УТВЕРЖДЕН
ПФНА.501410.003 РЭ-ЛУ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ

Dallas Lock

(версия изделия 348.1)

Руководство по эксплуатации

ПФНА.501410.003 РЭ

АННОТАЦИЯ

Данное руководство по эксплуатации распространяется на изделие «Средство доверенной загрузки «Dallas Lock» (далее — СДЗ Dallas Lock, СДЗ).

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 работа механизмов СДЗ Dallas Lock;
- раздел 2: сведения, необходимые для установки и эксплуатации изделия, подготовки его к работе;
- раздел 3: описание задач по администрированию изделия, описание пользовательского интерфейса оболочки администратора СДЗ Dallas Lock и функционала, доступного администратору изделия;
- разделы 4–5: сведения о техническом обслуживании, ремонте, хранении и транспортировании изделия.

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ 4

1 ОПИСАНИЕ И НАЗНАЧЕНИЕ 5

1.1 Назначение и технические характеристики 5
1.2 Состав изделия 6
1.3 Устройство и работа 10
1.4 Маркировка и упаковка 11

2 ПОДГОТОВКА ИЗДЕЛИЯ К ИСПОЛЬЗОВАНИЮ 12

2.1 Эксплуатационные ограничения и технические требования 12
2.2 Меры безопасности при подготовке изделия 12
2.3 Предварительная подготовка 12

3 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ 15

3.1 Вход на защищенное ТС 15
3.2 Смена пароля 22
3.3 Администрирование СДЗ Dallas Lock 24
3.3.1 Управление учетными записями пользователей 25
3.3.2 Контроль целостности 35
3.3.3 Настройка авторизации в СДЗ Dallas Lock 41
3.3.4 Регистрация и учёт 45
3.3.5 Управление параметрами платы 49
3.3.6 Дополнительные функции СДЗ Dallas Lock 53
3.4 Выключение/перезагрузка ТС 54
3.5 Удаленная перезагрузка и удаленное выключение клиентов СДЗ 54
3.5.1 Запуск Агента ШОС 55
3.6 Использование сервисной утилиты (восстановление заводских настроек) 58
3.6.1 Запуск сервисной утилиты KtService 59
3.6.2 Интерфейс сервисной утилиты 59
3.7 Порядок обновления изделия 61
3.8 Перечень возможных неисправностей в процессе использования 62
3.9 Порядок выполнения контроля работоспособности изделия 62
3.10 Порядок выключения изделия 62

4 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ 64

5 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ 65

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

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

Пользователь — пользователь, не имеющий полномочий на администрирование СДЗ Dallas Lock, но в соответствии с политиками безопасности имеющий возможность выполнения других операций.

АИ	аппаратный идентификатор
ДВК	датчик вскрытия корпуса
ДСЧ	датчик случайных чисел
ЕЦУ	Единый центр управления
КС	контрольная сумма
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
СДЗ	средство доверенной загрузки
СЗИ НСД	средство защиты информации от несанкционированного доступа
ТС	техническое средство
ШОС	штатная операционная система

1 ОПИСАНИЕ И НАЗНАЧЕНИЕ

1.1 Назначение и технические характеристики

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

Обозначение изделия: ПФНА.501410.003.

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

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

Изделие предназначено для использования на персональных компьютерах (в том числе на ноутбуках) и серверах с соответствующими техническими характеристиками.

СДЗ Dallas Lock позволяет контролировать целостность реестра ОС Windows.

СДЗ Dallas Lock поддерживает следующие виды АИ:

- 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 Token ГОСТ);
- USB-ключи и смарт-карты JaCarta (JaCarta ГОСТ, JaCarta SF/ГОСТ, JaCarta-2 PKI/ГОСТ, JaCarta-2 ГОСТ, JaCarta PKI).

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

СДЗ Dallas Lock предназначено для защиты рабочих ТС 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 ТС и (или) состава компонентов аппаратного обеспечения ТС;
- нарушение целостности ПО СДЗ Dallas Lock, обход нарушителем компонентов СДЗ Dallas Lock;
- несанкционированное изменение конфигурации СДЗ Dallas Lock;
- преодоление или обход функций идентификации и аутентификации СДЗ Dallas Lock за счет недостаточного качества аутентификационной информации и (или) недоверенного маршрута между СДЗ Dallas Lock и пользователями;
- получение остаточной информации СДЗ Dallas Lock из памяти ТС после завершения

---

[1] Кроме eToken с памятью 32 Кб.

[2] Рутокен S можно только назначить пользователю, записать данные учетной записи пользователя на него нельзя. Для совместного использования с СДЗ Dallas Lock АИ 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-код администратора>" --so-puk "" --pin "<ПИН-код пользователя>"
$ pkcs15-init --store-pin --label "<имя АИ>" --auth-id 02 --pin "<ПИН-код пользователя>" --puk ""
```

[3] При подключении считывателя Touch Memory непосредственно к СДЗ Dallas Lock 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 ТС USB-считывателя Touch Memory и до перезагрузки ТС.

работы СДЗ Dallas Lock;
- получение доступа к ресурсам СДЗ Dallas Lock из программной среды ТС после завершения работы СДЗ Dallas Lock;
- сбои и ошибки в процессе функционирования СДЗ Dallas Lock.

СДЗ Dallas Lock может работать в одном из двух режимов работы, выбираемых при первом запуске продукта:

- «Базовый режим работы»;
- «Усиленный режим работы»[1].

В базовом режиме работы доступны гибкие настройки политик авторизации пользователей, работа с локальными и доменными учетными записями пользователей, локальное и удаленное управление платой СДЗ.

В усиленном режиме работы устанавливается принудительная двухфакторная идентификация для всех учетных записей пользователей, возможна работа только с локальными учетными записями пользователей и локальное управление платой СДЗ.

Выбранный режим работы СДЗ Dallas Lock возможно изменить только с помощью утилиты KtService (подробнее в разделе «Использование сервисной утилиты (восстановление заводских настроек)».

СДЗ Dallas Lock реализует следующие функции безопасности:

- разграничение доступа к управлению СДЗ Dallas Lock;
- управление работой СДЗ Dallas Lock;
- управление параметрами СДЗ Dallas Lock;
- аудит безопасности СДЗ Dallas Lock;
- идентификация и аутентификация пользователей;
- тестирование СДЗ Dallas Lock, контроль целостности ПО и параметров СДЗ Dallas Lock;
- контроль компонентов ТС;
- блокирование загрузки ОС средствами доверенной загрузки;
- сигнализация СДЗ;
- обеспечение безопасности при возникновении сбоев и ошибок в процессе работы;
- обеспечение безопасности после завершения работы СДЗ Dallas Lock.

1.2 Состав изделия

СДЗ Dallas Lock состоит из аппаратной части и прошивки (программной части).

Аппаратная часть СДЗ Dallas Lock представляет собой один из следующих вариантов печатных плат:

- PCIe «КТ-500» (ПФНА.501410.003-01) (рис. 1);
- miniPCIe-HalfSize «КТ-521» (ПФНА.501410.003-02) (рис. 2);
- M.2 «КТ-550» (ПФНА.501410.003-04) (рис. 3);
- PCIe «КТ-500 r3» (ПФНА.501410.003-09) (рис. 4);
- miniPCIe-HalfSize «КТ-521 r3» (ПФНА.501410.003-10) (рис. 5);
- M.2 «КТ-550 r3» (ПФНА.501410.003-11) (рис. 6).

[1] Не является обязательным. Представляет собой возможность автоматизированного приведения настроек к усиленным значениям для систем с повышенными требованиями к безопасности.

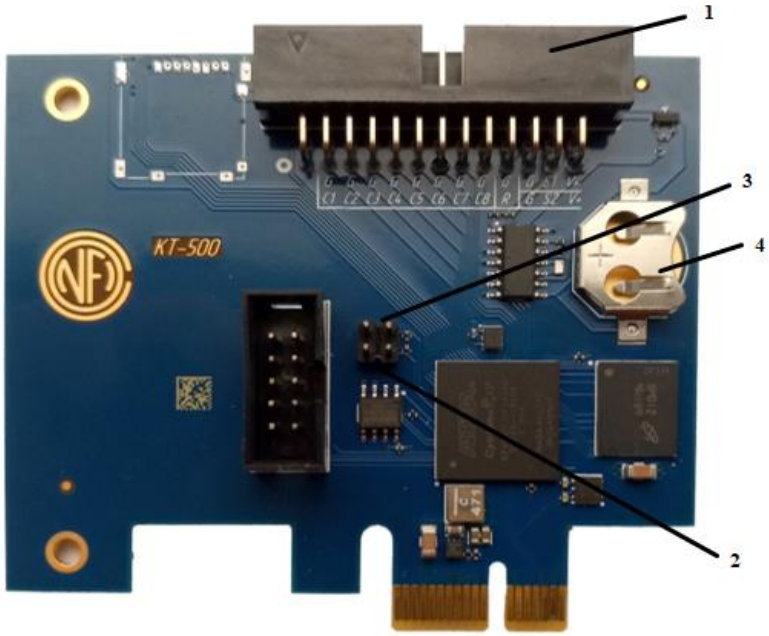


Рис. 1. Плата «КТ-500» и расположение ее основных элементов

1 — Группа штыревых разъемов для подключения ДВК, цепи системного сброса, считывателя Touch Memory (или кабеля для подключения считывателя Touch Memory через разъем RJ11 ПФНА.501410.003-08).
2 — Контакты под джампер для входа в сервисный режим СДЗ для обновления прошивки платы. При установленном джампере разрешается запись в системную область памяти СДЗ.
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.

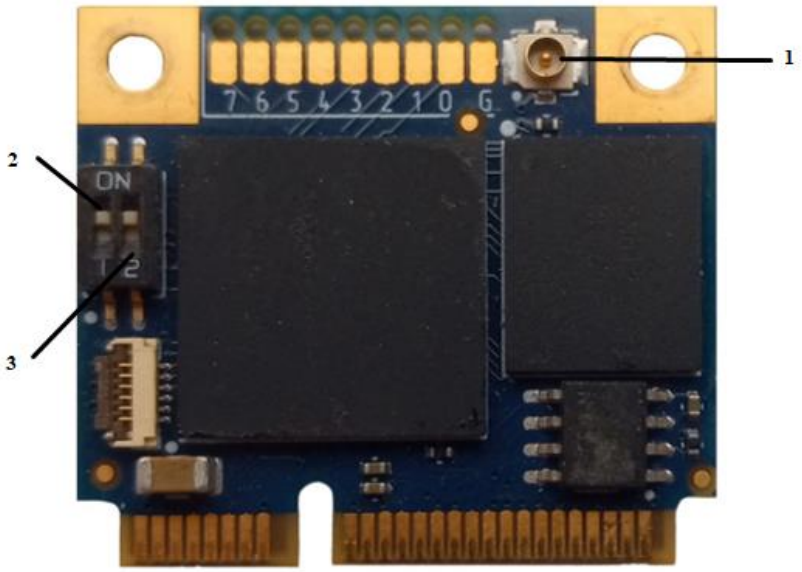


Рис. 2. Плата «КТ-521» и расположение ее основных элементов

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.

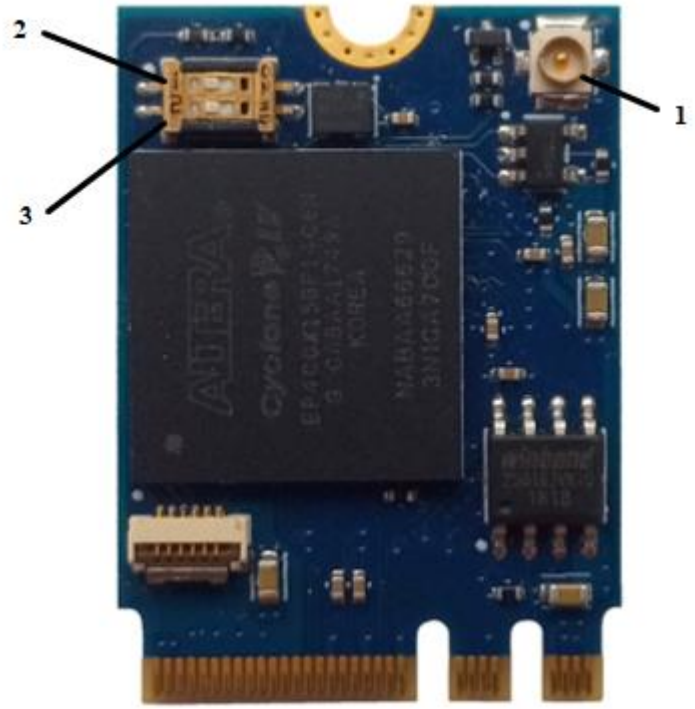


Рис. 3. Плата «КТ-550» и расположение ее основных элементов

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.

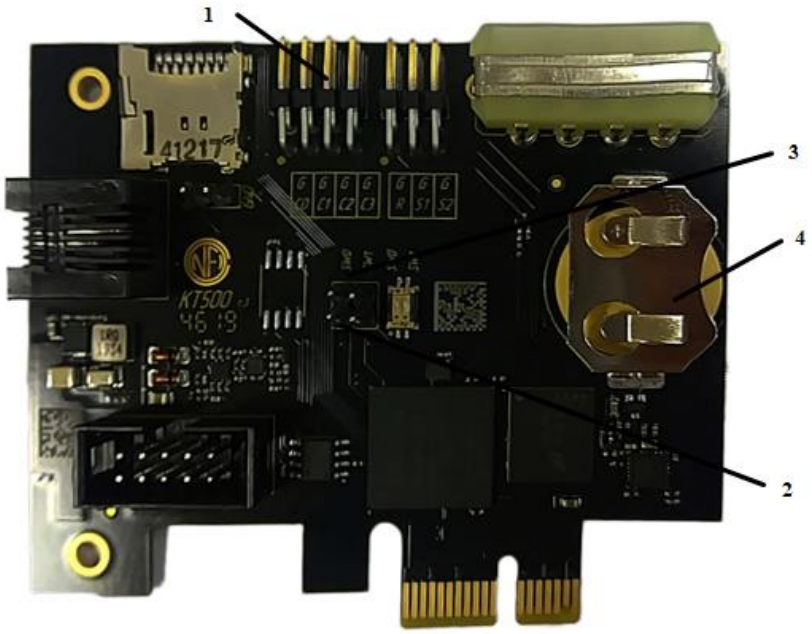


Рис. 4. Плата «КТ-500 r3» и расположение ее основных элементов

1 — Группа штыревых разъемов для подключения ДВК, цепи системного сброса, считывателя Touch Memory (или кабеля для подключения считывателя Touch Memory через разъем RJ11 ПФНА.501410.003-08).
2 — Контакты под джампер для входа в сервисный режим СДЗ для обновления прошивки

платы. При установленном джампере разрешается запись в системную область памяти СДЗ.
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.

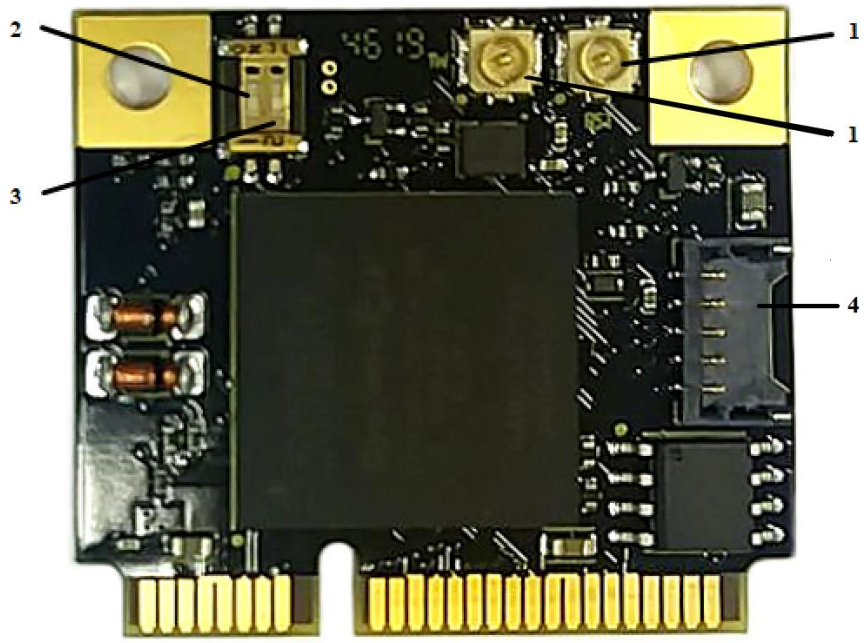


Рис. 5. Плата «КТ-521 r3» и расположение ее основных элементов

1 — Коаксиальные разъемы для подключения «сторожевого таймера» и для подключения считывателя Touch Memory.
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.
4 — Разъем для подключения платы RTC с источником питания, необходимым для работы часов реального времени.

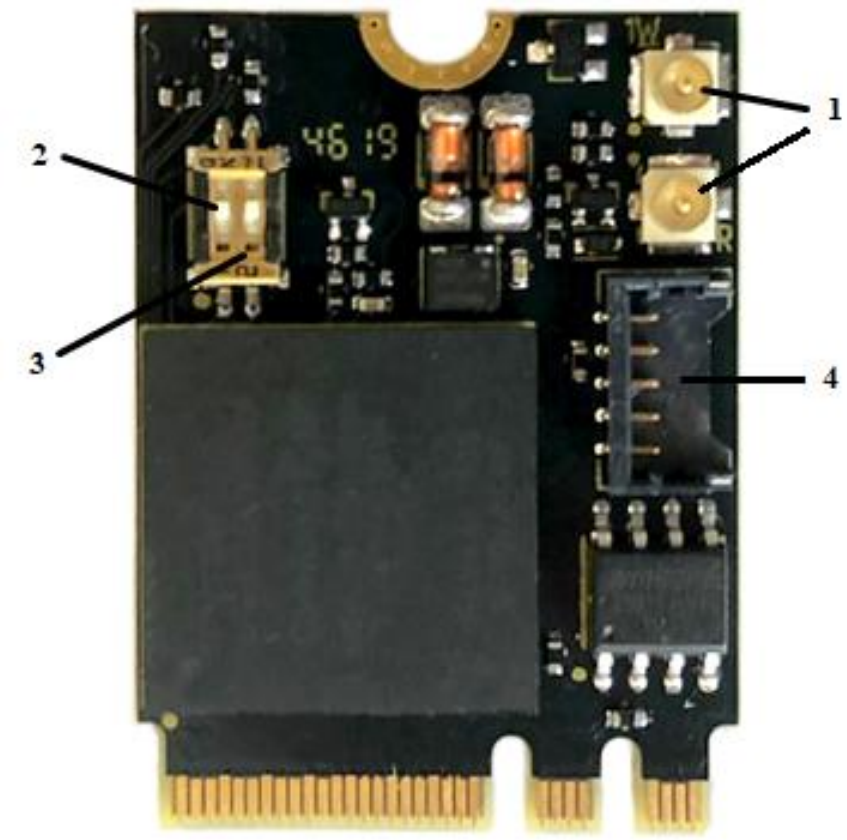


Рис. 6. Плата «КТ-550 r3» и расположение ее основных элементов

1 — Коаксиальные разъемы для подключения «сторожевого таймера» и для подключения считывателя Touch Memory.
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.
4 — Разъем для подключения платы RTC с источником питания, необходимым для работы часов реального времени.

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

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

1.3 Устройство и работа

При включении/перезагрузке ТС 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 ТС.

Оболочка функций безопасности СДЗ Dallas Lock отображает окно авторизации.

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

1.4 Маркировка и упаковка

Маркировка СДЗ Dallas Lock содержит:

- товарный знак предприятия-изготовителя;
- заводской (учетный) порядковый номер изделия;
- год, месяц, число упаковки (указаны в разделе 5 «Свидетельство об упаковывании и приемке» в поле «год, число, месяц» печатной копии Формуляра ПФНА.501410.003 ФО, поставляемого в составе комплекта СДЗ Dallas Lock);
- идентификатор СЗИ (вклеен в раздел 5 «Свидетельство об упаковывании и приемке» в поле «Маркирован идентификатором» печатной копии Формуляра ПФНА.501410.003 ФО, поставляемого в составе комплекта СДЗ Dallas Lock);
- соответствующие подписи и печати.

Маркировка наносится на печатную плату СДЗ Dallas Lock, упаковку изделия и в печатную копию Формуляра ПФНА.501410.003 ФО.

Надписи при маркировке выполняются одним из следующих способов:

- рукописным — основным чертежным шрифтом (черного цвета высотой не менее 1,6 мм по ГОСТ 2.304);
- с применением печатающих устройств (высотой 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 ПОДГОТОВКА ИЗДЕЛИЯ К ИСПОЛЬЗОВАНИЮ

2.1 Эксплуатационные ограничения и технические требования

СДЗ Dallas Lock исправно работает на ТС (персональные и портативные компьютеры, серверы) архитектуры Intel x64. Минимальные аппаратные требования к ТС 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 АИ (за исключением случаев, когда в качестве АИ используются электронные ключи Touch Memory, а считыватель Touch Memory подключен непосредственно к платам формата PCIe «КТ-500» и «КТ-500 r3», либо формата Mini PCI-express «КТ-521 r3», либо формата M.2 «КТ-550 r3»);
- клавиатура, мышь или совместимое указывающее устройство;
- видеоадаптер и монитор, поддерживающие режим Super VGA с разрешением не менее чем 800x600 точек.

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

Реализована поддержка наиболее распространенных файловых систем, включая FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3, VMFS5, XFS на LVM.

2.2 Меры безопасности при подготовке изделия

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

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

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

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

2.3 Предварительная подготовка

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:

1. 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.

2. 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).

3. 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. «Запуск сервисной утилиты KtService»).

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 и необходимо отключить загрузку через сетевую карту PXE Option ROM.

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

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

В СДЗ Dallas Lock реализован беспроводной (программный) «сторожевой таймер».

Также при наличии разъемов «Reset» или «Power» рекомендуется подключать ***аппаратный «сторожевой таймер»*** изделия к ТС с помощью поставляемого:

- кабеля ПФНА.501410.003-05 для плат «КТ-500» и «КТ-500 r3» (на плате кабель подключается к штыревым разъемам «R» и «G» (рис. 7), на ТС — к разъему «Reset» («Power»));
- кабеля ПФНА.501410.003-06 для плат «КТ-521», «КТ-550», «КТ-521 r3» и «КТ-550 r3» (на платах кабель подключается к коаксиальному разъему (рис. 2, рис. 3, рис. 5 и рис. 6 соответственно), на ТС — к разъему «Reset» («Power»)).

Примечание. Если ТС при включении уходит в перезагрузку или выключается (в зависимости от того, к какому разъему кабель «сторожевого таймера» подключен со стороны ТС), то кабель подключен неверно. Полярность подключения двухконтактного разъема кабеля не соблюдена.

Для подключения ***ДВК***:

- на платах «КТ-500» используются штыревые разъемы «V+», «S1» и «S2» (рис. 7);
- на платах «КТ-500 r3» используются штыревые разъемы «G», «S1» и «S2» (рис. 7);
- на платах «КТ-521 r3» и «КТ-550 r3» необходимо подключить плату RTC (плата часов реального времени)[1] с помощью кабеля (п. 4 на рис. 5, рис. 6), после подключить к ней ДВК.

Внимание! Для корректной работы ДВК и «сторожевого таймера» на платах формата miniPCIe-HS «КТ-521 r3» и M.2 «КТ-550 r3» следует подключать плату RTC обязательно с рабочим источником питания, который необходим для работы часов.

Для подключения ***считывателя Touch Memory***:

- на платах «КТ-500» и «КТ-500 r3» используются штыревые разъемы «C1», «C2» и «G» (подключение возможно в том числе через Кабель ПФНА.501410.003-08) (рис. 7);
- на платах «КТ-521 r3» и «КТ-550 r3» используется коаксиальный разъем (п.1 на рис. 5, рис. 6).

[1] Поставляется только для плат формата miniPCIe-HS «КТ-521 r3» и M.2 «КТ-550 r3», наличие определяется договором.

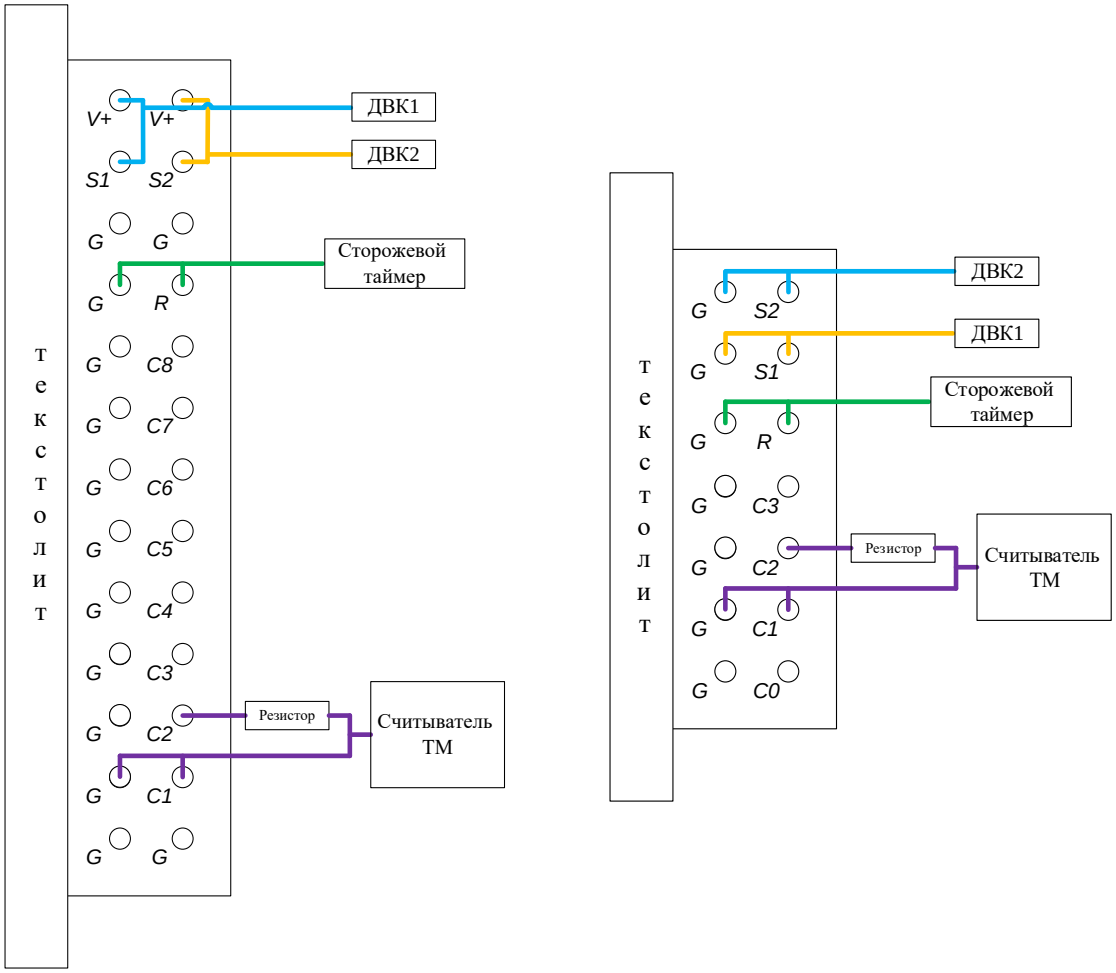


Рис. 7. Схема подключения ДВК, сторожевого таймера и считывателя Touch Memory к штыревым разъемам на платах «КТ-500» и «КТ-500 r3» соответственно

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

Примечание. Необходима установка драйвера платы КТ, расположенного на идущем в комплекте с СДЗ Dallas Lock диске, в случае:

- работы функции автовхода по авторизационным данным из СДЗ Dallas Lock в ШОС, защищенную средством защиты информации от несанкционированного доступа Dallas Lock 8.0 (далее — СЗИ НСД, СЗИ НСД Dallas Lock 8.0);
- работы службы Агент ШОС (см. «Запуск Агента ШОС»);
- использования часов плат «КТ-500», «КТ-500 r3», «КТ-521 r3» и «КТ-550 r3» при регистрации времени событий в журналах СЗИ НСД Dallas Lock 8.0.

3 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

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 Руководстве оператора ПФНА.501410.003 34.

3.1 Вход на защищенное ТС

При первом включении ТС с установленной платой СДЗ Dallas Lock производится предварительная настройка СДЗ (первичная инициализация), во время которой администратором СДЗ устанавливается режим работы изделия (рис. 8).

Рис. 8. Выбор режима работы СДЗ Dallas Lock

При выборе базового режима появляется окно регистрации учётной записи администратора СДЗ Dallas Lock (рис. 9), в котором необходимо обязательно указать имя пользователя и задать пароль к его учётной записи. После успешной регистрации учётных данных производится перезагрузка ТС.

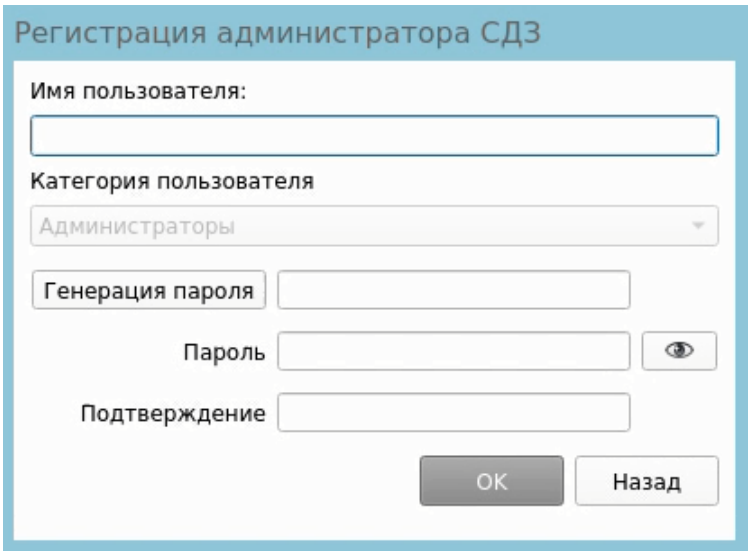


Рис. 9. Регистрация администратора СДЗ Dallas Lock

При выборе усиленного режима появляется окно регистрации учётной записи администратора СДЗ Dallas Lock, в котором необходимо выбрать тип регистрации:

1. Первичная регистрация (рис. 10), во время которой в аппаратный идентификатор записывается новая служебная информация, содержимое аппаратного идентификатора перезаписывается полностью. Необходимо обязательно указать имя администратора, задать и подтвердить пароль к его учётной записи, выбрать аппаратный идентификатор.

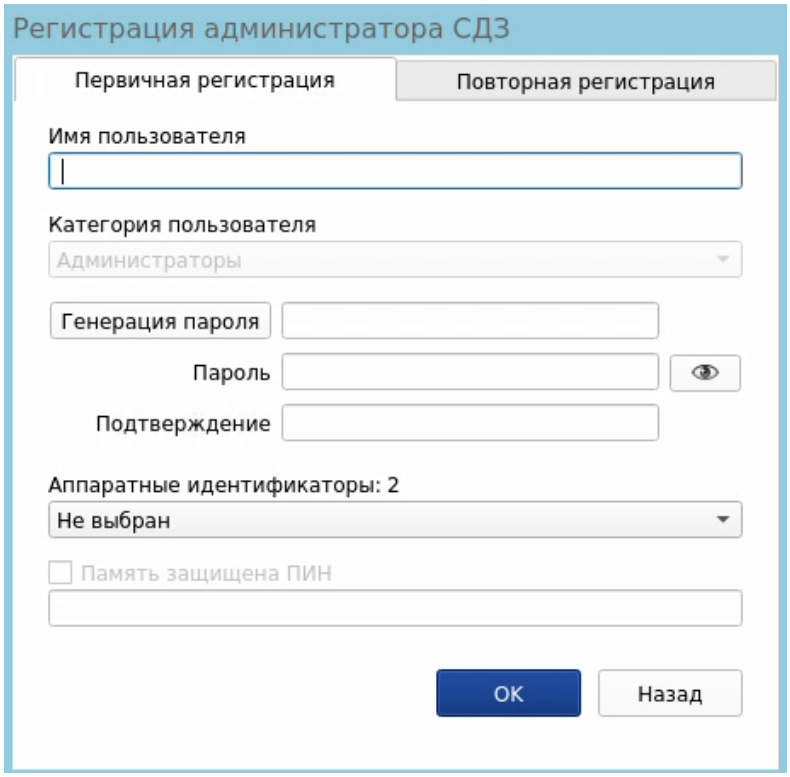


Рис. 10. Первичная регистрация администратора СДЗ Dallas Lock

2. Повторная регистрация (рис. 11), во время которой служебная информация, записанная в аппаратный идентификатор при первичной регистрации учетной записи пользователя, считывается из аппаратного идентификатора. В этом случае пользователь может использовать один и тот же аппаратный идентификатор для входа в систему на нескольких компьютерах, защищенных СДЗ Dallas Lock, работающих в усиленном режиме. Необходимо ввести имя администратора и пароль к его учётной записи, выбрать аппаратный идентификатор.

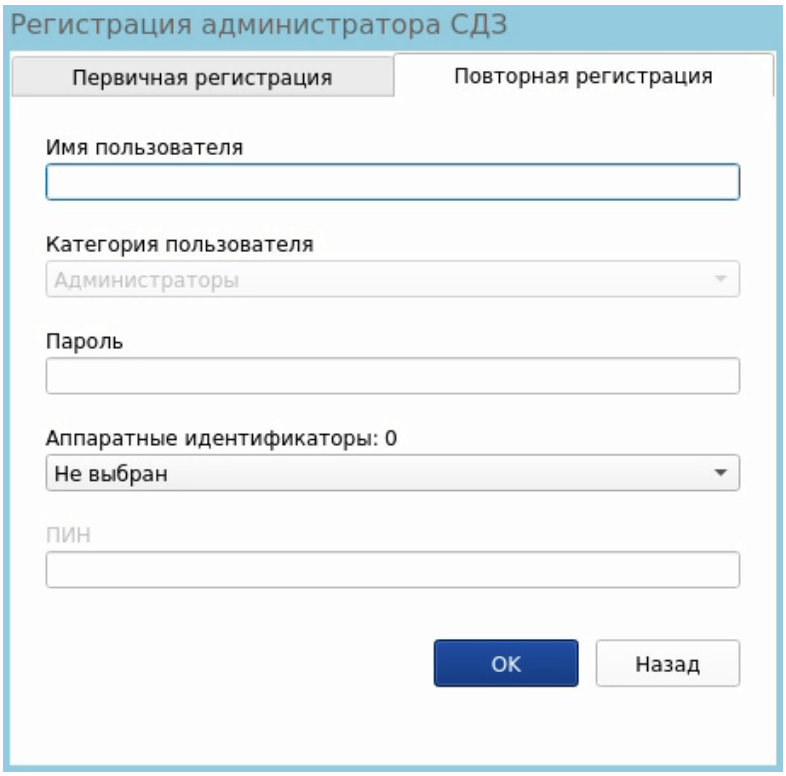


Рис. 11. Повторная регистрация администратора СДЗ Dallas Lock

Выбранный режим работы СДЗ вступает в силу после перезагрузки системы, производящейся после успешной регистрации учетной записи администратора.

После прохождения процедуры первичной инициализации при загрузке компьютера с установленной платой СДЗ Dallas Lock появляется экран приглашения на вход в систему (рис. 12).

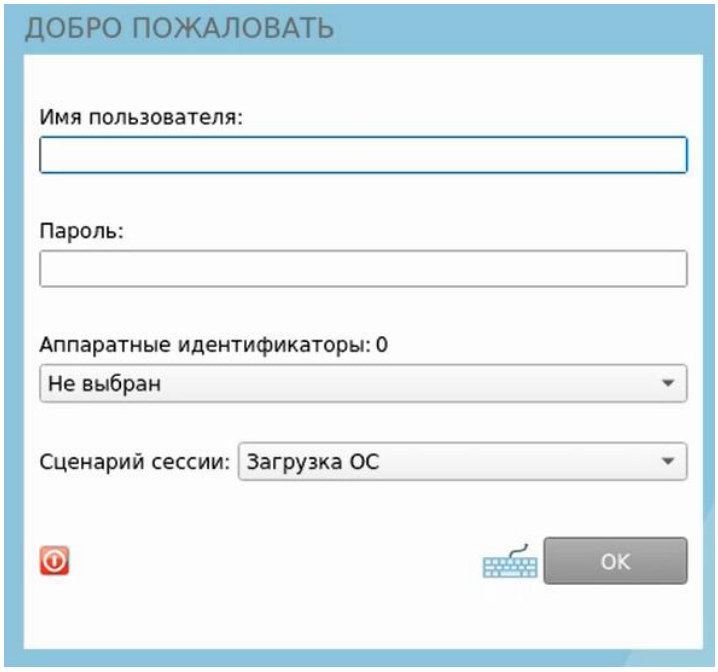


Рис. 12. Экран приглашения на вход в систему

Примечание. Если защищенный СДЗ Dallas Lock компьютер введен в ДБ, в левом нижнем углу экрана приглашения на вход, рядом со значком выведено соответствующее сообщение:

- «Соединение с СБ установлено»;
- «Соединение с СБ не установлено».

Для входа на защищенный СДЗ Dallas Lock компьютер необходимо:

1. Предъявить АИ, если он назначен учетной записи пользователя, а именно:
   - вставить его в USB-порт или прикоснуться к считывателю (в зависимости от типа устройства);
   - выбрать наименование АИ, которое появится в выпадающем меню «аппаратные идентификаторы».

Процедура авторизации с использованием АИ возможна одним из следующих способов:

- Если АИ сопоставлен учетной записи пользователя, то для авторизации необходимо предъявить АИ, ввести имя пользователя и пароль. В таком случае происходит проверка соответствия предъявленного АИ с введенным именем учетной записи пользователя.

Примечание. В случае предъявления не сопоставленного данной учетной записи пользователя АИ при попытке авторизации будет выведено соответствующее сообщение (рис. 13).

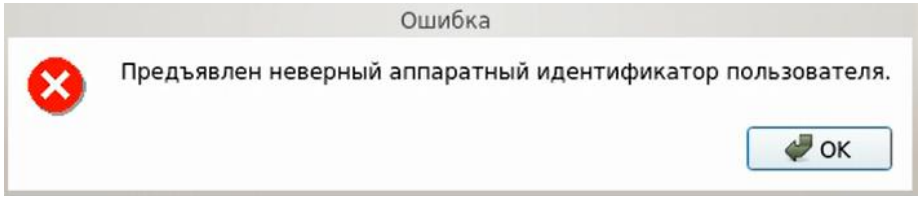


Рис. 13. Окно сообщения при предъявлении неверного АИ

- Если АИ сопоставлен учетной записи пользователя, и в незащищенной памяти АИ

хранится идентификационная информация, то для авторизации необходимо предъявить АИ (при этом в поле «Имя пользователя» будет подставлена хранящаяся в памяти АИ идентификационная информация, поле будет недоступно для редактирования) и ввести пароль учетной записи пользователя.

- Если АИ сопоставлен учетной записи пользователя, и в незащищенной памяти АИ хранится идентификационная и аутентификационная информация, то для авторизации необходимо предъявить АИ (при этом в поля «Имя пользователя» и «Пароль» будет подставлена хранящаяся в памяти АИ идентификационная и аутентификационная информация, поля будут недоступны для редактирования).
- Если АИ сопоставлен учетной записи пользователя и в защищенной ПИН-кодом памяти АИ хранится аутентификационная информация, то для авторизации необходимо предъявить АИ (при этом в поле «Имя пользователя» будет подставлена хранящаяся в памяти АИ идентификационная информация, поле будет недоступно для редактирования) и ввести ПИН-код АИ, при этом пароль будет получен из защищенной памяти АИ, если введен верный ПИН-код.

2. Используя клавиатуру, ввести в поле «Имя пользователя» 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 [dom] — только полное имя домена.

Доменная учетная запись пользователя должна быть предварительно зарегистрирована в СДЗ Dallas Lock.

Использование доменной учетной записи доступно только в базовом режиме функционирования СДЗ.

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 получить 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, чтобы результатом запроса преобразования адреса 192.168.0.1 в имя было dns.dl.local. Таким образом, будет создана возможность авторизовываться пользователям по короткому суффиксу (user@dl) в полном доменном имени (user@dl.local).

3. Ввести пароль. При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ ● (точка). Строчные и прописные буквы в пароле различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля. В базовом режиме дополнительная кнопка  изменит скрытые символы на явные.

Примечание. Авторизация доменной учетной записи пользователя с паролем из русских символов невозможна. Необходимо использовать пароль в английской раскладке.

4. Выбрать в выпадающем списке поля «Сценарий сессии» допустимую для учетной записи пользователя операцию по работе с системой:
   - «Загрузка ОС» — 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»).
5. Нажать клавишу «Enter» или кнопку «ОК» на экранной форме.

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 (рис. 14), осуществляется возврат к окну авторизации.

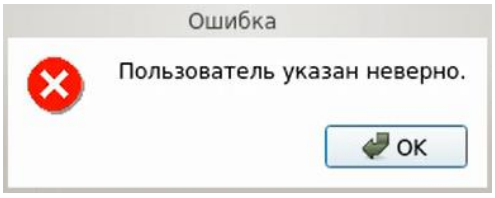


Рис. 14. Окно сообщения при неверном указании имени пользователя

Далее проверяется правильность указанного пользователем пароля. В случае успеха разрешается вход в систему, иначе выводится соответствующее сообщение (рис. 15), осуществляется возврат к окну авторизации.

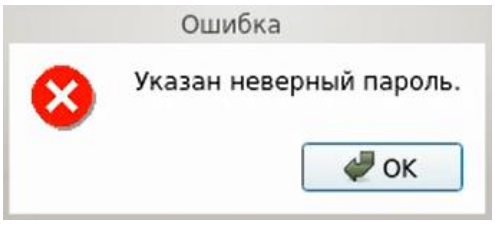


Рис. 15. Окно сообщения при неверном указании пароля учетной записи пользователя

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

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. «Настройка авторизации в СДЗ Dallas Lock») присвоено значение «Не используется». Выводится соответствующее сообщение (рис. 16).

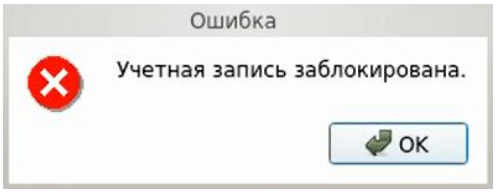


Рис. 16. Окно сообщения блокировки учетной записи пользователя

Если в свойствах учетной записи пользователя администратор установил атрибут «Отключен», при успешной проверке пароля выводится соответствующее сообщение о неактивности учетной записи пользователя (рис. 17). В этом случае включение осуществляется только администратором.

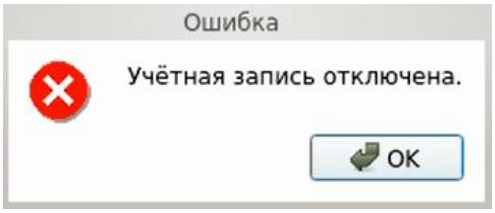


Рис. 17. Окно сообщения при попытке входа отключенного пользователя

После этого происходит проверка аппаратного идентификатора, если он назначен данной учетной записи администратором. Его настройка в свойствах учётной записи находится в отдельной вкладке «Аппаратная идентификация».

В случае если не выбран аппаратный идентификатор, выводится соответствующее сообщение (рис. 18).

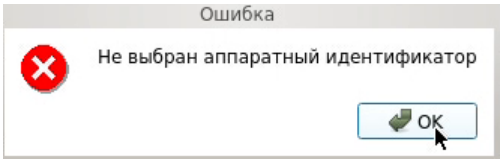


Рис. 18. Окно сообщения при попытке входа с невыбранным аппаратным идентификатором

Если память выбранного аппаратного идентификатора защищена ПИН-кодом, ПИН-код не введен или введен неверно, то выводится диалоговое окно с соответствующей ошибкой (рис. 19), осуществляется возврат к окну авторизации.

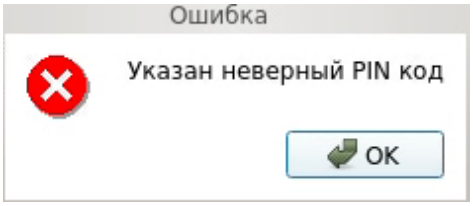


Рис. 19. Окно сообщения при неверном указании ПИН-кода аппаратного идентификатора

Примечание. В усиленном режиме работы происходит обязательная проверка аппаратного идентификатора.

Далее осуществляется проверка допустимого времени работы согласно установленному для учетной записи пользователя расписанию. Если осуществляется попытка авторизации пользователя в неустановленное для него время работы, выводится соответствующее сообщение (рис. 20), осуществляется возврат к окну авторизации.

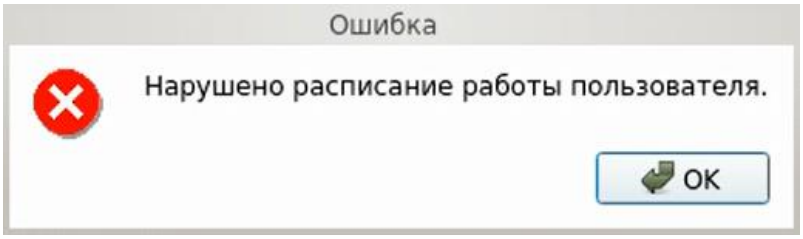


Рис. 20. Окно сообщения при попытке входа в неустановленное время работы

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 (рис. 21).

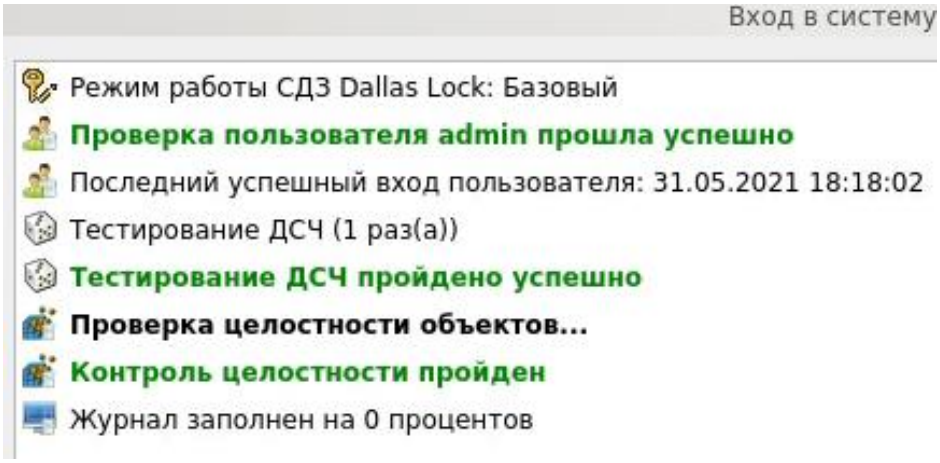


Рис. 21. Пример окна сообщения при успешном прохождении контроля целостности

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

В случае неуспешного прохождения процедуры контроля целостности при входе пользователя, учетной записи которого установлен атрибут «Запретить работу при нарушении целостности» (см. «Управление учетными записями пользователей»), выводится соответствующее сообщение (рис. 22). В окне доступны следующие действия:

- «Выход» — возврат к окну авторизации;
- «Выключить» — отключение ТС.

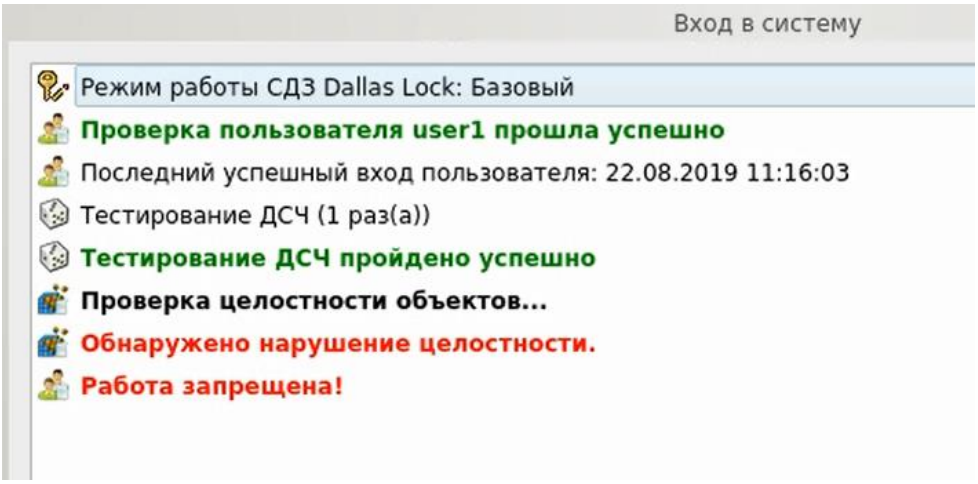


Рис. 22. Пример окна сообщения при неуспешном прохождении контроля целостности при входе непривилегированного пользователя

Если пользователю разрешено работать в системе с нарушенной целостностью контролируемых объектов, осуществляется вывод соответствующего сообщения (рис. 23), и вход в систему продолжается при нажатии кнопки «Далее». Осуществляется работа в соответствии с выбранным действием («Загрузка ОС», «Смена пароля» или «Администрирование»).

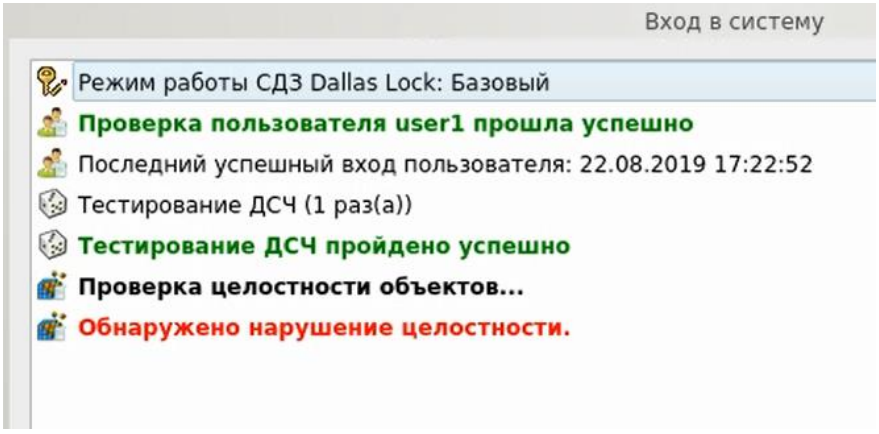


Рис. 23. Пример окна сообщения при неуспешном прохождении контроля целостности при входе пользователя

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, выводится соответствующее сообщение о необходимости изменения пароля (рис. 24) и происходит переход к процедуре смены пароля (см. «Смена пароля»).

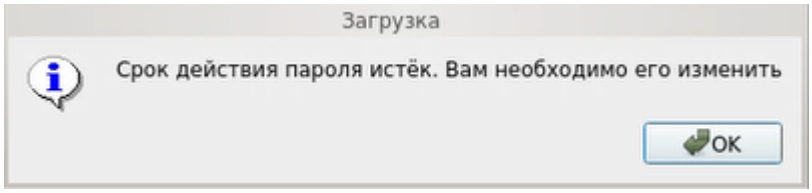


Рис. 24. Сообщение о необходимости изменения пароля учетной записи

В случае, когда разрешение на смену пароля отсутствует, выводится сообщение о ошибке (рис. 25) и производится возврат к окну авторизации.

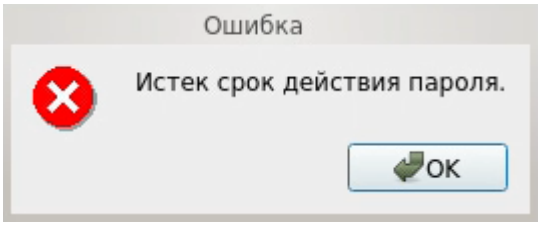


Рис. 25. Сообщение об истечении срока действия пароля

3.2 Смена пароля

При выборе действия «Смена пароля» осуществляется переход к диалоговому окну процедуры смены пароля учетной записи пользователя (рис. 26).

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.

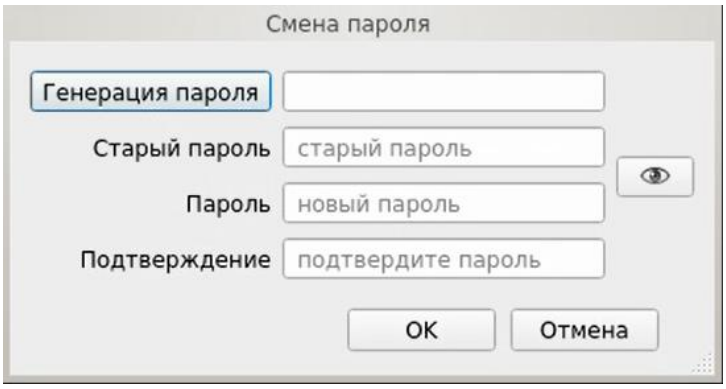


Рис. 26. Диалоговое окно смены текущего пароля учетной записи пользователя

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 (рис. 27).

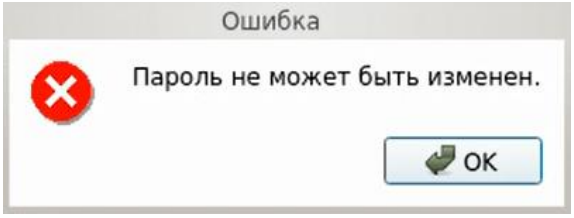


Рис. 27. Окно сообщения при запрете смены пароля пользователем

Для смены пароля необходимо корректно:

- ввести текущий пароль;
- ввести новый пароль, который должен отвечать установленным политикам сложности паролей;
- подтвердить новый пароль.

Также пользователь имеет возможность воспользоваться генератором паролей.

При несоответствии пароля требованиям политики сложности паролей выводится соответствующее сообщение (рис. 28 либо рис. 29), смена пароля не производится, осуществляется возврат к окну смены пароля.

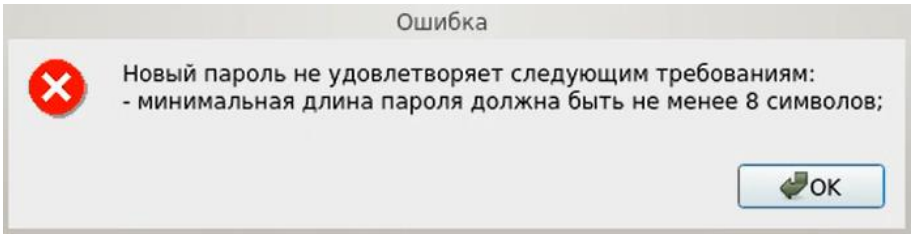


Рис. 28. Сообщение при несоответствии длины пароля учетной записи пользователя политике сложности паролей

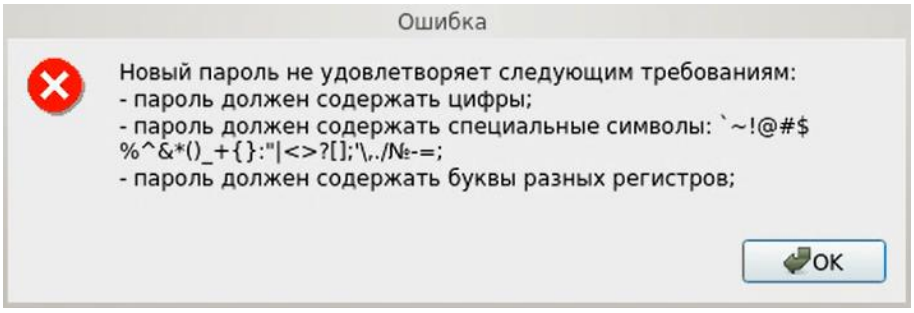


Рис. 29. Сообщение при несоответствии сложности пароля учетной записи пользователя политике сложности паролей

При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ ● (точка).

Если значения пароля в поле ввода и в поле повтора не совпадают, выводится соответствующее сообщение и осуществляется возврат к окну смены пароля (рис. 30).

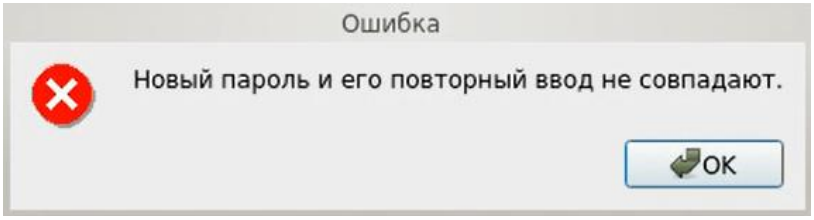


Рис. 30. Сообщение при несовпадении паролей

В базовом режиме дополнительная кнопка  изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет неактивно.

В усиленном режиме работы после окна «Смена пароля» выводится окно, запрашивающее, какой ключ аутентификации использовать (рис. 31). Для генерации ключа аутентификации используется ДСЧ СДЗ Dallas Lock. Ключ аутентификации представляет собой последовательность случайных символов размером 16 байт, он и ПИН-код аппаратного идентификатора обеспечивают двухфакторную аутентификацию. После нажатия кнопки «ОК» соответствующая служебная информация перезаписывается на аппаратном идентификаторе, а также в памяти платы СДЗ Dallas Lock.

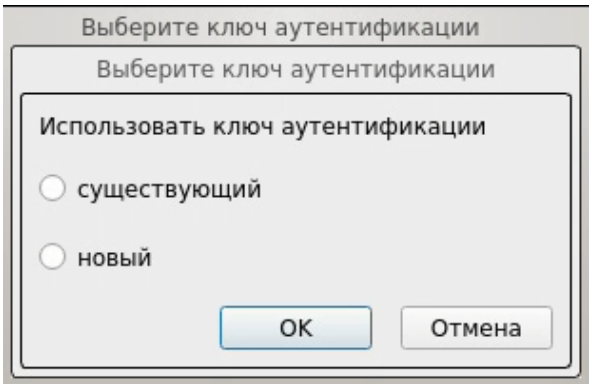


Рис. 31. Окно выбора ключа аутентификации

В случае, когда память предъявленного пользователем аппаратного идентификатора защищена ПИН-кодом, далее появляется окно, в которое необходимо ввести ПИН-код АИ (рис. 32).

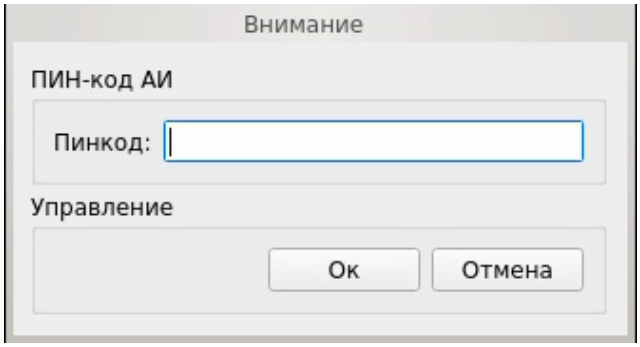


Рис. 32. Окно ввода ПИН-кода АИ

При успешной смене текущего пароля учетной записи пользователя выводится соответствующее сообщение (рис. 33) и осуществляется возврат в окно авторизации.

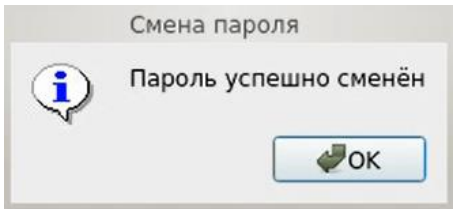


Рис. 33. Сообщение при успешной смене текущего пароля учетной записи пользователя

Примечание. При использовании авторизационных данных из АИ новый пароль записывается в АИ.

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 (рис. 34) расположены вкладки, обеспечивающие доступ к соответствующим разделам:

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

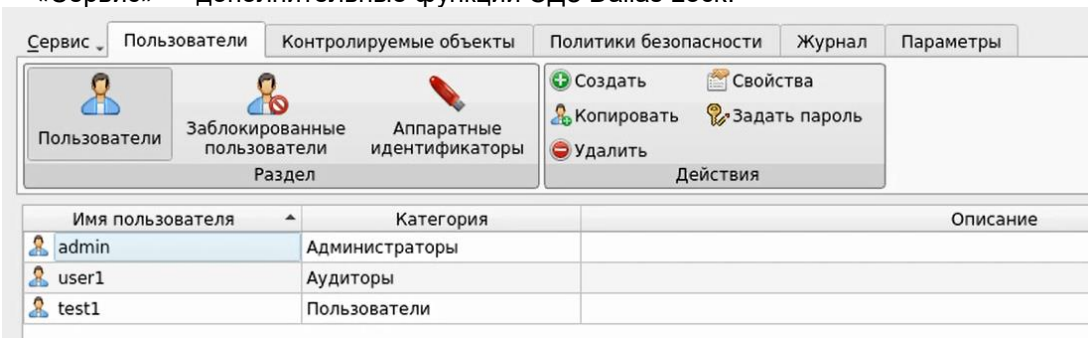


Рис. 34. Главное окно. Пользователи

При попытке запуска оболочки администратора пользователем, не входящим в категорию «Аудитор» или «Администратор», выводится соответствующее сообщение (рис. 35).

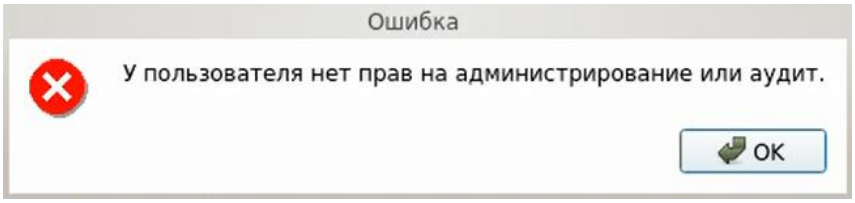


Рис. 35. Сообщение при запрете на администрирование или аудит СДЗ Dallas Lock

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 (рис. 36).

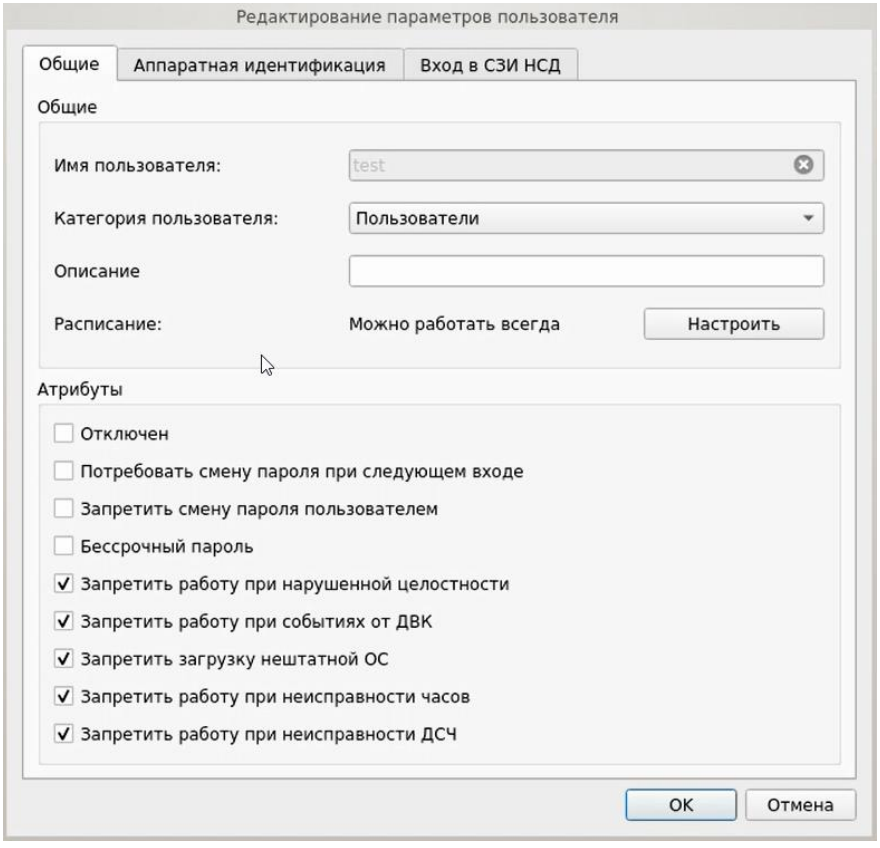


Рис. 36. Окно редактирования параметров учетной записи пользователя.
Данные пользователя

На вкладке «Общие» допустимо редактирование следующих параметров учетной записи пользователя:

- «Категория пользователя» — выбирается из выпадающего списка;

Примечание. Штатные пользователи, допущенные к работе на защищенном компьютере, 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 (рис. 37).

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 нижней части окна.

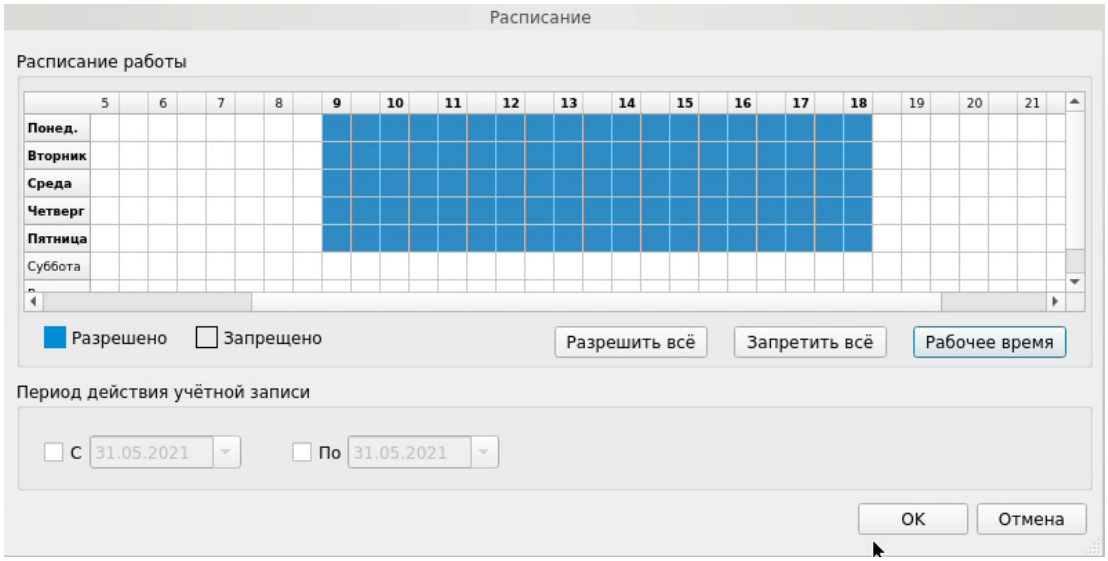


Рис. 37. Окно редактирования разрешенного времени работы в системе

Допустимо присвоение следующих атрибутов учетной записи пользователя (рис. 36):

- «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. Чекбокс данного атрибута отсутствует в окне редактирования доменной учетной записи пользователя.
- «Запретить смену пароля пользователем» — запрет для пользователя на смену своего пароля, в том числе и по истечении срока действия.

Примечание. Присвоить атрибуты «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. 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 ТС запрещается.
- «Запретить работу при событиях от ДВК» — вход в систему блокируется при срабатывании

ДВК. На экране приглашения в систему отображается сообщение об ошибке (рис. 38).

Примечание. Данный атрибут не применим для вариантов исполнения изделия ПФНА.501410.003-02 и ПФНА.501410.003-04 (платы формата miniPCIe-HS «КТ-521» и формата и M.2 «КТ-550»).

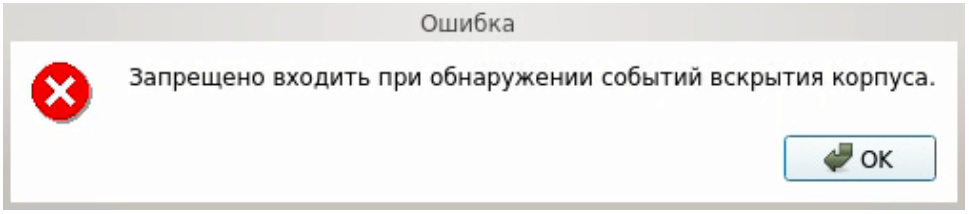


Рис. 38. Сообщение о запрете входа при срабатывании ДВК

- «Запретить загрузку нештатной ОС» — запрет на загрузку ОС с носителя, отличающегося 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 не применим для вариантов исполнения изделия ПФНА.501410.003-02 и ПФНА.501410.003-04 (платы формата miniPCIe-HS «КТ-521» и формата и M.2 «КТ-550»).

- «Запретить работу при неисправности ДСЧ» — вход в систему блокируется при неисправности датчика случайных чисел (далее — ДСЧ). На экране приглашения в систему отображается соответствующее сообщение.

Примечание. В усиленном режиме работы СДЗ атрибуты «Запретить работу при нарушенной целостности», «Запретить работу при событиях от ДВК», «Запретить работу при неисправности часов» и «Запретить работу при неисправности ДСЧ» присвоены по умолчанию категории «Пользователи» и недоступны для изменения.

На вкладке «Аппаратная идентификация» (рис. 39) возможно назначение АИ в следующем порядке:

- предъявить АИ 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 АИ 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.

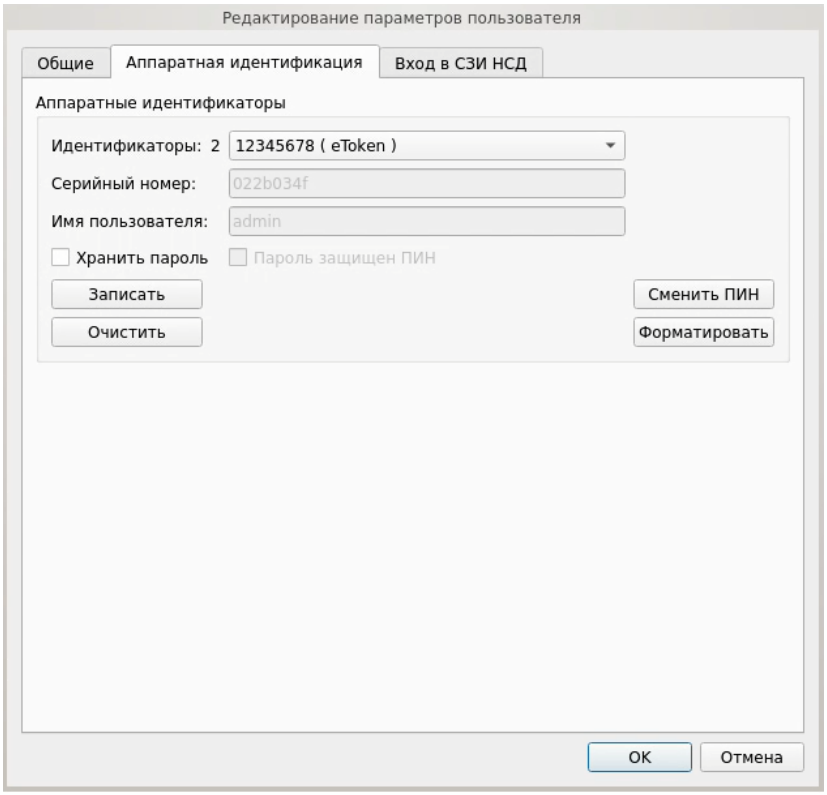


Рис. 39. Окно редактирования параметров учетной записи пользователя. Аппаратная идентификация (базовый режим работы)

Примечание. В усиленном режиме работы на вкладке «Аппаратная идентификация» отсутствуют чекбокс «Хранить пароль», кнопки «Записать» и «Очистить» (рис. 40).

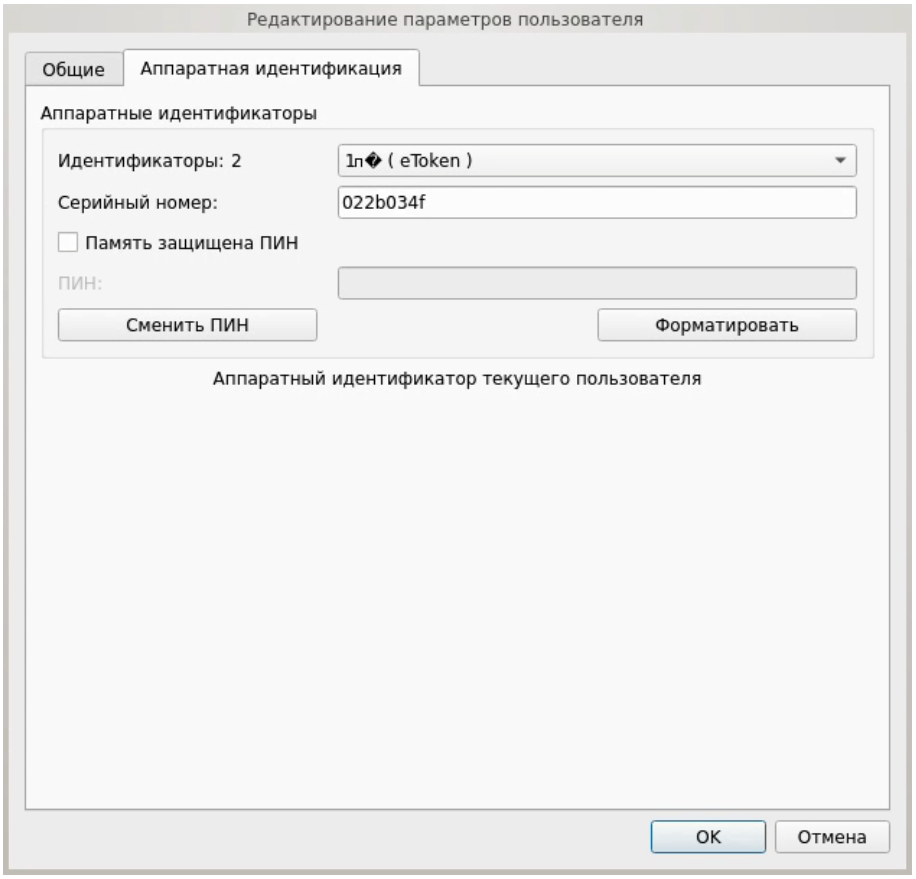


Рис. 40. Окно редактирования параметров учетной записи пользователя. Аппаратная идентификация (усиленный режим работы)

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 соответствующие поля будет подставлена записанная информация, поля будут недоступны для редактирования. 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 АИ.

- «Хранить пароль» — данный атрибут позволяет хранить пароль в незащищенной 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. 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-код.

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

- «Сменить ПИН» — данная кнопка позволяет сменить ранее назначенный ПИН-код учетной записи пользователя для АИ. В окне «Изменение ПИН-кода» (рис. 41) ввести старый, новый ПИН-код и повторить ввод нового ПИН-кода.

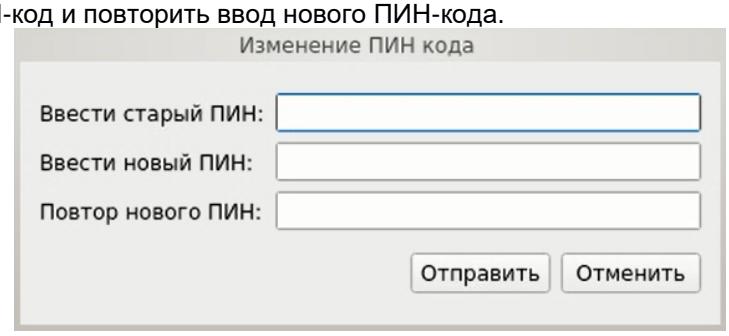


Рис. 41. Окно смены ПИН-кода

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

- «Форматировать» — данная кнопка позволяет провести форматирование АИ и очистить всю ранее записанную идентификационную и аутентификационную информацию (рис. 42).

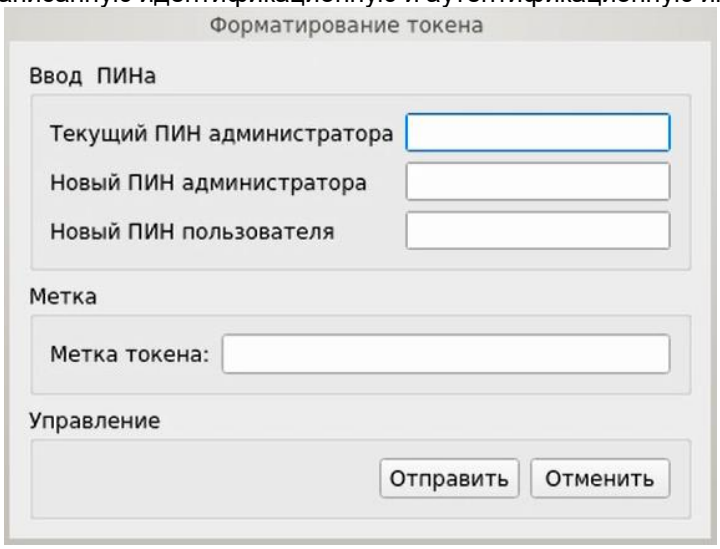


Рис. 42. Окно форматирования токена

В окне «Форматирование токена» необходимо ввести следующую информацию:

- старый ПИН-код администратора;
- новый ПИН-код администратора;
- новый ПИН-код пользователя;
- метку токена.

Нажать кнопку «Отправить».

В базовом режиме функционирования СДЗ в окне «Редактирование параметров пользователя» имеется вкладка «Вход в СЗИ НСД» (рис. 43), позволяющая дополнительно настроить автовход в СЗИ НСД Dallas Lock, установив соответствующий атрибут. При этом можно выбрать опцию:

- «Авторизационные данные, введенные пользователем при входе», чтобы использовать данные учетной записи пользователя, которые были введены при входе;
- «Предопределенные данные», чтобы внести данные учетной записи пользователя вручную.

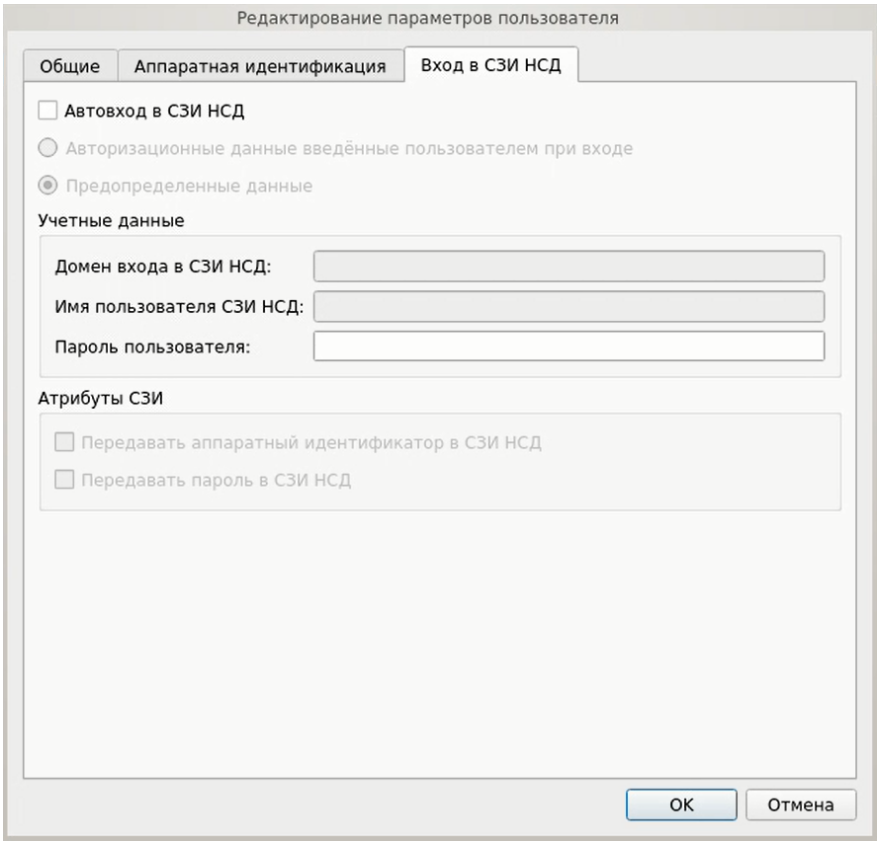


Рис. 43. Окно редактирования параметров учетной записи пользователя. Вход в СЗИ НСД

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

- «Домен входа в СЗИ НСД»;
- «Имя пользователя СЗИ НСД»;
- «Пароль пользователя».

Допустимо присвоение следующих атрибутов СЗИ НСД:

- «Передавать аппаратный идентификатор в СЗИ НСД»;
- «Передавать пароль в СЗИ НСД».

Примечание. Обязательным условием корректной работы автовхода является включение в СЗИ НСД Dallas Lock параметра безопасности «Использовать авторизационную информацию от СДЗ Dallas Lock» в категории «Вход».

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

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 (рис. 44) и по окончании настройки выводится окно «Ввод пароля» (аналогично рис. 45), в котором необходимо установить пароль для учетной записи пользователя.

Примечание. Требования к имени учетной записи пользователя:

- имя учетной записи не может быть пустым и содержать более 31 символа;
- имя учетной записи не может начинаться и заканчиваться пробелом или точкой;
- имя учетной записи может содержать латинские и кириллические символы, цифры;
- имя учетной записи может содержать специальные символы, такие как "`", "~", "!", "?", "#", "№", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", " ", "}", "[", "]", "/", "|",":", ";", """, "'", "<", ">", ".", ",", "=".

Примечание. В усиленном режиме работы при создании новой учетной записи пользователя также можно выбрать тип регистрации: первичная или вторичная.

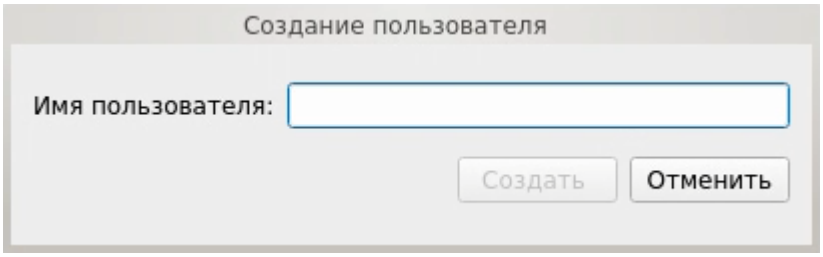


Рис. 44. Окно ввода имени пользователя новой учетной записи

Примечание. Доменные учетные записи нельзя создать средствами СДЗ Dallas Lock, можно зарегистрировать лишь 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 выбранной 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 (рис. 45) имеется возможность установить новый пароль учетной записи пользователя.

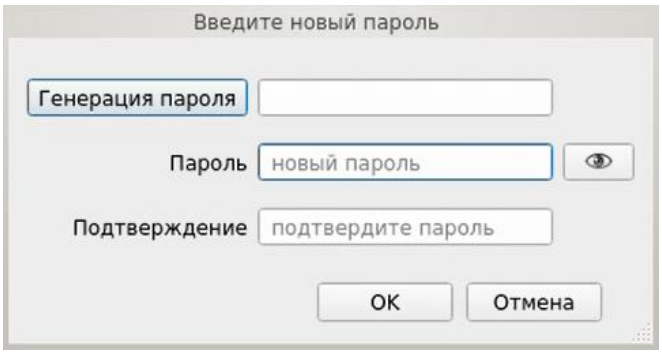


Рис. 45. Окно установки пароля для учетной записи пользователю

Заблокированные пользователи

Учетная запись пользователя по разным причинам может быть заблокирована, например, вследствие неправильного ввода пароля несколько раз.

Разблокировка учетной записи пользователя осуществляется автоматически по истечении указанного времени блокировки или после явной разблокировки администратором в разделе «Заблокированные пользователи» (рис. 46). В таком случае у пользователя появляется возможность осуществить вход в систему снова.

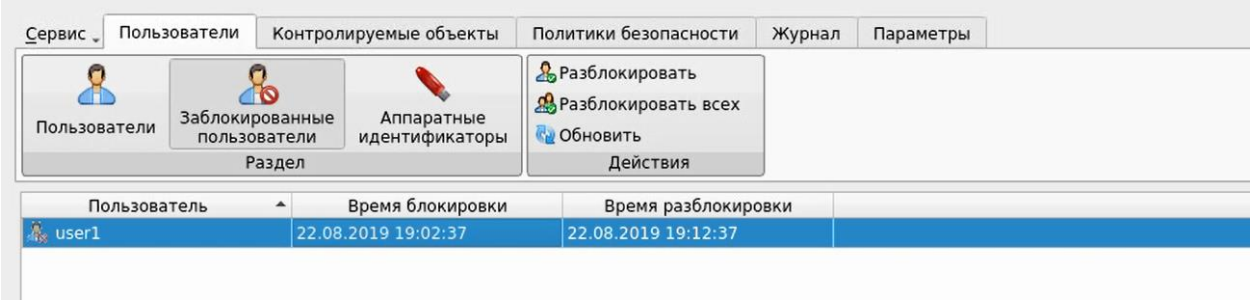


Рис. 46. Окно «Заблокированные пользователи»

Для разблокирования конкретной учетной записи необходимо выбрать ее из списка и нажать кнопку «Разблокировать» в панели «Действия».

Для разблокирования всех заблокированных учетных записей необходимо нажать кнопку «Разблокировать всех».

Для обновления списка заблокированных учетных записей пользователей необходимо нажать кнопку «Обновить».

Внимание! Важно не путать данное свойство с параметром «отключена» учетной записи, не смотря на одинаковый запрет доступа к работе на ТС. Примером различного состояния заблокированных и отключенных учетных записей может быть следующий.

Под одной доменной учетной записью, зарегистрированной в СДЗ Dallas Lock по маске, могут работать несколько доменных пользователей, и некоторые из них могут быть заблокированы, но в тоже время доменная учетная запись по маске не отключена. Учетные записи данных заблокированных пользователей будут отображаться в списке несмотря на то, что индивидуально в СДЗ Dallas Lock они не зарегистрированы (зарегистрирована уч. запись по маске). В этом случае для разблокировки индивидуальных пользователей, для которых зарегистрирована одна на всех учетная доменная запись по маске, используется данная функция разблокировки в окне «Заблокированные пользователи».

Управление аппаратными идентификаторами

Управление АИ пользователей осуществляется в разделе «Аппаратные идентификаторы» (рис. 47).

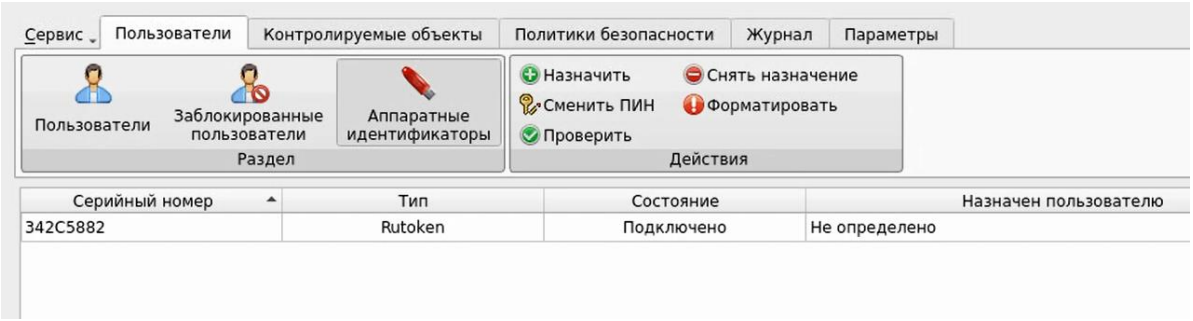


Рис. 47. Окно «Аппаратные идентификаторы»

Для назначения АИ пользователю необходимо нажать кнопку «Назначить» в блоке «Действия», в появившемся диалоговом окне выбрать пользователя и при необходимости установить флаг в поле напротив «Память защищена ПИН» — в этом случае необходимо также указать ПИН АИ. (рис. 48).

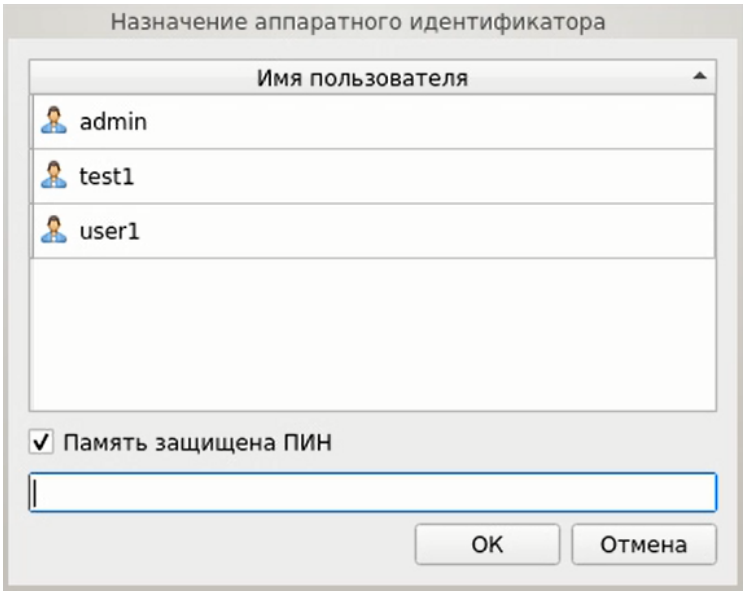


Рис. 48. Диалоговое окно «Назначение аппаратного идентификатора»

По нажатию кнопки «Проверить» запускается процесс тестирования АИ. По завершению тестирования появится соответствующее сообщение (рис. 49).

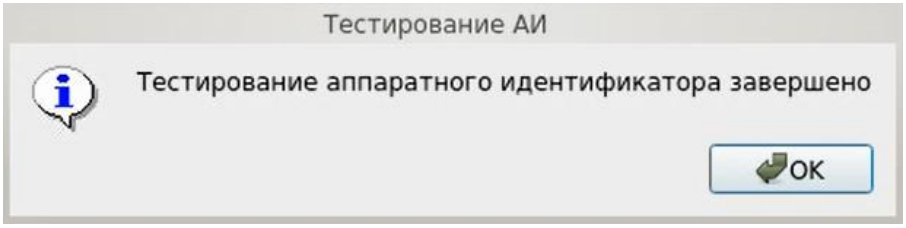


Рис. 49. Сообщение о завершении тестирования АИ

Примечание. Для JaCarta и Rutoken lite процесс проверки памяти может занимать около 5–10 минут.

Для форматирования АИ необходимо нажать кнопку «Форматировать» в блоке «Действия» и в диалоговом окне ввести соответствующие данные (рис. 50).

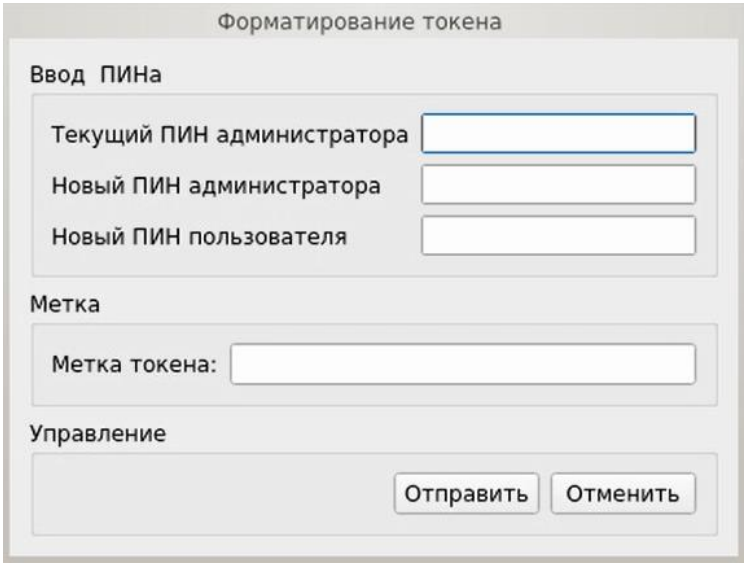


Рис. 50. Окно «Форматирование токена»

3.3.2 Контроль целостности

В разделе «Контролируемые объекты» в виде таблицы отображаются все контролируемые объекты, зарегистрированные в СДЗ Dallas Lock (рис. 51).

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»;
- «Прошивка СДЗ».

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

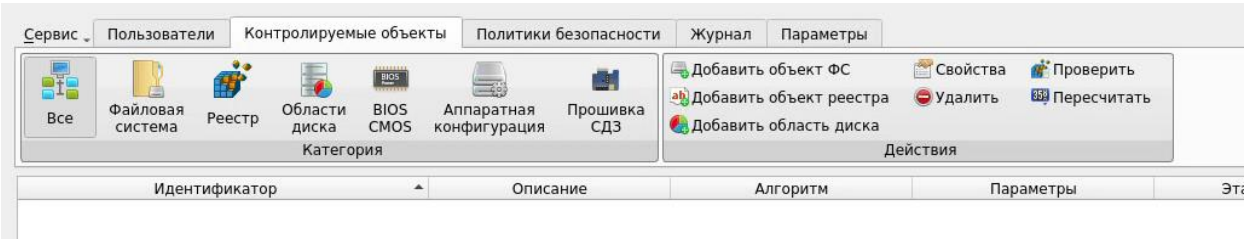


Рис. 51. Главное окно. Контролируемые объекты

Возможны следующие действия с контролируемыми объектами:

- «Добавить объект ФС»;
- «Добавить объект реестра»;
- «Добавить область диска»;
- «Свойства»;
- «Удалить»;
- «Проверить»;
- «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» (рис. 52), 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».

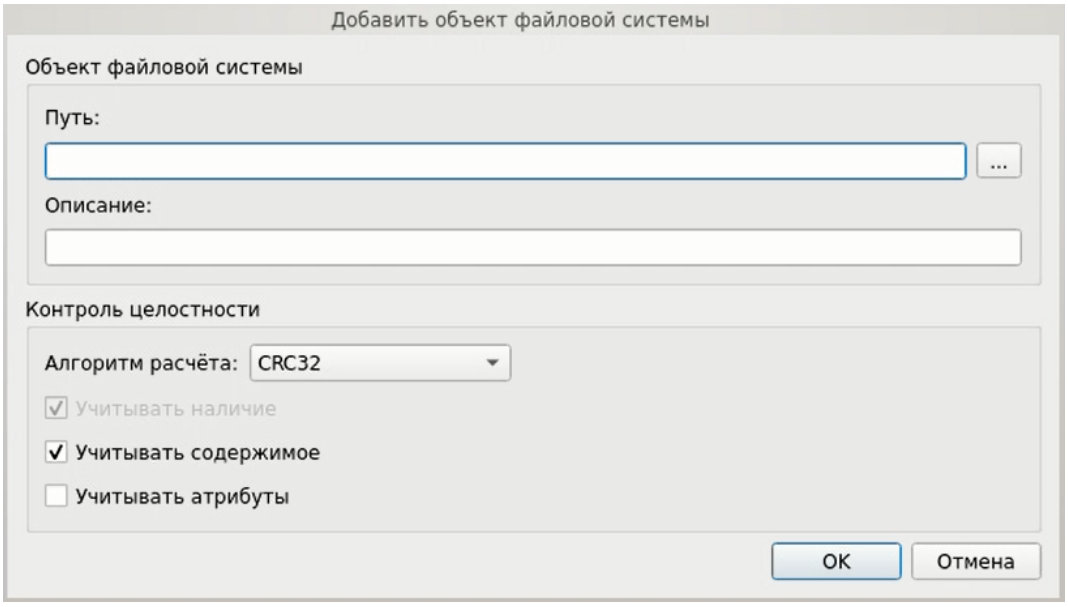


Рис. 52. Окно добавления объекта ФС в контролируемые объекты

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 без вывода предупреждения.

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

При нажатии кнопки «Пересчитать» 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» (рис. 53), 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».

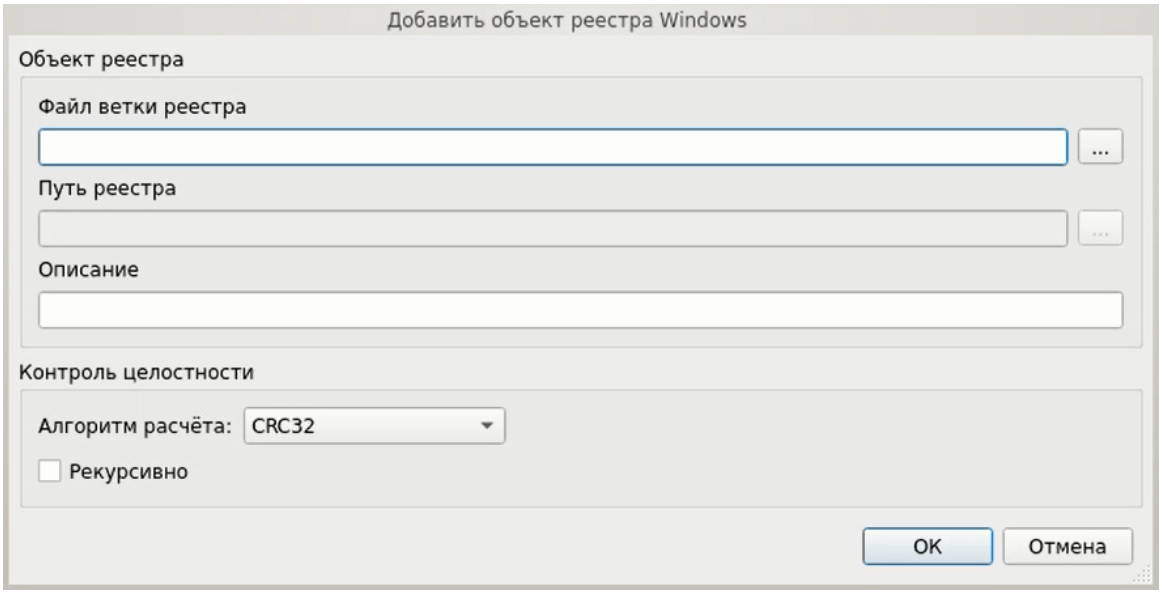


Рис. 53. Окно добавления объекта реестра в контролируемые объекты

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 «Пересчитать» 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» (рис. 54), где доступно редактирование следующих параметров:

- «Диск» — из выпадающего списка выбирается жесткий диск, подключенный к ТС. 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».

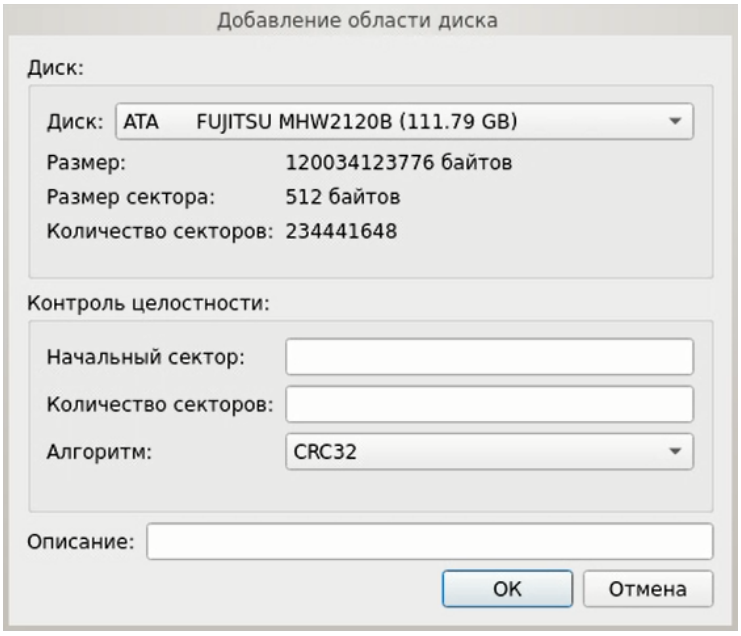


Рис. 54. Окно добавления области диска в контролируемые объекты

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 «Пересчитать» 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» (рис. 55). 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» предусмотрены кнопки «Выделить все» и «Очистить». В блоке «CMOS» это кнопки «Инверсия», которая заменяет назначение целостности для каждой ячейки на обратное значение, «Очистить» и «По умолчанию». На выделенные цветом ячейки назначен контроль целостности. Если ячейки красного цвета — контроль целостности для них не пройден.

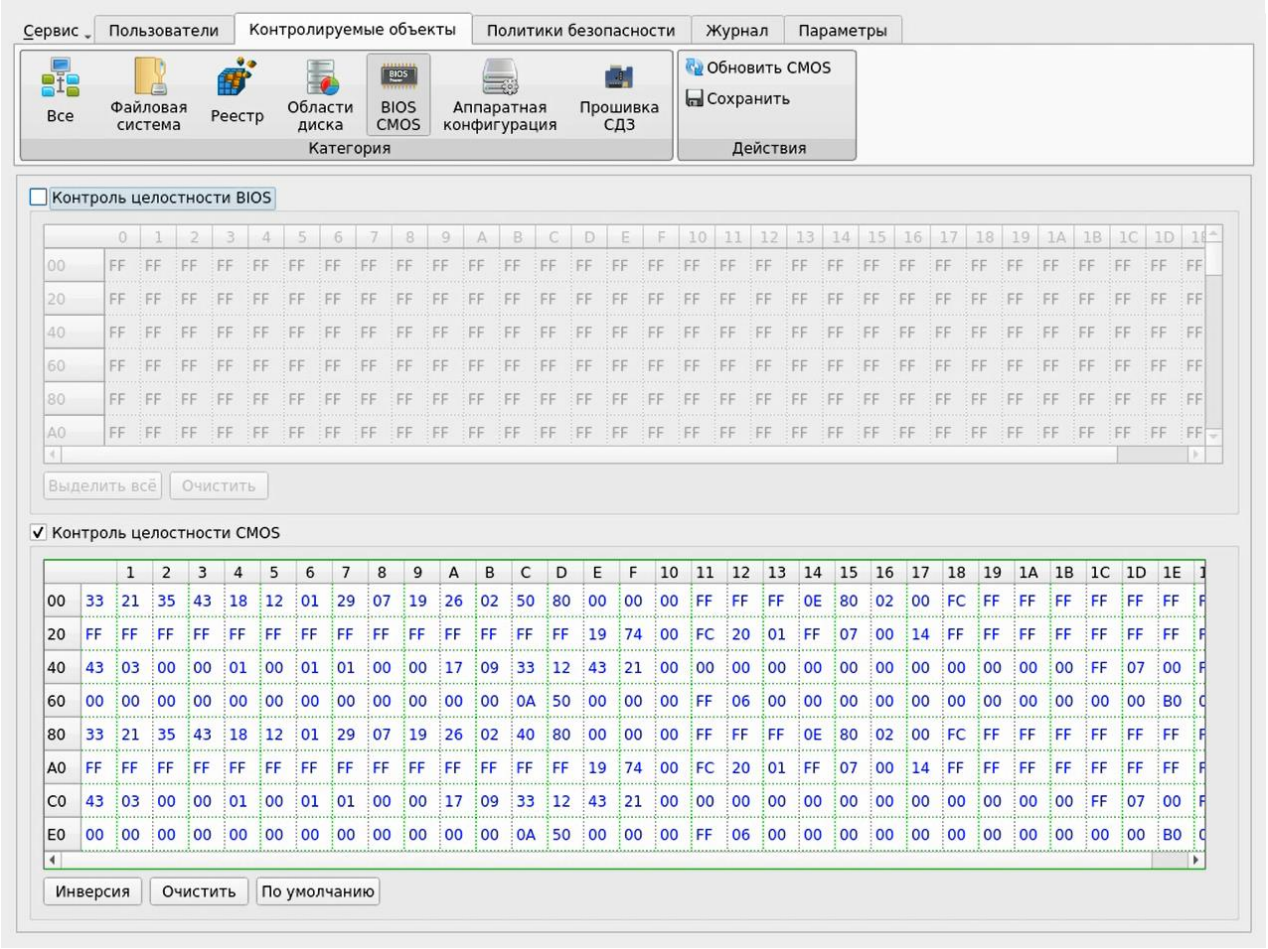


Рис. 55. Контроль BIOS CMOS

Контроль целостности объектов аппаратной конфигурации ТС

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

Для категории «Аппаратная конфигурация» доступны следующие функциональные кнопки:

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

Для настройки контроля аппаратной конфигурации в основной области доступны соответствующие группам чекбоксы (рис. 56) «контролировать группу» и напротив конкретного идентификатора в группе «исключить из контроля»/«включить контроль».

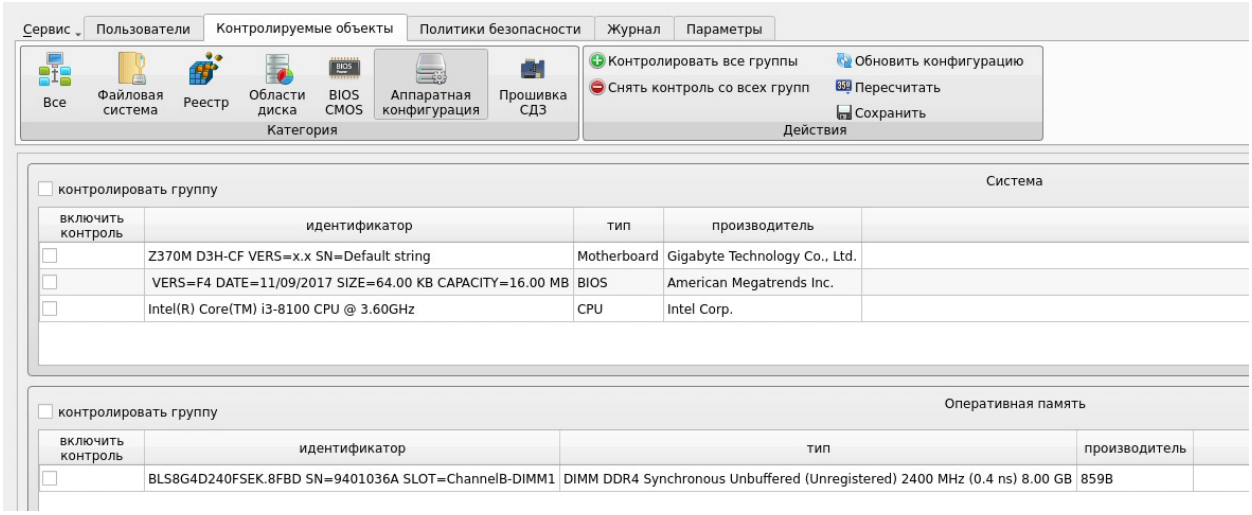


Рис. 56. Главное окно. Контролируемые объекты аппаратной конфигурации ТС

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

Таблица 1 — Пример списка групп аппаратной конфигурации

Группа	Описание
Система	Информация о материнской плате, BIOS и центральном процессоре
Оперативная память	Установленные модули оперативной памяти
PCI-Устройства	Подключенные PCI-устройства
Накопители	Установленные накопители
USB-Устройства	Различные устройства, подключенные через USB-порт, например, АИ, USB-преобразователи и USB-HID устройства

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

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

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

Контроль целостности прошивки СДЗ

Для категории «Прошивка СДЗ» доступны следующие действия:

- «Проверить» — при нажатии осуществляется обновление расчетных контрольных сумм прошивки СДЗ;
- «Сохранить» — при нажатии осуществляется сохранение выбранного алгоритма и расчет контрольных сумм прошивки СДЗ.

Для установки контроля целостности прошивки СДЗ необходимо установить флаг в поле «Включить контроль прошивки СДЗ» (рис. 57).

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

Для сохранения установленных данных необходимо нажать кнопку «Сохранить».

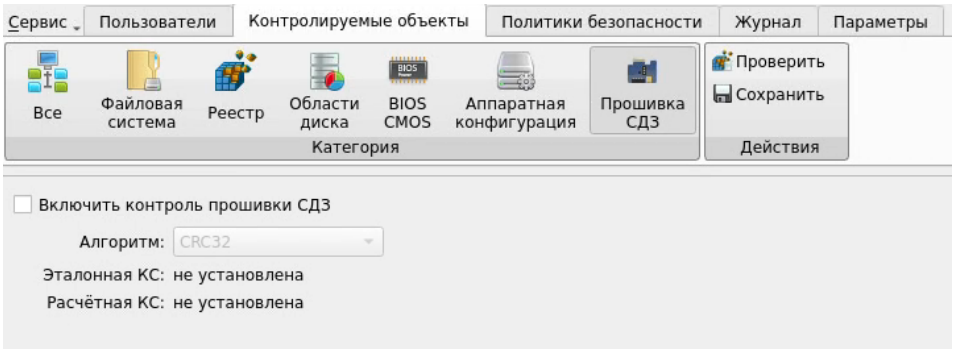


Рис. 57. Главное окно. Контроль прошивки СДЗ

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» (рис. 58, рис. 59, рис. 60). Описание и возможные значения политик приведены в Таблицах 2, 3 и 4.

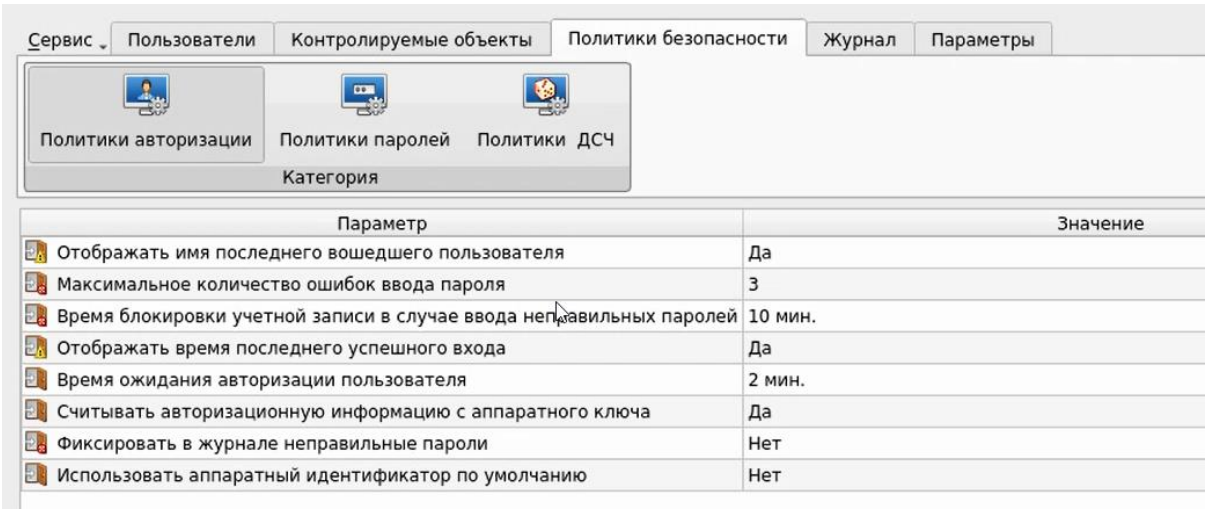


Рис. 58. Главное окно. Политики авторизации

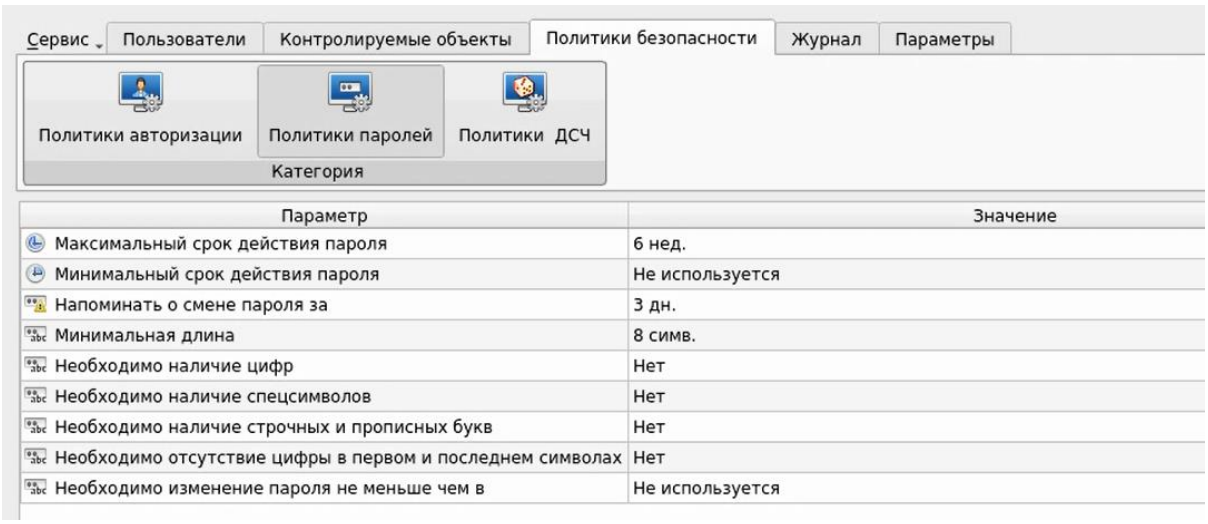


Рис. 59. Главное окно. Политики паролей

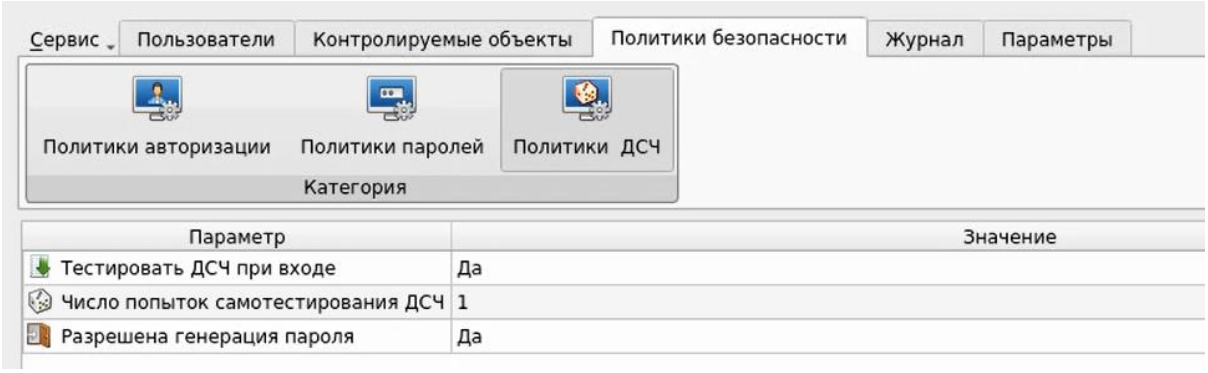


Рис. 60. Главное окно. Политики ДСЧ

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 приведен на рис. 61. Сохранение измененных значений параметров политики безопасности осуществляется после нажатия кнопки «ОК» в диалоговом окне редактирования параметров политики безопасности.

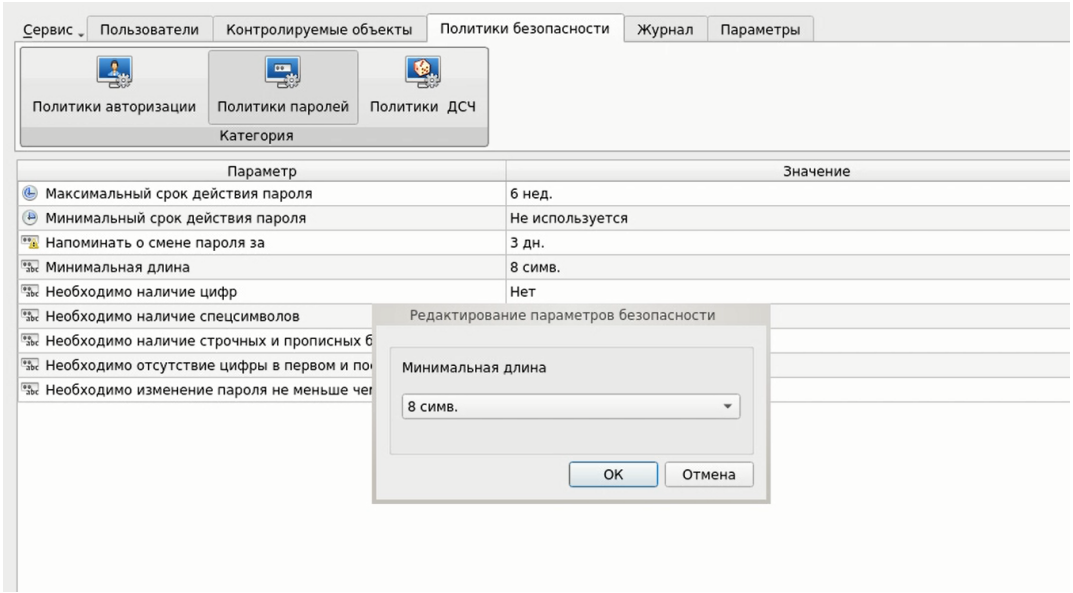


Рис. 61. Диалоговое окно редактирования параметров политики безопасности

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 «Имя пользователя» 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 учетная запись пользователя блокируется на определенное время, устанавливаемое параметром «Время блокировки учетной записи в случае ввода неправильных паролей».

Параметр политики	Описание
	Возможное значение параметра: от 1 до 10 и «Не используется» — количество попыток ввода пароля не ограничено
«Время блокировки учетной записи в случае ввода неправильных паролей»	Установленное значение регламентирует время блокировки учетной записи после ввода неверного пароля более допустимого числа раз (определяется параметром «Максимальное количество ошибок ввода пароля»). В данный интервал времени вход невозможен даже при верном вводе пароля. 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, то уже введенные данные очищаются. Возможное значение параметра: от 1 мин до 10 мин и «Не используется» — время ожидания ввода авторизационных данных не ограничено
«Считывать авторизационную информацию с аппаратного ключа»	Возможное значение параметра: «Да/Нет». В значении «Нет» авторизационная информация вводится пользователем с клавиатуры. В значении «Да» авторизационная информация считывается с памяти АИ в соответствии с настройками учетной записи пользователя, указанными на вкладке «Аппаратная идентификация». Данная политика авторизации доступна только в базовом режиме работы СДЗ Dallas Lock
«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 «Да» во время авторизации информация автоматически считывается с АИ. В значении «Нет» этого не происходит.
«Срок действия ключа аутентификации»	Значение данного параметра определяет срок автоматической смены ключа аутентификации. Возможное значение параметра: от 1 дня до 52 недель и «Не используется» — срок действия не ограничен. Данная политика авторизации доступна только в усиленном режиме работы СДЗ Dallas Lock

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 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 еще не истек, смена пароля пользователем запрещена. Возможное значение параметра: от 1 дня до 4 недель и «Не используется» — минимальный срок действия не установлен
«Напоминать о смене пароля за»	Параметр задает 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 нем 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 прочие. Возможное значение параметра: «Да/Нет»
«Необходимо наличие строчных и прописных букв»	Если данный параметр включен, то при создании пароля в него должны быть включены как строчные, так и прописные буквы. Возможное значение параметра: «Да/Нет»
«Необходимо отсутствие цифры в первом и последнем символах»	Если данный параметр включен, то при создании пароля его первый и последний символ не должны являться цифрами. Возможное значение параметра: «Да/Нет»
«Необходимо изменение пароля не меньше, чем в»	Если данный параметр включен, то при смене пароля новый пароль должен отличаться от старого не менее, чем на указанное количество символов. Сверка старого и нового пароля осуществляется посимвольно. Возможное значение параметра: от 1 до 10 символов 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 самотестирование ДСЧ при входе. При значении «Нет» самотестирование 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».

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

3.3.4 Регистрация и учёт

В разделе «Журнал» в виде таблицы отображаются все события, зарегистрированные в ходе работы СДЗ Dallas Lock (рис. 62).

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.

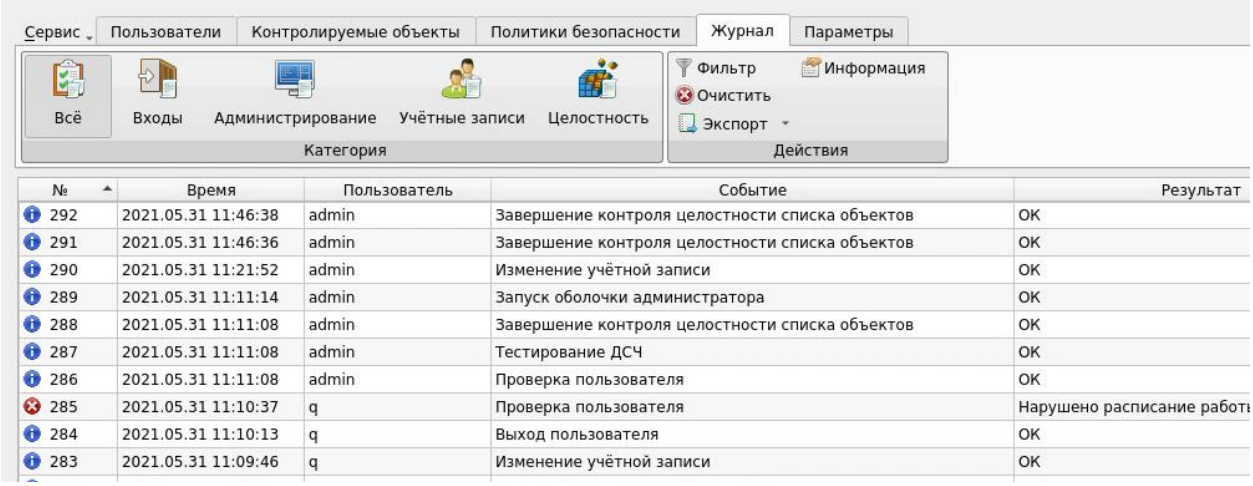
Примечание. Журнал в усиленном режиме работы имеет дополнительное поле «Аппаратный идентификатор», в котором содержится серийный номер АИ пользователя.

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».



№	Время	Пользователь	Событие	Результат
292	2021.05.31 11:46:38	admin	Завершение контроля целостности списка объектов	OK
291	2021.05.31 11:46:36	admin	Завершение контроля целостности списка объектов	OK
290	2021.05.31 11:21:52	admin	Изменение учётной записи	OK
289	2021.05.31 11:11:14	admin	Запуск оболочки администратора	OK
288	2021.05.31 11:11:08	admin	Завершение контроля целостности списка объектов	OK
287	2021.05.31 11:11:08	admin	Тестирование ДСЧ	OK
286	2021.05.31 11:11:08	admin	Проверка пользователя	OK
285	2021.05.31 11:10:37	q	Проверка пользователя	Нарушено расписание работ
284	2021.05.31 11:10:13	q	Выход пользователя	OK
283	2021.05.31 11:09:46	q	Изменение учётной записи	OK

Рис. 62. 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 (рис. 63), в котором при нажатии правой кнопки мыши осуществляется выбор:

- текстового фильтра;
- интервального фильтра;
- фильтра по значению;
- регулярного выражения;
- автофильтра (рис. 64).

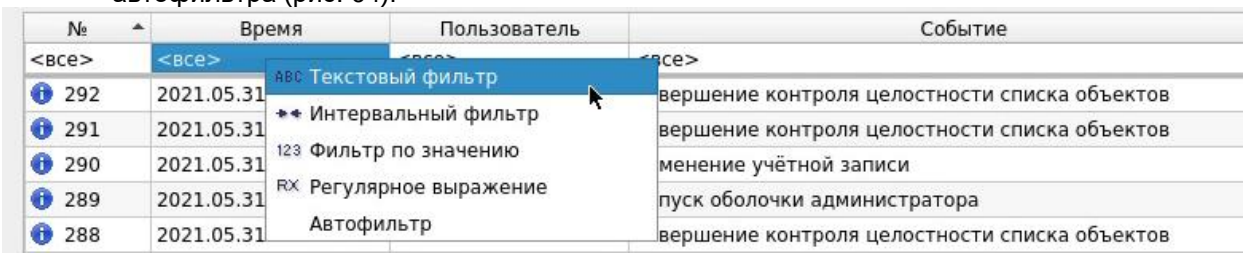


Рис. 63. Главное окно. Назначение фильтра

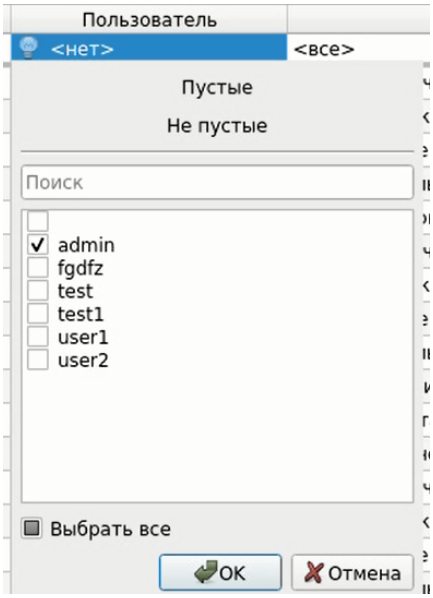


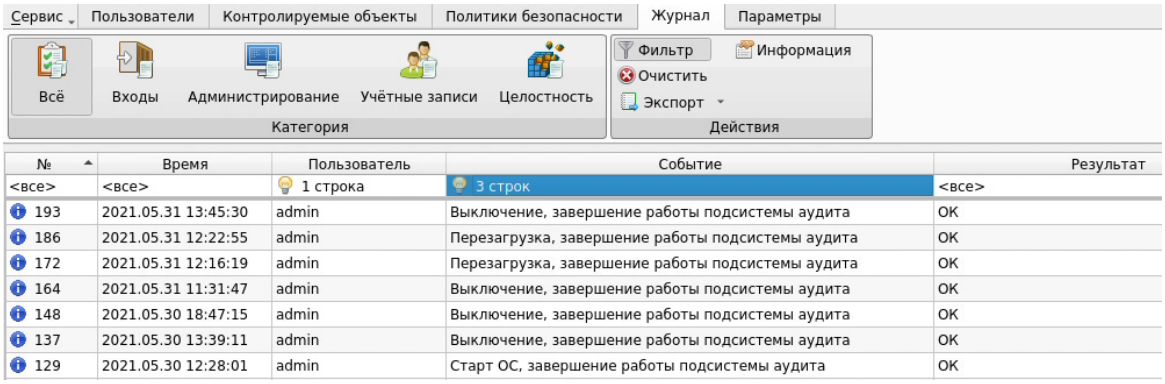
Рис. 64. Меню назначения автофильтра журнала

Результат применения фильтра журнала по заданию пользователя «admin» приведен на рис. 65.

№	Время	Пользователь	Событие	Результат
<все>	<все>	1 строка	<все>	<все>
292	2021.05.31 11:46:38	admin	Завершение контроля целостности списка объектов	OK
291	2021.05.31 11:46:36	admin	Завершение контроля целостности списка объектов	OK
290	2021.05.31 11:21:52	admin	Изменение учётной записи	OK
289	2021.05.31 11:11:14	admin	Запуск оболочки администратора	OK
288	2021.05.31 11:11:08	admin	Завершение контроля целостности списка объектов	OK
287	2021.05.31 11:11:08	admin	Тестирование ДСЧ	OK
286	2021.05.31 11:11:08	admin	Проверка пользователя	OK
202	2021.05.31 18:29:16	admin	Выход пользователя	OK
201	2021.05.31 18:29:12	admin	Создание учётной записи	OK
200	2021.05.31 18:18:08	admin	Запуск оболочки администратора	OK

Рис. 65. Результат применения фильтра журнала по заданию пользователя

Результат применения автофильтра журнала по наименованию события (Выключение, завершение работы подсистемы аудита/Перезагрузка, завершение работы подсистемы аудита/Старт ОС, завершение работы подсистемы аудита) приведен на рис. 66.



№	Время	Пользователь	Событие	Результат
<все>	<все>	1 строка	3 строк	<все>
193	2021.05.31 13:45:30	admin	Выключение, завершение работы подсистемы аудита	OK
186	2021.05.31 12:22:55	admin	Перезагрузка, завершение работы подсистемы аудита	OK
172	2021.05.31 12:16:19	admin	Перезагрузка, завершение работы подсистемы аудита	OK
164	2021.05.31 11:31:47	admin	Выключение, завершение работы подсистемы аудита	OK
148	2021.05.30 18:47:15	admin	Выключение, завершение работы подсистемы аудита	OK
137	2021.05.30 13:39:11	admin	Выключение, завершение работы подсистемы аудита	OK
129	2021.05.30 12:28:01	admin	Старт ОС, завершение работы подсистемы аудита	OK

Рис. 66. Результат применения автофильтра журнала по наименованию события

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

При нажатии кнопки «Очистить» выводится соответствующее предупреждение (рис. 67).

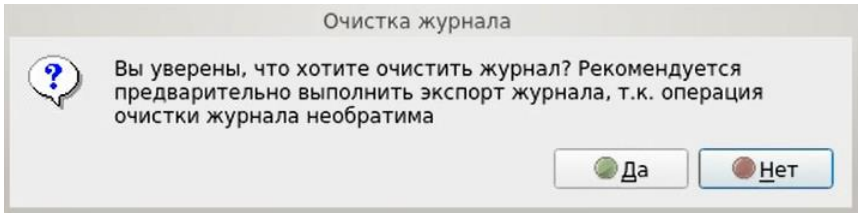


Рис. 67. Сообщение «Очистка журнала»

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

Поскольку операция удаления записей журнала необратима, то перед очисткой журнала рекомендуется произвести экспорт записей журнала в файл. При нажатии кнопки «Экспорт» из выпадающего списка выбирается формат создаваемого файла (рис. 68). Данная функция также доступна пользователям категории «Аудиторы».

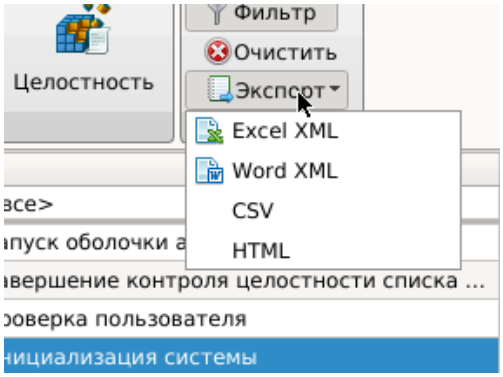


Рис. 68. Главное окно. Меню экспорта журнала в файл

При нажатии кнопки «Информация» выводится соответствующее информационное окно для выбранного события (рис. 69).

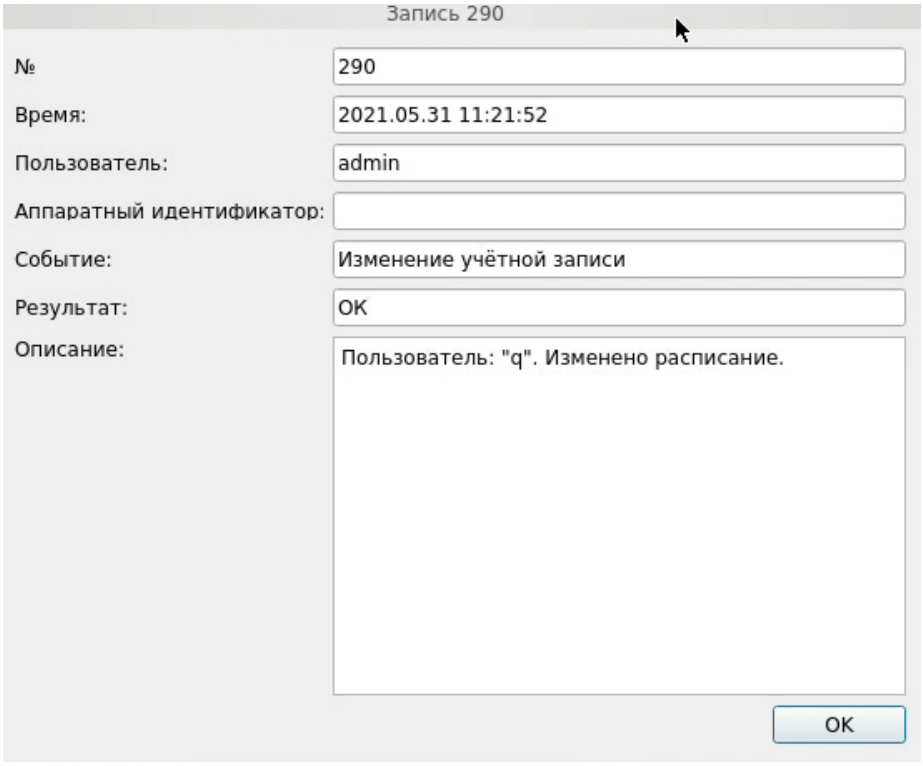


Рис. 69. Информационное окно

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» (рис. 70, рис. 73, рис. 74).

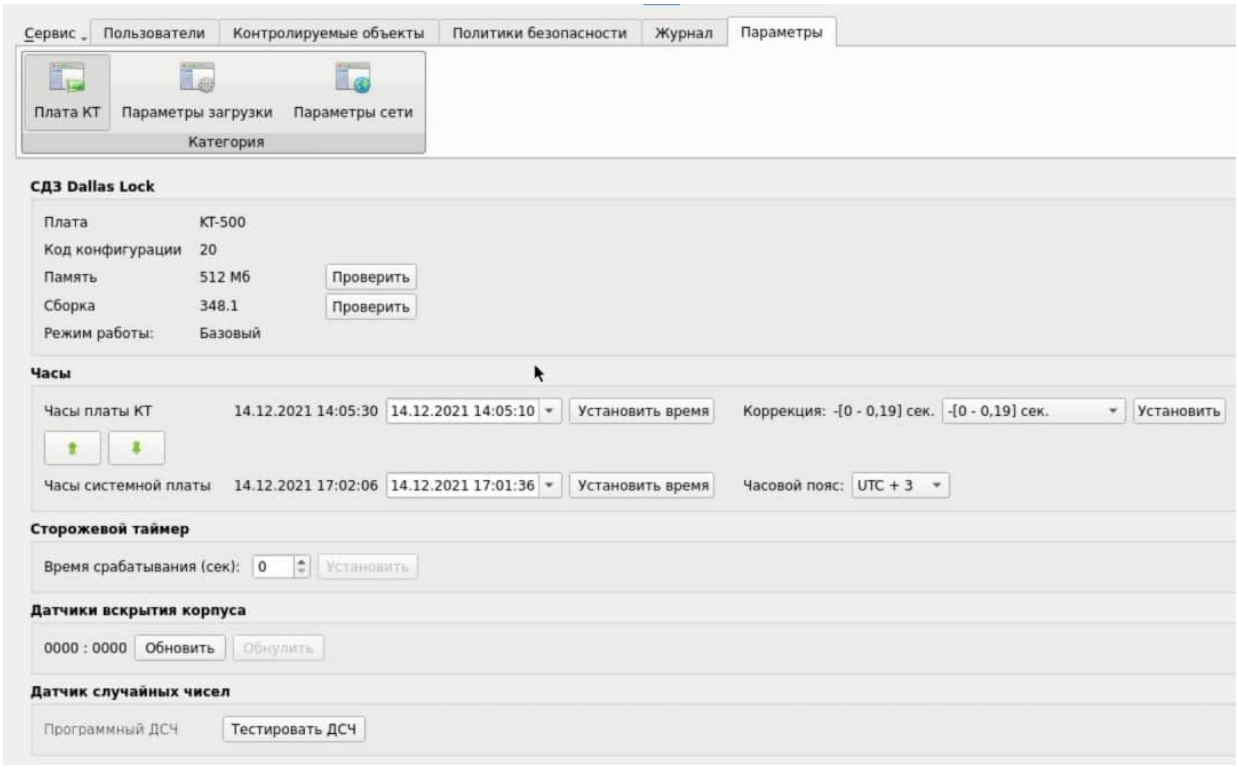


Рис. 70. Главное окно. Плата КТ

Категория «Плата КТ»:

- «СДЗ Dallas Lock» — 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» не применим для вариантов исполнения изделия ПФНА.501410.003-02 и ПФНА.501410.003-04 (платы формата miniPCIe-HS «КТ-521» и формата и M.2 «КТ-550»).

- «Сторожевой таймер» — для сторожевого таймера возможно установить/изменить время срабатывания в секундах. Проверить подключение сторожевого таймера можно при помощи соответствующей кнопки.
- «Датчики вскрытия корпуса» — 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 «Датчики вскрытия корпуса» не применим для вариантов исполнения изделия ПФНА.501410.003-02 и ПФНА.501410.003-04 (платы формата miniPCIe-HS «КТ-521» и формата и M.2 «КТ-550»).

- «Датчик случайных чисел» — возможен запуск тестирования ДСЧ из оболочки администратора при помощи соответствующей кнопки.
- «Батарея» — у печатных плат miniPCIe-HalfSize «КТ-521 r3» (ПФНА.501410.003-10) и M.2 «КТ-550 r3» (ПФНА.501410.003-11) есть разъем для подключения платы RTC с источником питания, необходимым для работы часов реального времени. Чтобы посмотреть уровень заряда батареи, нужно зайти в категорию «Плата КТ». В поле «Батарея» будет указано значение напряжения и уровень заряда батареи (Рис. 71).

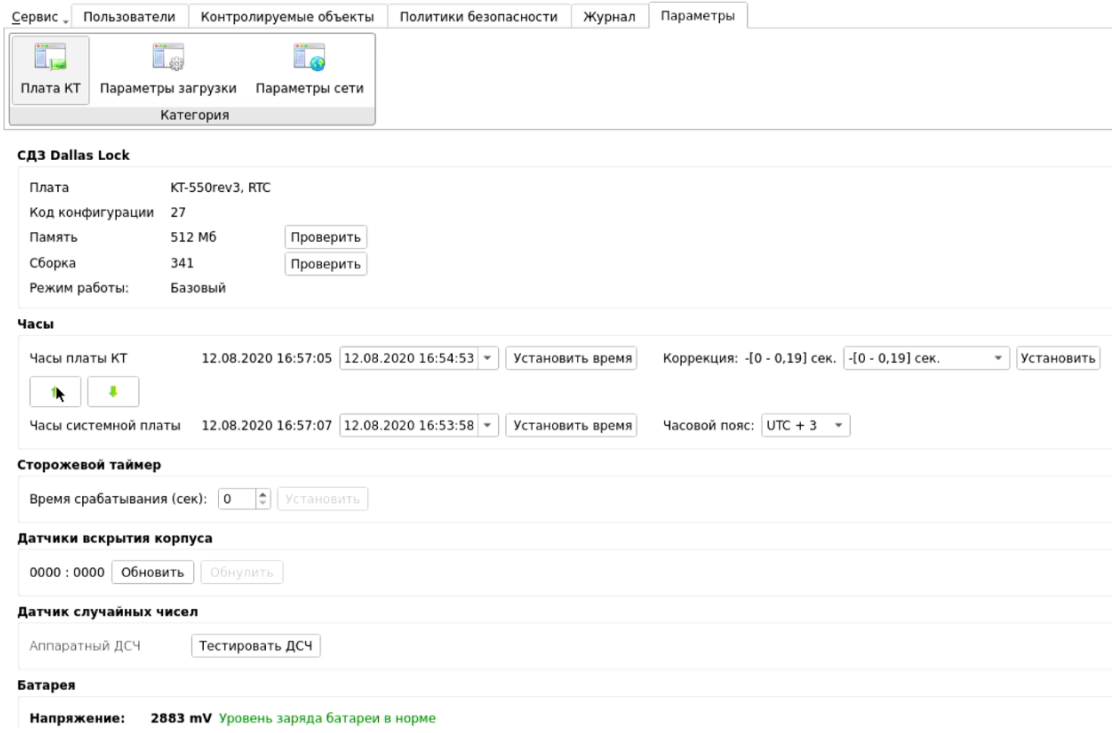


Рис. 71. Уровень заряда батареи в норме

Если батарея разряжена, то в полях «Часы» и «Батарея» выводится информационное сообщение «Батарея полностью разряжена!», а указанное напряжение будет равно 0 mV (Рис. 72):

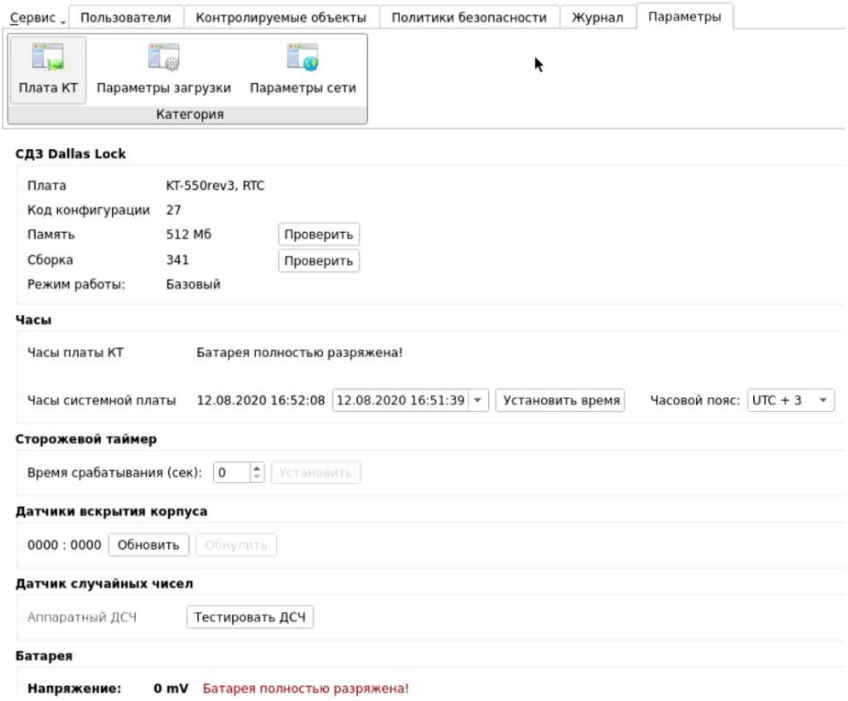


Рис. 72. Батарея разряжена

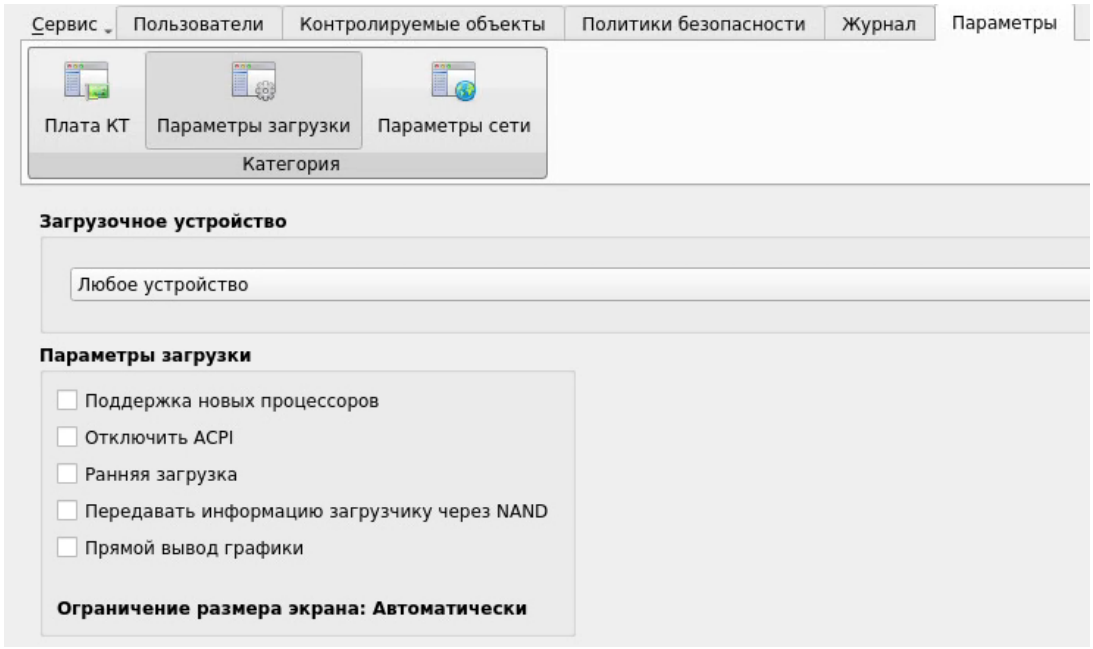


Рис. 73. Главное окно. Параметры загрузки

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:
  - «Поддержка новых процессов» — устанавливается для поддержки новых графических процессоров (GPU) платой СДЗ для UEFI-совместимых материнских плат. По умолчанию — включен.
  - «Отключить ACPI» — устанавливается для отключения механизма получения данных платой СДЗ от механизма ACPI материнской платы. Используется в случае возникновения проблем совместимости. По умолчанию — отключен.

Примечание. Данная функция может некорректно работать на некоторых типах системных плат.

  - «Ранняя загрузка» — устанавливается, если СДЗ Dallas Lock некорректно работает с UEFI-совместимой материнской платой и ШОС, установленной в режиме UEFI-загрузки. По умолчанию — включен.
  - «Передавать информацию загрузчику через NAND» — устанавливается для передачи информации через NAND вместо передачи через RAM.

Примечание. При режиме загрузки платы «UEFI в режиме совместимости» (см. «Интерфейс сервисной утилиты») этот чекбокс должен быть выключен.

  - «Прямой вывод графики» — устанавливается для повышения удобства работы в консоли: появляется возможность изменить разрешение экрана, размеры и стили шрифтов, установить фоновое изображение в загрузчике и т.д. Используется FrameBuffer.

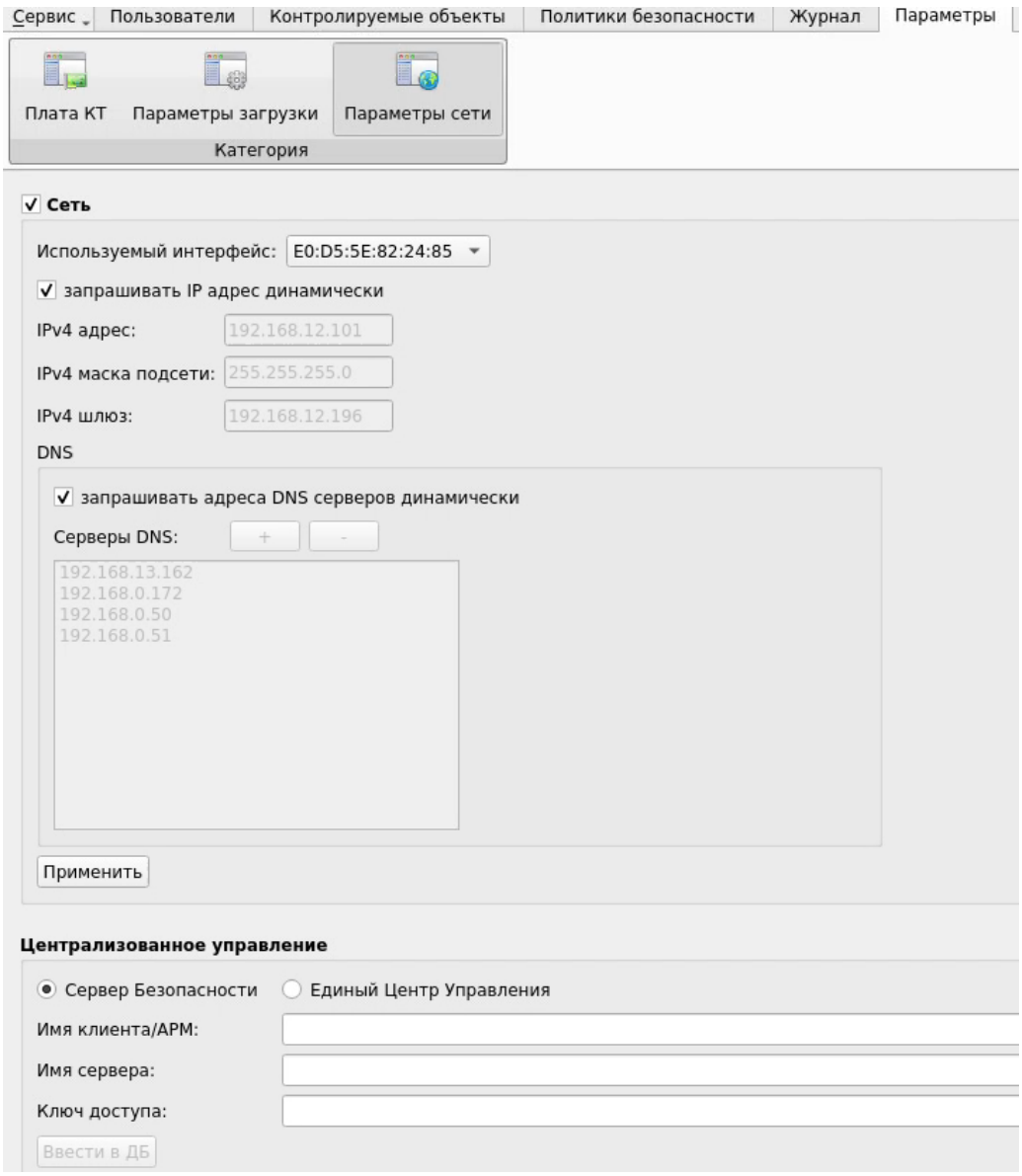


Рис. 74. Главное окно. Параметры сети

Категория «Параметры сети»:

- «Сеть» — чекбокс для включения сети. Содержит сетевые параметры, необходимые для удаленного администрирования с Консоли Сервера безопасности (далее — КСБ) или с Консоли Единого центра управления. Для настройки требуется заполнить следующие поля:
  - «Используемый интерфейс» — из выпадающего списка необходимо выбрать MAC-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, установив флаг в поле «запрашивать динамически. Также для сервера DNS доступны управляющие кнопки «+» и «-», которые позволяют добавлять и удалять DNS-серверы.

  После окончания настройки необходимо нажать кнопку «Применить».
- «Централизованное управление» — для централизованного и оперативного управления клиентами они должны быть введены в Домен безопасности. Для ввода СДЗ клиента в Домен безопасности необходимо выбрать Сервер безопасности (далее по тексту — СБ)

или Единый Центр Управления (далее — ЕЦУ) и заполнить следующие поля:

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

После нажатия кнопки «Ввести в ДБ» клиент СДЗ будет введен в ДБ, появится сообщение об успешном вводе клиента (рис. 75). Для завершения операции и перезагрузки клиента СДЗ необходимо нажать кнопку «ОК».

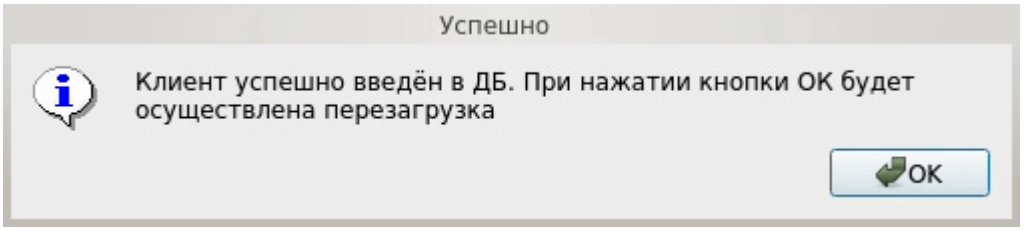


Рис. 75. Информационное сообщение о вводе клиента в ДБ

Примечание. Функция ввода клиента СДЗ в ДБ доступна только в базовом режиме работы СДЗ.

Примечание. Для удаленной перезагрузки/выключения клиентов СДЗ, находящихся в режиме работы ШОС, необходима установка Агента ШОС (см. «Удаленная перезагрузка и удаленное выключение клиентов СДЗ»).

В дереве объектов КСБ или консоли ЕЦУ появится новый клиент СДЗ, после чего в категории «Параметры сети» будет доступна только кнопка «Вывести из ДБ» (рис. 76).

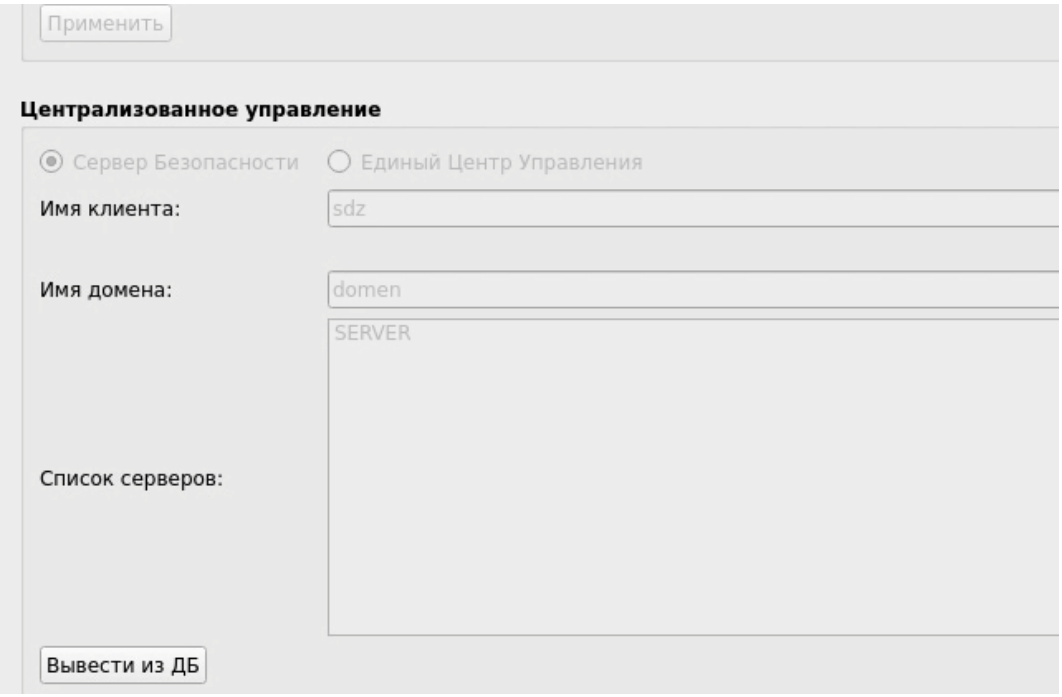


Рис. 76. Параметры сети. Кнопка вывода из ДБ

3.3.6 Дополнительные функции СДЗ Dallas Lock

Меню «Сервис» позволяет получить доступ к дополнительным функциям СДЗ Dallas Lock (рис. 77):

- «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 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. Доступно формирование отчётов «Права и конфигурация» и «Аппаратная часть».
  В отчете «Права и конфигурации» указываются следующие данные:
  - имя пользователя, который создал отчет;
  - дата и время формирования отчета;
  - версия прошивки СДЗ Dallas Lock;
  - режим работы СДЗ;
  - параметры конфигурации СДЗ Dallas Lock в соответствии с настройками отчета.

  В отчете «Аппаратная часть» указываются следующие данные:
  - имя пользователя, который создал отчет;
  - дата и время формирования отчета;
  - характеристики аппаратной конфигурации ТС (система, оперативная память, PCI-устройства, накопители, USB-устройства).
- «О СДЗ Dallas Lock» — вывод информации о версии прошивки СДЗ, указанного кода технической поддержки и контактов производителя. Здесь возможно сменить код технической поддержки.

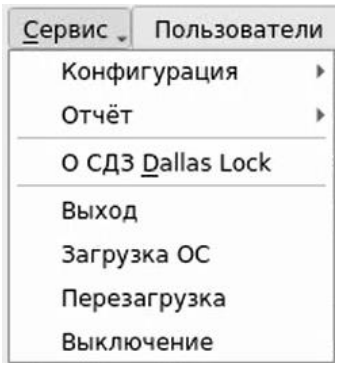


Рис. 77. Главное окно. Меню «Сервис»

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

3.4 Выключение/перезагрузка ТС

В меню «Сервис» также сгруппированы функциональные кнопки, отвечающие за соответствующие процедуры управления ТС (рис. 77):

- «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 ШОС;
- «Перезагрузка» — осуществляется перезагрузка ТС;
- «Выключение» — осуществляется выключение ТС.

3.5 Удаленная перезагрузка и удаленное выключение клиентов СДЗ

В СБ Dallas Lock реализована возможность удаленной перезагрузки/выключения ТС с установленной платой СДЗ Dallas Lock для отдельных клиентов СДЗ, для групп клиентов СДЗ и для домена клиентов СДЗ, находящихся в режиме работы ШОС.

Перезагрузка и выключение удалённой рабочей станции с установленной платой СДЗ Dallas Lock доступны посредством КСБ и осуществляются с помощью устанавливаемого в ШОС Агента.

События удаленной перезагрузки/выключения с помощью СБ клиентов СДЗ Dallas Lock, которые находятся в режиме работы ШОС или доступны для оперативного управления, фиксируются в журнале Сервера безопасности отдельно для каждого клиента СДЗ. В журнале СДЗ «Администрирование» фиксируются только события удаленной перезагрузки/выключения клиентов СДЗ, которые доступны для оперативного управления.

Примечание. Функция удаленной перезагрузки/выключения доступна только для клиентов, работающих в базовом режиме работы СДЗ.

3.5.1 Запуск Агента ШОС

Агент представляет собой службу (демон) ШОС, инсталляторы которой располагаются на компакт-диске, идущем в комплекте с СДЗ Dallas Lock.

Агент ШОС поддерживает следующие типы операционных систем:

- ОС семейства Windows:
  - Windows XP (SP 3) (Professional, Home, Starter);
  - Windows Server 2003 (SP 2) (Web, Standard, Enterprise, Datacenter);
  - Windows Server 2003 R2 (SP 2) (Web, Standard, Enterprise, Datacenter);
  - Windows Vista (SP 2) (Ultimate, Enterprise, Business, Home Premium, Home Basic, Starter);
  - Windows Server 2008 (SP 2) (Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
  - Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
  - Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
  - Windows 8 (Core, Pro, Enterprise);
  - Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
  - Windows 8.1 (Core, Pro, Enterprise);
  - Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
  - Windows 10 (Enterprise, Education, Pro, Home);
  - Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server, Hyper-V Server);
- ОС семейства Linux:
  - ALT Linux 8.2 x64;
  - ALT Linux СПТ 8 x64 (ограничение: корректная работа Агента ШОС возможна с версией ядра **«**4.19.109-un-def-alt0.M80C.1»);
  - Astra Linux Special Edition (Смоленск) 1,5 x64 (ограничение: корректная работа Агента ШОС возможна с версией ядра «4.15.3-1-generic» и при выключенном режиме ЗПС);
  - Astra Linux Special Edition (Смоленск) 1.6 x64 (ограничение: корректная работа Агента ШОС возможна с версией ядра «4.15.3-1-generic»);
  - Astra Linux Common Edition (Орёл) 2.12 x64;
  - Debian 8 x64;
  - CentOS 7 x64;
  - Red Hat Enterprise Linux Server 7 x64;
  - Fedora 24 x64;
  - OpenSUSE 42 x64;
  - Ubuntu 16.04 x64;
  - Ред ОС 7.1 МУРОМ x64.

Для ОС семейства Windows инсталлятор Агента ШОС представляет собой msi-пакет. После запуска инсталлятора и подтверждения согласия на установку (рис. 78) данная процедура проходит в фоновом режиме. По завершению установки выводится сообщение об успешном выполнении процедуры (рис. 79).

Примечание. Необходимым условием корректной работы Агента ШОС является установка драйвера платы КТ, расположенного на идущем в комплекте с СДЗ Dallas Lock диске.

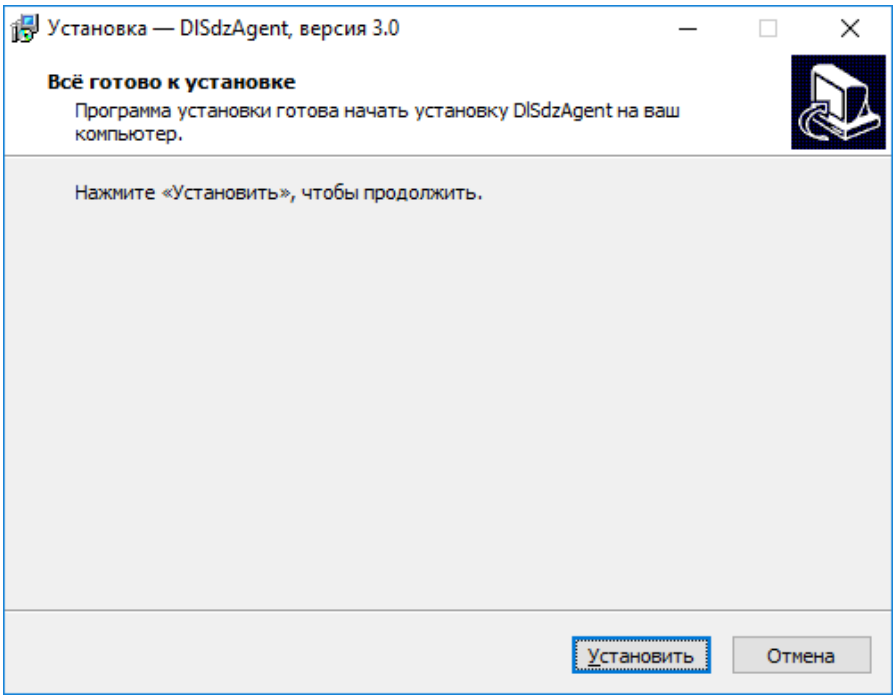


Рис. 78. Подтверждение установки Агента ШОС

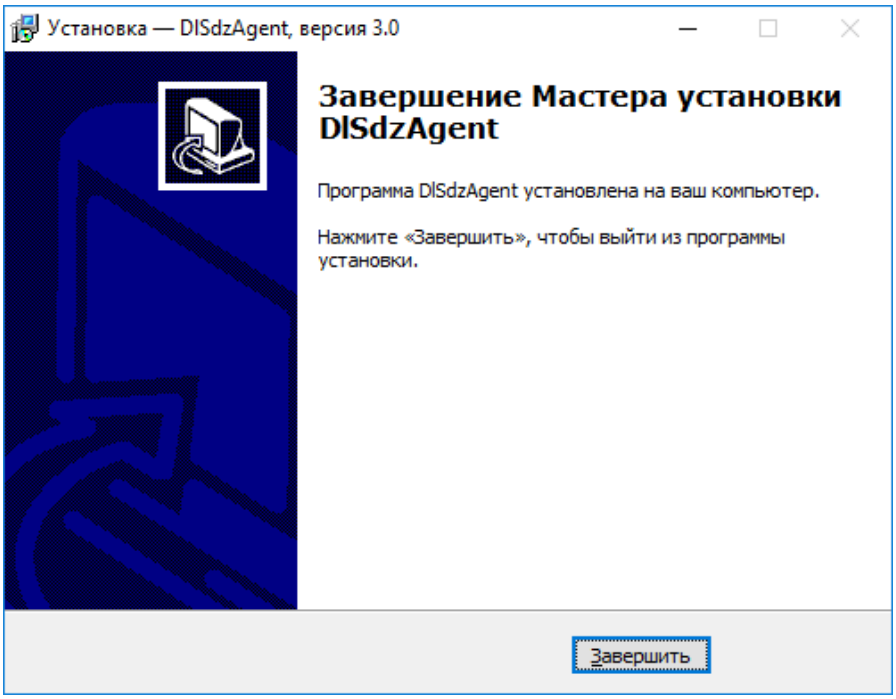


Рис. 79. Сообщение об успешной установке Агента ШОС

Для ОС семейства Linux инсталлятор Агента ШОС представляет собой самоисполняющийся архив с набором *.deb и *.rpm пакетов. В зависимости от ОС будет разархивирован и установлен нужный архив.

Порядок установки Агента ШОС на ОС семейства Linux:

1. Перед запуском инсталлятора администратору необходимо проверить наличие и при необходимости установить:

- заголовки файлов для загруженного ядра;
- инструменты для разработчиков;
- библиотеку systemd и заголовки библиотеки systemd.

2. Задать права на исполнение установочного файла. Для этого следует открыть свойства файла, перейти на вкладку «Права» и поставить флаг в поле «Выполнение» (рис. 80).

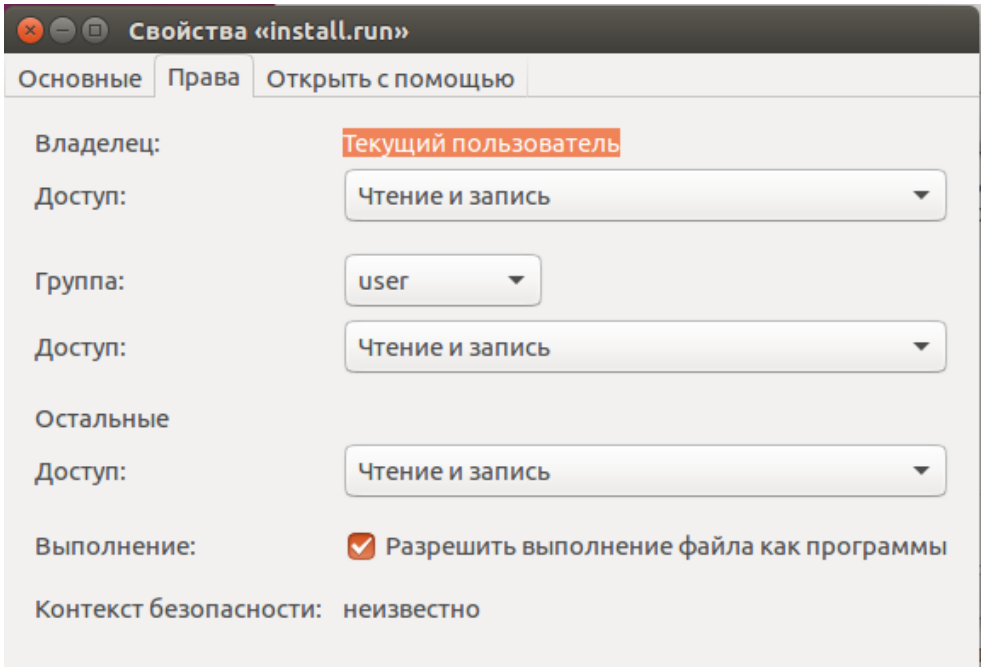


Рис. 80. Свойства файла

3. Открыть терминал и запустить установочный файл от имени администратора. Для этого необходимо выполнить команду «*sudo ./<имя установочного файла>*».
4. После запуска инсталлятора администратору необходимо ознакомиться с информацией, которая появится в окне терминала, и подтвердить согласие на установку Агента ШОС (рис. 81).

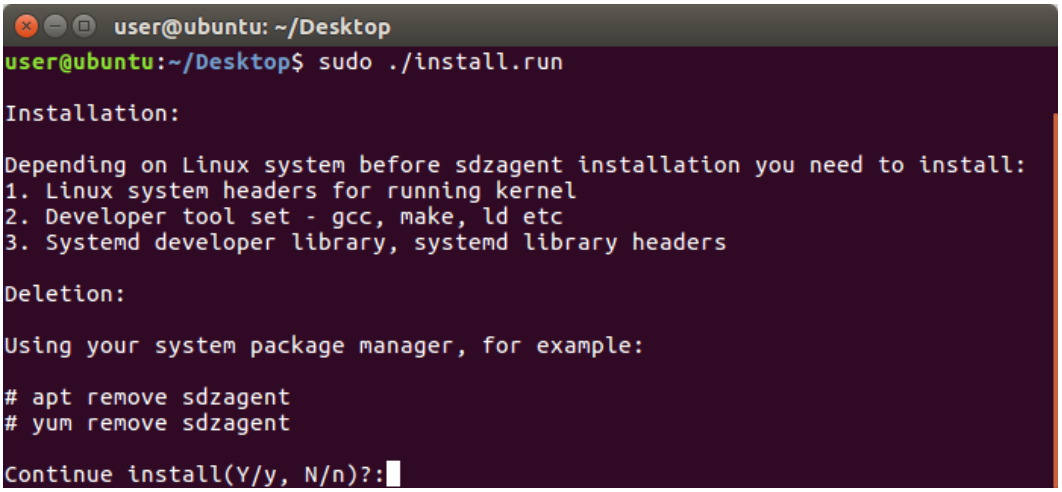


Рис. 81. Процесс установки Агента ШОС

5. Дождаться завершения процедуры установки и перезагрузить компьютер.

После установки Агент ШОС работает в фоновом режиме и постоянно поддерживает связь с СБ Dallas Lock. При отсутствии связи Агент ШОС пытается подключиться к СБ Dallas Lock с периодичность раз в минуту. События подключения и отключения Агента ШОС к СБ Dallas Lock фиксируются в журнале СБ.

Для ОС семейства Windows установленный Агент ШОС отображается в области уведомлений панели задач в виде значка. При наведении курсора мышки на данный значок появляется соответствующая информация о состоянии подключения с СБ (В Linux системах значок агента ШОС не отображается в системном трее.

Таблица 5).

В Linux системах значок агента ШОС не отображается в системном трее.

Таблица 5 — Информационные сообщения о состоянии подключения с СБ

Значок	Информационное сообщение
	Агент СДЗ Dallas Lock подключён к Серверу Безопасности
	Агент СДЗ Dallas Lock не подключён к Серверу Безопасности
	Плата СДЗ Dallas Lock не установлена или не удается получить данные с платы Dallas Lock

Примечание. При некоторых обновлениях ОС возможно изменение загрузчика, в таком случае пользователь, которому назначен запрет загрузки НШОС, после авторизации и перезагрузки увидит сообщение «Untrusted UEFI image» (Рис. 82) и не сможет продолжить загрузку ОС. В данном случае администратору безопасности необходимо убедиться в легитимности обновления ОС и переназначить загрузчик.

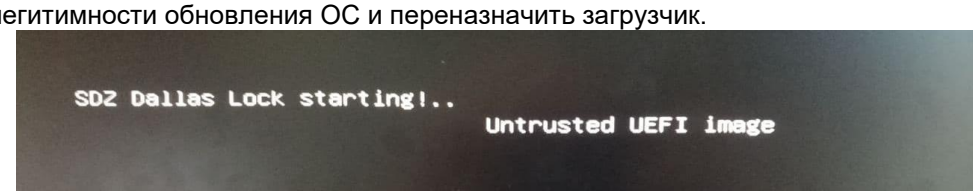


Рис. 82. Ошибка загрузки пользователя при обновлении ОС

3.6 Использование сервисной утилиты (восстановление заводских настроек)

Восстановление изделия к заводским настройкам возможно при помощи сервисной утилиты СДЗ Dallas Lock (рис. 83).

Данная утилита позволяет:

- посмотреть информацию о плате;
- применить/обновить прошивку;
- вернуть настройки платы в исходное состояние;
- сменить режим загрузки.

Утилита не предназначена для устранения неисправностей аппаратной составляющей изделия и не может быть использована в этом случае, необходимо обратиться к поставщику изделия.

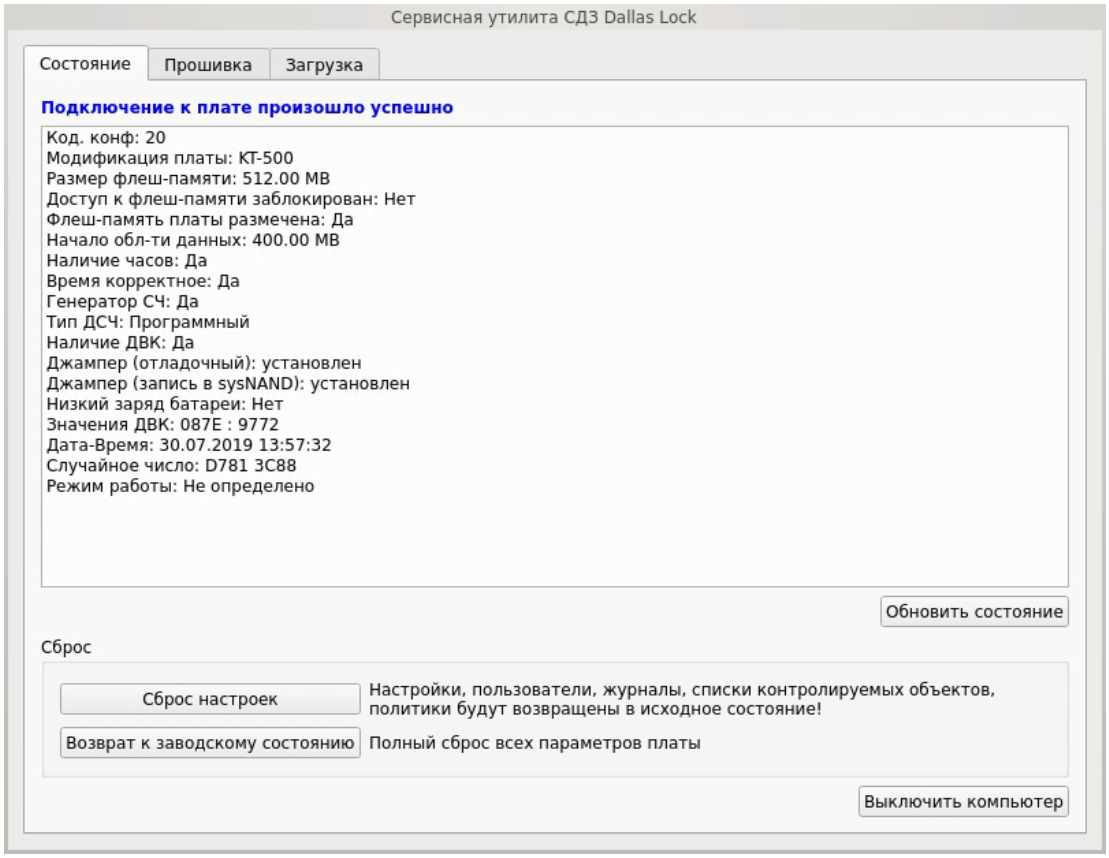


Рис. 83. Сервисная утилита

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 платах формата PCIe «КТ-500» и «КТ-500 r3» установить оба джампера на контакты «3» и «5» (рис. 1 и рис. 4). На платах формата miniPCIe-HalfSize «КТ-521» и «КТ-521 r3» и формата M.2 «КТ-550» и «КТ-550 r3» установить микропереключатели «2» и «3» в положение «ON» (рис. 2, рис. 5, рис. 3 и рис. 6 соответственно);

Примечание. Следует обратить внимание, что необходимо всегда включать/отключать оба джампера или микропереключателя.

- установить плату СДЗ Dallas Lock в системную плату ТС в свободный слот PCI-express/mini PCI-express/M.2;
- выполнить загрузку с флеш-накопителя с записанным ранее файл-образом. Сервисная утилита запустится автоматически.

3.6.2 Интерфейс сервисной утилиты

На вкладке «Состояние» приведены (рис. 83):

- таблица с выводом основной информации о подключенной к компьютеру плате: модификация платы, размер флеш-памяти платы, наличие и состояние аппаратных средств, состояние джамперов и прочее;
- «Обновить состояние» — происходит обновление таблицы;
- «Сброс настроек» — при нажатии все настройки СДЗ будут сброшены в исходное состояние, журналы очищены;

- «Возврат к заводскому состоянию» — при нажатии происходит полный сброс всех параметров платы;
- «Выключить компьютер» — при нажатии происходит выключение компьютера.

На вкладке «Прошивка» (рис. 84) 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 (для подробного описания процедуры обновления см. «Порядок обновления изделия»).
- «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.
- «Установить пакет дополнительных микрокодов устройств».

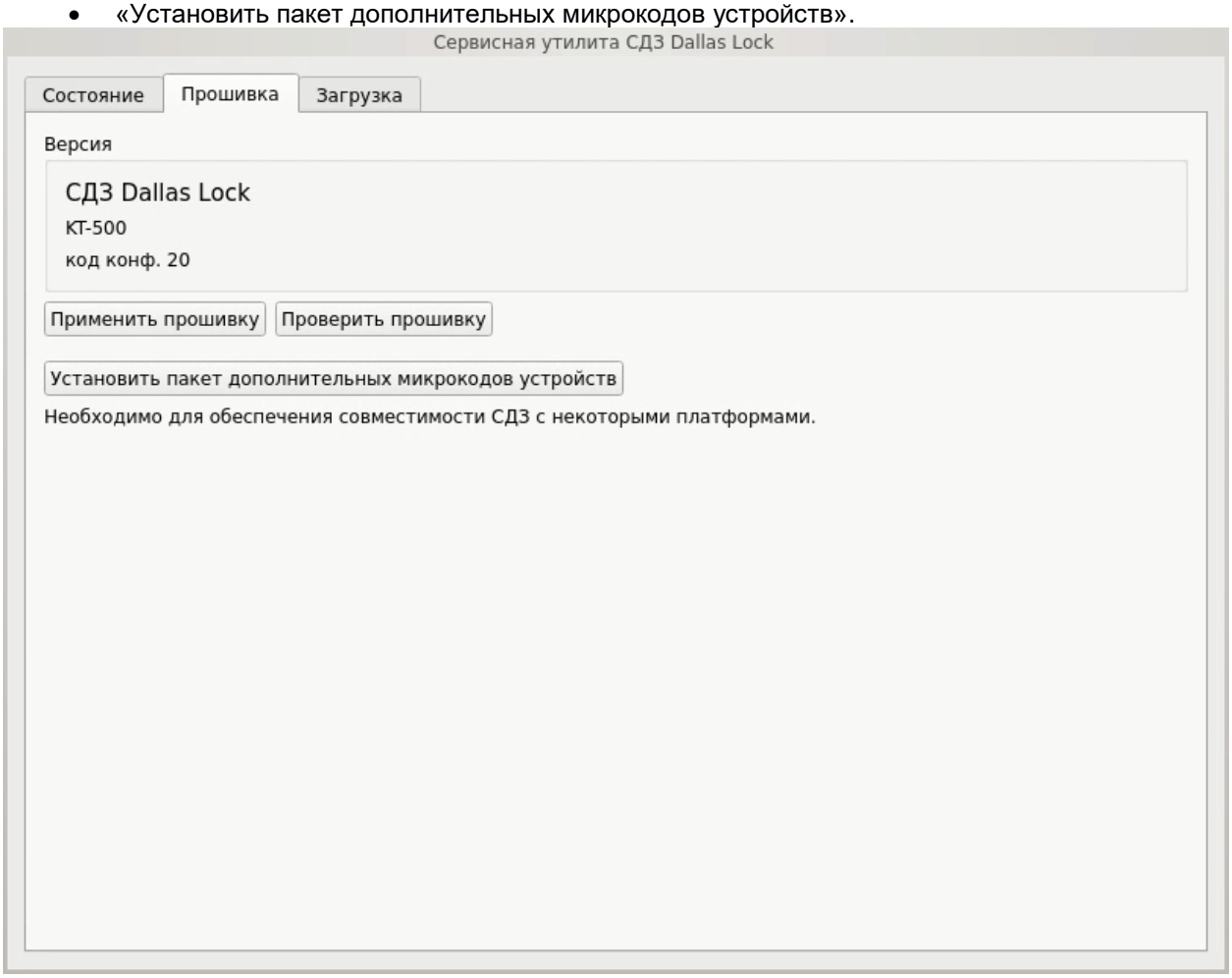


Рис. 84. Сервисная утилита. Вкладка «Прошивка»

На вкладке «Загрузка» (рис. 85) 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.
- «Передавать информацию загрузчику через NAND» — устанавливается для передачи информации в загрузчик среды исполнения прошивки СДЗ через NAND.

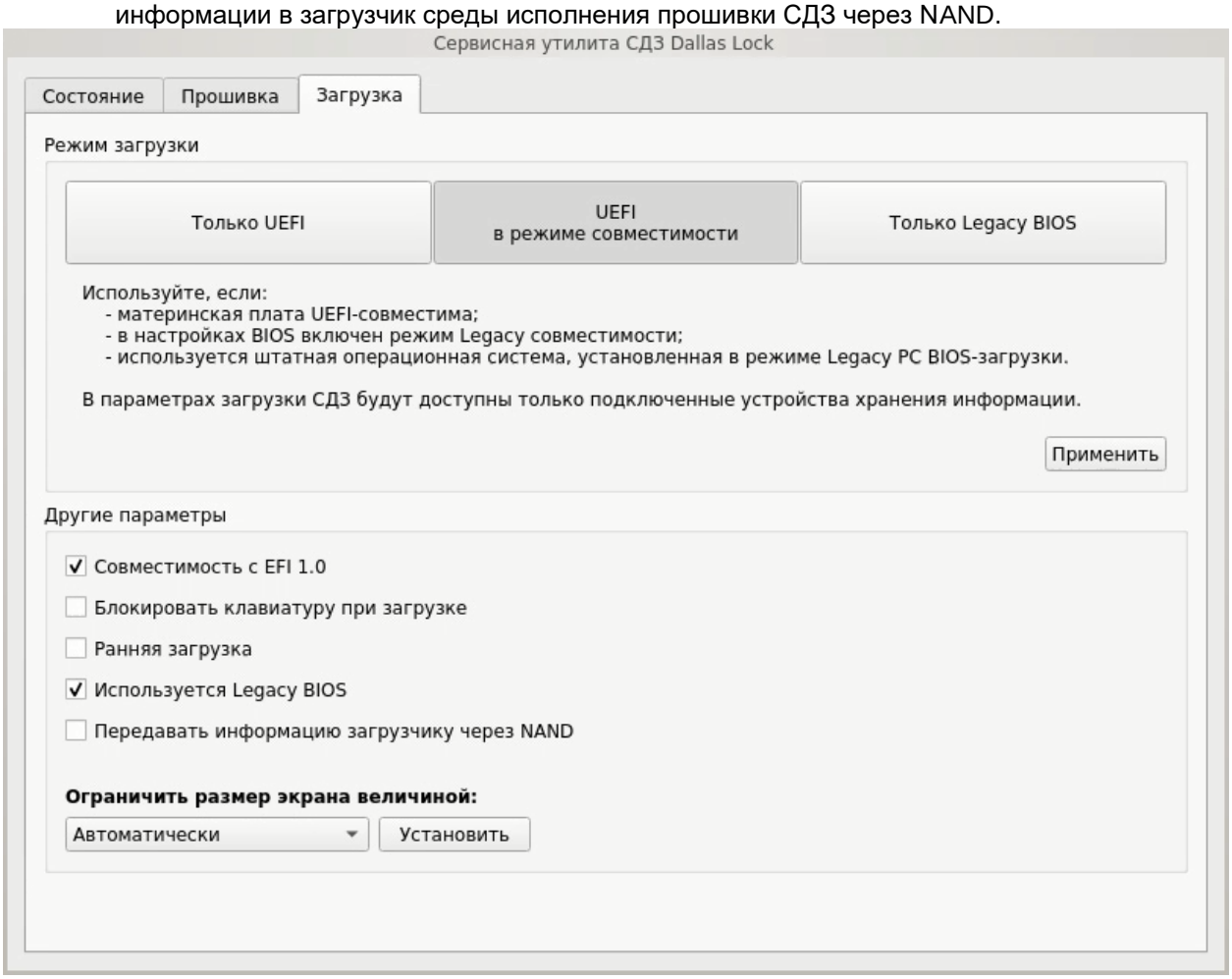


Рис. 85. Сервисная утилита. Вкладка «Загрузка»

3.7 Порядок обновления изделия

Обновление программной части изделия доступно через сервисную утилиту «KtService» на вкладке «Прошивка» (см. «Интерфейс сервисной утилиты») и осуществляется следующим образом:

- Предприятие-изготовитель доводит до потребителей информацию о выпуске обновлений изделия и устраненных в новых версиях недостатках по электронной почте письмом с вложенным документом, подписанным ЭП, о новом обновлении продукта и публикует информацию на сайте www.dallaslock.ru.
- Потребитель при получении указанной информации выполняет загрузку обновления с сайта предприятия-изготовителя в виде дистрибутива, информация о контрольной сумме которого содержится на сайте предприятия-изготовителя, а также файл электронной подписи.
- Перед установкой обновления потребитель выполняет проверку подлинности электронной подписи (согласно инструкции, представленной на сайте предприятия-изготовителя),

расчет[1] и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте предприятия-изготовителя.

- В случае успешной проверки электронной подписи и совпадения контрольных сумм, потребитель выполняет установку обновлений. Если проверка электронной подписи и контрольных сумм не пройдена, потребитель не выполняет установку обновлений и обращается к предприятию-изготовителю изделия.
- Для установки обновления необходимо запустить сервисную утилиту KtService, после чего убедиться, что разрешена запись в системную область энергонезависимой памяти СДЗ (см. «Запуск сервисной утилиты KtService»).
- Перейти на вкладку «Прошивка», выбрать действие «Применить прошивку», 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 прошивка 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 чекбоксы «Совместимость с EFI 1.0», «Блокировать клавиатуру при загрузке», «Ранняя загрузка» и «Используется Legacy BIOS» при необходимости (см. «Интерфейс сервисной утилиты»);
  - 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 чекбоксы «Совместимость с EFI 1.0», «Блокировать клавиатуру при загрузке» и «Ранняя загрузка» при необходимости (см. «Интерфейс сервисной утилиты»);
  - 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 плат формата PCIe «КТ-500» и «КТ-500 r3» джамперы, на платах формата miniPCIe-HalfSize «КТ-521» и «КТ-521 r3» и формата M.2 «КТ-550» и «КТ-550 r3» установить микропереключатели в положение «OFF».

3.8 Перечень возможных неисправностей в процессе использования

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

3.9 Порядок выполнения контроля работоспособности изделия

Контроль работоспособности изделия осуществляется в ходе проведения приемо-сдаточных испытаний в объеме, предусмотренном в Технических условиях ПФНА.501410.003 ТУ.

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

3.10 Порядок выключения изделия

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

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

Извлечение СДЗ Dallas Lock из системной платы осуществлять только при выключенном питании ТС. При извлечении СДЗ Dallas Lock, а также при техническом обслуживании ТС избегать возможных повреждений элементов, выступающих над поверхностью печатной платы изделия.

4 ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ

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

Техническое обслуживание изделия производить только при отключенном электропитании ТС, в котором он установлен.

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

При возникновении неисправностей, вызванных конфликтом ПО ТС 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.

5 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.