - при установленном чекбоксе во время запуска оболочки функций безопасности сетевые параметры автоматически назначаются DHCP-сервером;
- «IPv4 адрес», «IPv4 маска подсети», «IPv4 шлюз», «Серверы DNS» - сетевые параметры компьютера, которые можно заполнить вручную или автоматически, нажав кнопку «Запросить динамически». Также для сервера DNS доступны управляющие кнопки «+» и «-», которые позволяют добавлять и удалять DNS сервера;

После окончания настройки необходимо нажать кнопку «Применить».

– «Домен безопасности» – для централизованного и оперативного управления клиентами они должны быть введены в Домен безопасности. Для ввода СДЗ клиента в Домен

безопасности необходимо заполнить следующие поля:

- «Имя клиента» - необходимо ввести имя клиента, которое будет отображаться в дереве КСБ;
- «Сервер безопасности» - необходимо ввести имя компьютера в сети или IP-адрес, на котором установлен СБ;
- «Ключ доступа СБ» - необходимо ввести ключ удаленного доступа к СБ. По умолчанию ключ доступа – пустой.

После нажатия кнопки «Ввести в ДБ» клиент СДЗ будет введен в Домен безопасности, появится сообщение об успешном вводе клиента (Рисунок 55). Для завершения операции и перезагрузки клиента СДЗ необходимо нажать кнопку «ОК».

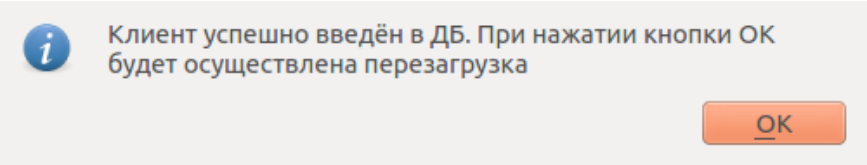

Рисунок 55 – Информационное сообщение

В дереве объектов КСБ появятся новый клиент СДЗ. После чего в категории «Параметры сети» будет доступна только кнопка «Вывести из ДБ» (Рисунок 56).

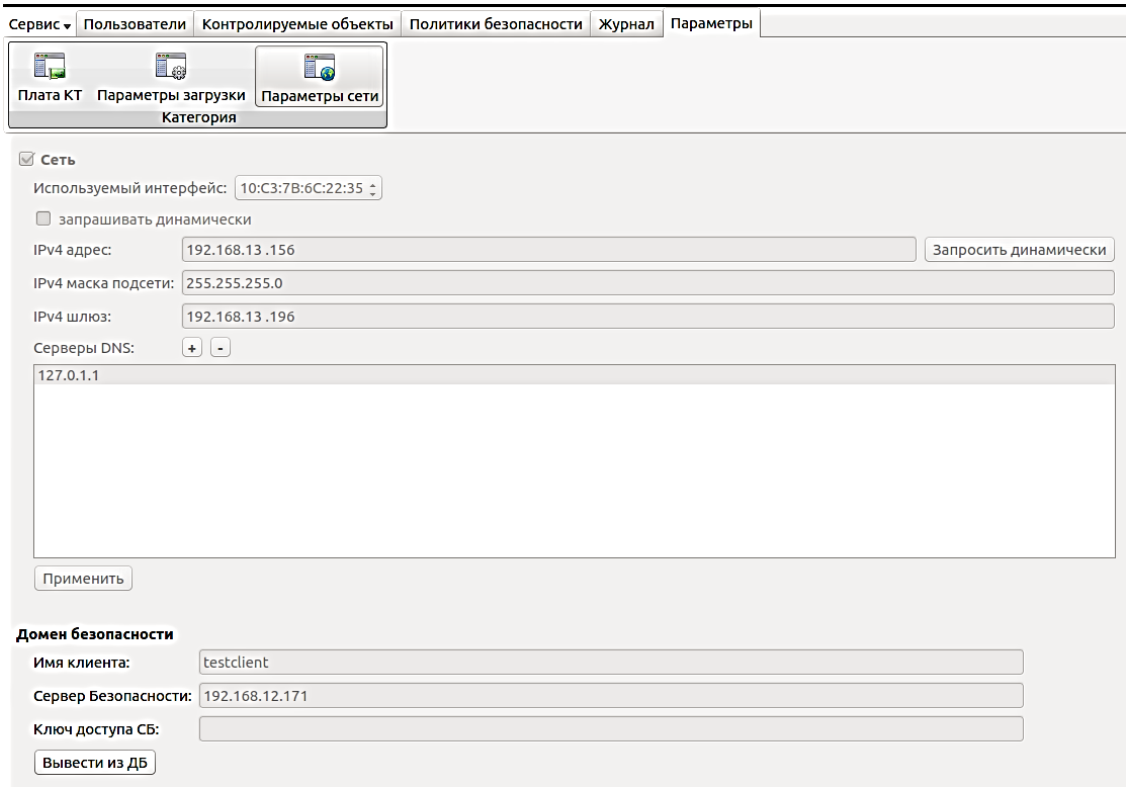

Рисунок 56 – Главное окно. Параметры сети

2.3.3.6 Дополнительные функции СДЗ Dallas Lock.

Меню «Сервис» позволяет получить доступ к дополнительным функциям СДЗ Dallas Lock (Рисунок 57):

– «Конфигурация». 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;
  - «По умолчанию» - восстановление конфигурации СДЗ Dallas Lock по умолчанию.

– «Отчет…» - сохранение отчета о конфигурации СДЗ Dallas Lock в формате *.txt на различные носители информации. Функция сохранения отчета о конфигурации СДЗ Dallas Lock может использоваться для дальнейшей проверки соответствия этих настроек эталонным значениям. 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.

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

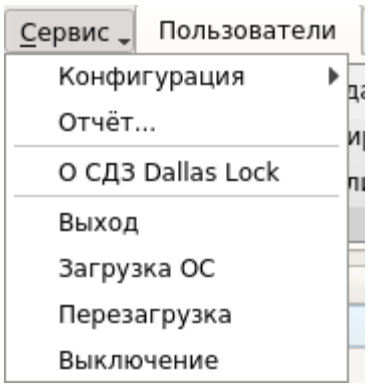

Рисунок 57 – Главное окно. Меню «Сервис»

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

2.3.4 Выключение/перезагрузка ЭВМ

В меню «Сервис» также сгруппированы функциональные кнопки, отвечающие за соответствующие процедуры управления ЭВМ (Рисунок 57):

– «Выход» – осуществляется выход текущей учетной записи пользователя из оболочки администратора и переход к окну авторизации пользователя в СДЗ Dallas Lock;

– «Загрузка ОС» – осуществляется переход к загрузке штатной операционной системы;

– «Перезагрузка» – осуществляется перезагрузка ЭВМ;

– «Выключение» – осуществляется выключение ЭВМ.

2.3.5 Порядок выполнения контроля работоспособности изделия

Контроль работоспособности изделия осуществляется в ходе проведения приемо-сдаточных испытаний в объеме, предусмотренном в документе «Технические условия» (ПФНА.501410.003 ТУ).

В ходе эксплуатации СДЗ Dallas Lock контроль работоспособности осуществляется встроенными в прошивку средствами самодиагностики.

2.3.6 Восстановление заводских настроек (использование сервисной утилиты)

Восстановление изделия к заводским настройкам возможно при помощи сервисной утилиты СДЗ Dallas Lock (Рисунок 58).

Данная утилита позволяет:

– посмотреть информацию о плате;

– применить/обновить прошивку;

– вернуть настройки платы в исходное состояние;

– сменить режим загрузки.

При неисправности аппаратной составляющей изделия - утилита не предназначена для устранения неисправностей такого вида и не может быть использована. В этом случае необходимо обратиться к поставщику изделия.

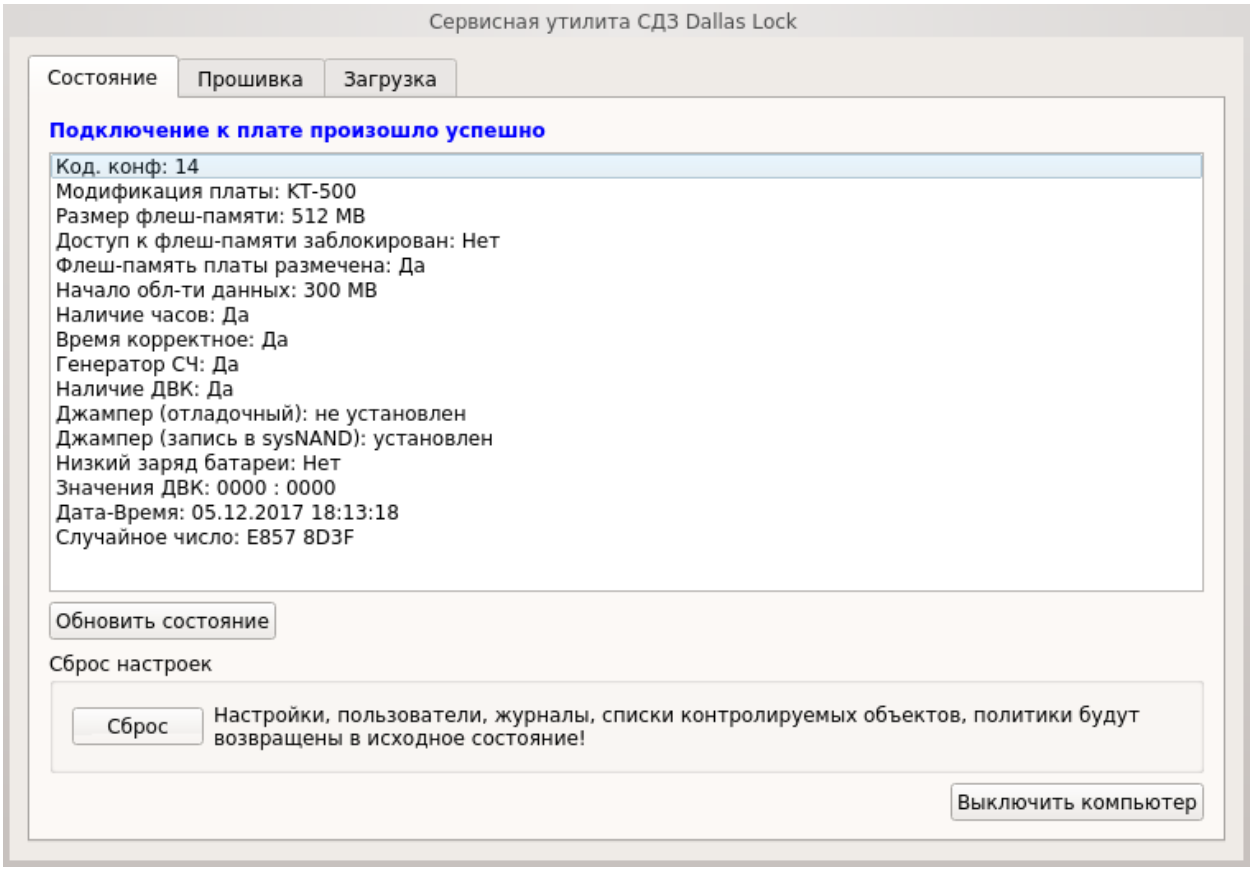

Рисунок 58 – Сервисная утилита

2.3.6.1 Запуск сервисной утилиты KtService

Для запуска сервисной утилиты необходимо:

– поставляемый файл-образ «KtService.img» записать на флеш-накопитель, что сделает его загрузочным (для записи файла-образа на флеш-накопитель, например, из среды Linux использовать следующую команду: **sudo dd if=KtService.img of=/dev/sdb**, где **/dev/sdb** – требуемый накопитель);

– на плате формата PCIe «КТ-500» установить оба джампера на контакты «3» и «5» (Рисунок 1). На платах формата miniPCIe-HalfSize «КТ-521» и M.2 «КТ-550» установить микропереключатели «2» и «3» в положение «ON» (Рисунок 2 и 3);

> **Примечание.** Следует обратить внимание, что необходимо всегда включать\отключать оба джампера или микропереключателя.

– установить плату СДЗ Dallas Lock в системную плату ЭВМ в свободный слот PCI-express / mini PCI-express / M.2;

– выполнить загрузку с флеш-накопителя с записанным ранее файл-образом. Сервисная утилита запустится автоматически.

2.3.6.2 Интерфейс сервисной утилиты

Вкладка «Состояние»:

– таблица с выводом основной информации о подключённой к компьютеру плате: модификация платы, размер флеш-памяти платы, наличие и состояние аппаратных средств, состояние джамперов и т. д.;

– «Обновить состояние» - происходит обновление таблицы;

– «Сброс» - при нажатии все настройки СДЗ будут сброшены в исходное состояние, журналы очищены;

– «Выключить компьютер» - при нажатии происходит выключение компьютера.

Вкладка «Прошивка» (Рисунок 59):

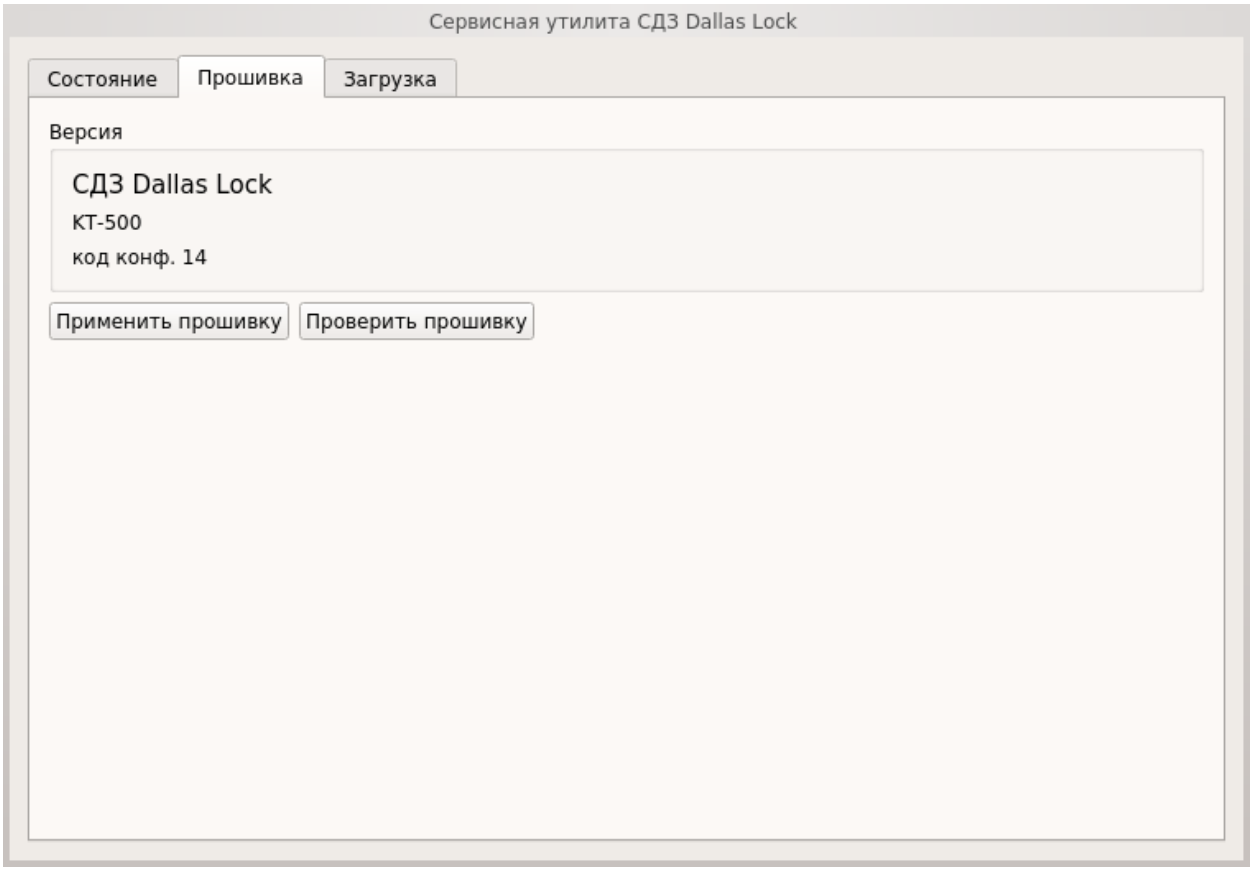

Рисунок 59 – Сервисная утилита. Вкладка «Прошивка»

Доступны следующие кнопки:

– «Применить прошивку» - при нажатии появится диалог выбора файла прошивки платы. Требуется выбрать файл с расширением .amfrm. Далее необходимо будет выбрать один из вариантов возможной прошивки и подтвердить установку, после чего она будет применена (подробное описание процедуры обновления описано в п. 2.3.9);

– «Проверить прошивку» - при нажатии появится диалог выбора файла прошивки

платы. Далее необходимо будет выбрать файл прошивки, после чего будет выведена информация о соответствии или не соответствии прошивки.

Вкладка «Загрузка» (Рисунок 60):

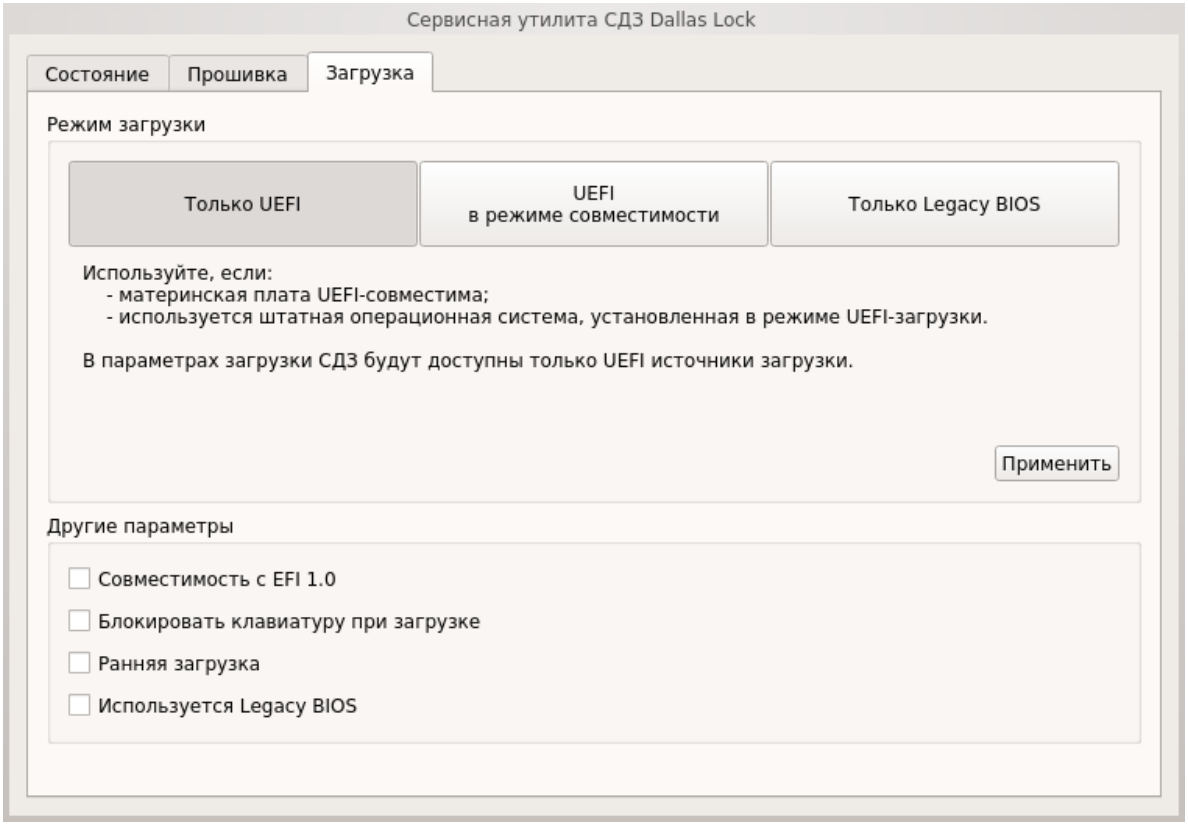

Рисунок 60 – Сервисная утилита. Вкладка «Загрузка»

Доступны следующие режимы загрузки с кратким описанием:

– «Только UEFI»;

– «UEFI в режиме совместимости»;

– «Только Legacy BIOS».

После выбора необходимого режима для сохранения нажать кнопку «Применить».

Другие параметры загрузки содержат чекбоксы:

– «Совместимость с EFI 1.0» - устанавливается, если СДЗ Dallas Lock некорректно работает с UEFI-совместимой материнской платой и ШОС, установленной в режиме UEFI-загрузки. По умолчанию – отключен.

– «Блокировать клавиатуру при загрузке» - устанавливается для блокировки клавиатуры в EFI-совместимых материнских платах при выборе в Boot Menu (меню загрузки) устройства, с которого требуется загрузить компьютер. По умолчанию – отключен.

– «Ранняя загрузка» - устанавливается, если СДЗ Dallas Lock некорректно работает с UEFI-совместимой материнской платой и ШОС, установленной в режиме UEFI-загрузки. По умолчанию - включен.

– «Используется Legacy BIOS» - устанавливается для работы с включенным CSM режимом (невозможно отключить) в UEFI-совместимых материнских платах с ШОС, установленной в режиме Legacy-загрузки. По умолчанию – отключен.

2.3.7 Перечень возможных неисправностей в процессе использования изделия

В ходе использования СДЗ Dallas Lock возможны неисправности, вызванные конфликтом программного обеспечения ЭВМ и прошивки СДЗ Dallas Lock, и неисправности, обусловленные условиями эксплуатации ЭВМ, не соответствующими эксплуатационной документации.

2.3.8 Порядок выключения изделия

Выключение изделия осуществляется автоматически при прекращении подачи питания на системную плату ЭВМ.

Извлечение СДЗ Dallas Lock из системной платы осуществлять только при выключенном питании ЭВМ.

При извлечении СДЗ Dallas Lock, а также при техническом обслуживании ЭВМ избегать возможных повреждений элементов, выступающих над поверхностью печатной платы изделия.

2.3.9 Порядок обновления изделия

Обновление программной части изделия доступно через сервисную утилиту «KtService» на вкладке «Прошивка» (п.п. 2.3.6.2) и осуществляется 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[1] и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте предприятия-изготовителя;

– для установки обновления необходимо запустить сервисную утилиту KtService (порядок запуска подробно описан в п.п. 2.3.6.1);

– перейти на вкладку «Прошивка», выбрать действие «Применить прошивку»,

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

после чего выбрать скачанный файл прошивки с расширением .amfrm, подтвердить применение прошивки;

– выбрать среду исполнения файла прошивки: для компьютеров DEPO выбрать – «1», для остальных моделей, а также для компьютеров DEPO до 280-й модели включительно – «2», подтвердить установку, после чего она будет применена;

– на вкладке «Загрузка» выбрать режим работы платы СДЗ Dallas Lock:

- для UEFI-режима (если материнская плата UEFI-совместима и используется ШОС, установленная в режиме UEFI-загрузки): из группы элементов «Режим загрузки» нажать кнопку «Только UEFI», из группы элементов «Другие параметры» установить галочки «Совместимость с EFI 1.0», «Блокировать клавиатуру при загрузке», «Ранняя загрузка» и «Используется Legacy BIOS» при необходимости (см. п.п. 2.3.6.2);
- для Combo-режима (если материнская плата UEFI-совместима, в настройках BIOS включен режим Legacy-совместимости (CSM), используется ШОС, установленная в режиме Legacy-загрузки): из группы элементов «Режим загрузки» нажать кнопку «UEFI в режиме совместимости», из группы элементов «Другие параметры» установить галочки «Совместимость с EFI 1.0», «Блокировать клавиатуру при загрузке» и «Ранняя загрузка» при необходимости (см. п.п. 2.3.6.2);
- для Legacy-режима (если материнская плата не UEFI-совместима и функционирование СДЗ Dallas Lock в других режимах невозможно): из группы элементов «Режим загрузки» нажать кнопку «Только Legacy BIOS».

– нажать кнопку «Применить»;

– на вкладке «Состояние» нажать кнопку «Выключить компьютер»;

– извлечь носители с сервисной утилитой и файлом прошивки из компьютера;

– удалить с платы формата PCIe «КТ-500» джампер с контакта «5», на платах формата miniPCIe-HalfSize «КТ-521» и M.2 «КТ-550» установить микропереключатель «3» в положение «OFF».

3 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ

Техническое обслуживание СДЗ Dallas Lock осуществляется в ходе профилактического обслуживания ЭВМ в соответствии с правилами, применяемыми для компонентов электронно-вычислительной техники.

Техническое обслуживание изделия производить только при отключенном электропитании ЭВМ, в которой он установлен.

При техническом обслуживании ЭВМ избегать возможных повреждений элементов, выступающих над поверхностью печатной платы изделия.

При возникновении неисправностей, вызванных конфликтом программного обеспечения ЭВМ и прошивки СДЗ Dallas Lock, необходимо обновить прошивку СДЗ Dallas Lock до необходимой версии.

Ремонт изделия в случае возникновения неисправностей печатной платы СДЗ Dallas Lock осуществляется только на предприятии-изготовителе.

4 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

При транспортировании и хранении СДЗ Dallas Lock должна обеспечиваться температура от минус 50 до плюс 55 °С и относительная влажность от 10 до 90% при температуре плюс 25 °С.

Транспортирование СДЗ Dallas Lock может производиться любым видом транспорта на любые расстояния при условии защиты упаковки (тары с упаковкой) от прямого воздействия атмосферных осадков, влаги, конденсата, солнечного света.

В транспортных средствах не допускается наличие кислот, щелочей и других химически активных веществ. Также не допускается наличие электрических и магнитных полей, которые могут привести к потере информации в элементах памяти СДЗ Dallas Lock и на магнитных носителях информации.

Изделие должно храниться в складских условиях в упаковке (таре с упаковкой) в условиях, защищающих изделие от воздействия атмосферных осадков, в окружающей среде, свободной от кислот, щелочей и других агрессивных примесей, при температуре окружающего воздуха от плюс 5 °С до плюс 30 °С и относительной влажности до 80%.

В помещениях для хранения не допускается наличие электрических и магнитных полей, которые могут привести к потере информации в элементах памяти СДЗ Dallas Lock.

5 УТИЛИЗАЦИЯ

Утилизация изделия осуществляется в соответствии с правилами, установленными в Российской Федерации, применяемыми для компонентов электронно-вычислительной техники.