УТВЕРЖДЕН
ПФНА.501410.003 32-ЛУ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ

Dallas Lock

(версия изделия 348.1)

Руководство системного программиста (администратора)

ПФНА.501410.003 32

Листов 66

СОДЕРЖАНИЕ

АННОТАЦИЯ

Настоящее руководство системного программиста (администратора) распространяется на изделие «Средство доверенной загрузки «Dallas Lock» (далее по тексту — изделие, СДЗ Dallas Lock).

Документ предназначается для системных администраторов и аудиторов СДЗ Dallas Lock.

Администратор — пользователь, ответственный за управление СДЗ Dallas Lock. Входит в группу пользователей «Администраторы». Функцию администратора могут выполнять несколько сотрудников подразделения информационной безопасности предприятия.

Аудитор — пользователь, имеющий права на просмотр всех установленных параметров безопасности СДЗ Dallas Lock без возможности их редактирования. Входит в группу пользователей «Аудиторы».

Пользователь — пользователь защищённого персонального компьютера, осуществляющий ввод и обработку информации любыми программными средствами. Входит в группу «Пользователи».

В разделе «Общие сведения о СДЗ Dallas Lock» указаны функции программно-аппаратного изделия и сведения о технических и программных средствах, обеспечивающих работу данного изделия.

В разделе «Структура СДЗ Dallas Lock» приведены сведения о структуре изделия.

В разделе «Установка и настройка СДЗ Dallas Lock» приведено описание действий по предварительной подготовке и настройке изделия.

В разделе «Проверка системы защиты» приведено описание способов проверки, позволяющих дать общее заключение о работоспособности СДЗ Dallas Lock.

ТЕРМИНЫ И СОКРАЩЕНИЯ

АИ	аппаратный идентификатор
АС	автоматизированная система
ДСЧ	датчик случайных чисел
ДВК	датчик вскрытия корпуса
ЕЦУ	Единый центр управления
КС	контрольная сумма
КСБ	Консоль Сервера безопасности
НШОС	нештатная операционная система
ОА	оболочка администратора
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
ЦП	центральный процессор
ШОС	штатная операционная система

1 ОБЩИЕ СВЕДЕНИЯ О СДЗ DALLAS LOCK

1.1 Назначение

Изделие предназначено для блокирования попыток несанкционированной загрузки НШОС, а также для предоставления доступа к информационным ресурсам в случае успешной проверки подлинности загружаемой ШОС.

Изделие предназначено для использования на различных технических средствах (далее — ТС) архитектуры Intel x64, таких как персональные и портативные компьютеры, серверы.

Использование СДЗ Dallas Lock при проектировании систем защиты информации позволяет привести АС в соответствие требованиям законодательства Российской Федерации.

1.2 Функции

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;

— 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 СДЗ Dallas Lock при возникновении сбоев и ошибок в процессе работы;

— обеспечение безопасности после завершения работы СДЗ Dallas Lock.

1.3 Технические характеристики

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,

---

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

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

```
$ pkcs15-init --erase-card
$ pkcs15-init --create-pkcs15 --so-pin "<ПИН администратора>" --so-puk "" --pin "<ПИН пользователя>"
$ pkcs15-init --store-pin --label "<имя АИ>" --auth-id 02 --pin "<ПИН пользователя >" --puk ""
```

[3] При подключении считывателя Touch Memory непосредственно к СДЗ Dallas есть возможность работы с памятью электронных ключей iButton (DS-1992, DS-1993, DS-1995, DS-1996) для хранения идентификационной и аутентификационной информации учётной 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.

JaCarta-2 ГОСТ, JaCarta PKI).

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

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

СДЗ Dallas Lock позволяет контролировать целостность реестра ОС Windows.

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

— получение остаточной информации СДЗ Dallas Lock из памяти ТС после завершения 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.

1.4 Требования к аппаратной составляющей

СДЗ Dallas Lock исправно работает на ТС архитектуры Intel x64. Минимальные аппаратные требования к компьютеру для установки СДЗ Dallas Lock:

— процессор Pentium с частотой 300 МГц;

— не менее 512 МБ оперативной памяти;

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

— наличие свободных портов USB, если изделие используется совместно с аппаратными идентификаторами (за исключением случаев, когда в качестве 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, манипулятор типа «мышь» или совместимое указывающее устройство;

— видеоадаптер и монитор, поддерживающие режим SVGA 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.

1.5 Процедуры приемки пользователем

Обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования, реализуется при помощи процедур верификации. В данном разделе описываются методы уникальной маркировки и связанные с ними компоненты для обеспечения пользователей возможностью идентифицировать СДЗ Dallas Lock и убедиться в том, что они используют сертифицированное (оцененное) средство доверенной загрузки и сопутствующую документацию.

1.5.1 Упаковка изделия при поставке

Упаковка изделия осуществляется в тару, обеспечивающую защиту и сохранность при транспортировании и хранении изделия согласно требованиям раздела 6 Технических условий ПФНА.501410.003 ТУ. Компакт-диск с документацией на изделие, проверенный на отсутствие царапин, сколов и других механических повреждений, помещается в футляр.

В упаковку вкладывается плата, кабель сторожевого таймера, формуляр, копия сертификата соответствия, краткое руководство пользователя, монтажная планка (полноформатная) и винты для крепления (только для плат PCIe «КТ-500» и «КТ-500 r3»), диск в футляре с обложкой. По заказу также вкладывается считыватель, аппаратный идентификатор, аппаратный датчик случайных чисел, монтажная планка (низкопрофильная), расширитель с Mini PCI-E Half в Full Size, датчик вскрытия корпуса, плата RTC с батарейкой и кабель для подключения платы RTC. Подробно комплектность СДЗ Dallas Lock указана в таблица 1.

Таблица 1 — Комплектность СДЗ Dallas Lock

Наименование	Обозначение	Кол-во, шт.	Заводской уч. номер	Примечание
Плата СДЗ Dallas Lock	ПФНА.501410.003-01	1		в зависимости от исполнения
	ПФНА.501410.003-02			
	ПФНА.501410.003-04			
	ПФНА.501410.003-09			
	ПФНА.501410.003-10			
	ПФНА.501410.003-11			
Кабель	ПФНА.501410.003-05	1		кабель для подключения сторожевого таймера, в зависимости от исполнения
	ПФНА.501410.003-06			
Формуляр	ПФНА.501410.003 ФО	1		печатный вариант
Краткое руководство пользователя		1		-/-
Описание применения	ПФНА.501410.003 31	1		на компакт-диске

Наименование	Обозначение	Кол-во, шт.	Заводской уч. номер	Примечание
Руководство по эксплуатации	ПФНА.501410.003 РЭ	1		-/-
Руководство оператора (пользователя)	ПФНА.501410.003 34	1		-/-
Руководство системного программиста (администратора)	ПФНА.501410.003 32	1		-/-
Сервисная утилита (файл-образ)		1		-/-
Файл прошивки СДЗ Dallas Lock		1		-/-
Драйверы платы КТ		1		-/-
Агент ШОС		1		-/-
Компакт-диск		1		
Копия сертификата соответствия Системы сертификации средств защиты информации Министерства обороны Российской Федерации по требованиям безопасности информации № РОСС RU.0001.01БИ00		1		печатный вариант
Идентификатор СЗИ		1		вклеен в раздел 5 формуляра на изделие
Упаковка		1		
Монтажная планка (полноформатная)		1		для плат PCIe «КТ-500» и «КТ-500 r3»
Винты для крепления монтажной планки (2 штуки, 3x6)		1		-/-
Аппаратный идентификатор iButton				определяется договором
Аппаратный идентификатор USB-ключ/смарт-карта JaCarta SF/ГОСТ				-/-
Аппаратный идентификатор USB-ключ/смарт-карта Рутокен ЭЦП				-/-
Считыватель Touch Memory (USB)				-/-
Считыватель Touch Memory	ПФНА.501410.003-07			для плат PCIe «КТ-500» и «КТ-500 r3», определяется договором
Кабель для подключения считывателя Touch Memory (RJ11)	ПФНА.501410.003-08			-/-
Считыватель Touch Memory с коаксиальным кабелем				для плат miniPCIe-HS «КТ-521 r3» и M.2 «КТ-550 r3», определяется договором

Наименование	Обозначение	Кол-во, шт.	Заводской уч. номер	Примечание
Аппаратный датчик случайных чисел				для плат PCIe «КТ-500 r3», miniPCIe-HS «КТ-521 r3» и M.2 «КТ-550 r3», определяется договором
Монтажная планка (низкопрофильная)				-/-
Датчик вскрытия корпуса				для плат PCIe «КТ-500» и «КТ-500 r3», miniPCIe-HS «КТ-521 r3» и M.2 «КТ-550 r3», определяется договором
Расширитель с Mini PCI-E Half в Full				для плат miniPCIe-HS «КТ-521» и «КТ-521 r3», определяется договором
Плата RTC с батарейкой				для плат miniPCIe-HS «КТ-521 r3» и M.2 «КТ-550 r3», определяется договором
Кабель для подключения платы RTC				-/-

Список компонентов для проверки пользователем при поставке:

— СДЗ Dallas Lock в упаковке, маркированной в установленном порядке;

— компакт-диск в футляре, маркированный в установленном порядке, с записанной на нем эксплуатационной документацией (см. Таблица 1);

— печатные копии документов (см. Таблица 1);

— аппаратные идентификаторы ruToken, eToken, iButton, JaCarta, eSmart (если предусмотрены договором, контрактом);

— считыватель, аппаратный датчик случайных чисел, монтажная планка (низкопрофильная), расширитель с Mini PCI-E Half в Full Size, датчик вскрытия корпуса, плата RTC с батарейкой и кабель для подключения платы RTC (если предусмотрены договором, контрактом).

1.5.2 Маркировка изделия при поставке

Маркировка изделия производится в соответствии с требованиями настоящего документа, а также технических условий ПФНА.501410.003 ТУ и включает в себя маркировку печатной платы СДЗ Dallas Lock, упаковки изделия, футляра компакт-диска и формуляра.

Маркировка в формуляре ПФНА.501410.003 ФО соответствует требованиям технической документации предприятия-изготовителя, наносится ручным способом и содержит:

— товарный знак предприятия-изготовителя;

— заводской (учётный) порядковый номер изделия (для верификации аппаратной части изделия заводской номер наносится на печатную плату СДЗ Dallas Lock и на печатную копию формуляра, поставляемого в составе комплекта СДЗ Dallas Lock);

— идентификатор СЗИ (вклеен в разделе 5 «Свидетельство об упаковывании и приемке» в поле «Маркирован идентификатором»);

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

— соответствующие подписи и печати.

Примечания.

Идентификатор СЗИ – идентификатор средства защиты информации, является уникальным параметром для каждого экземпляра изделия, указывается в формуляре изделия, наносится на корпус изделия.

Идентификатор СЗИ имеет следующий формат РОСС RU.01.YYYY.XXXXXX, где:

— *первая группа знаков содержит прописные буквы и цифры РОСС RU.01, указывающие на систему сертификации ФСТЭК России;*

— *вторая группа знаков указывает на номер сертификата соответствия Изделия в системе сертификации ФСТЭК России;*

— *третья группа знаков указывает на номер лицензии в системе учета средств защиты информации, произведенных ООО «Конфидент».*

Маркировка на футляр компакт-диска изделия наносится печатным способом на обратную сторону обложки футляра и содержит идентификатор СЗИ.

Идентификатор СЗИ регистрируется предприятием-изготовителем в «Журнале учета выпущенных изделий и учета идентификаторов СЗИ».

1.5.3 Инструкция по снятию и сверке КС

Для возможности верификации файла прошивки СДЗ Dallas Lock, поставляемого на компакт-диске, необходимо произвести расчет КС:

— с использованием программы ФИКС 2.0.1 (Fix-2.0.1) (разработчик — ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 913 от 28.05.2004) по алгоритму КС «Уровень-3»;

— с использованием программы фиксации и контроля исходного состояния, автоматизированного контроля целостности информационных массивов «Трафарет 2.0» (сертификат соответствия ФСТЭК России № 2031 от 03.02.2010).

Произвести сверку полученных КС с указанными в формуляре на изделие (ПФНА.501410.003 ФО).

1.5.4 Верификация программного обеспечения

Для идентификации программной части СДЗ Dallas Lock выполняется нумерация сборки. Для верификации версии СДЗ Dallas Lock необходимо выполнить следующие действия:

— запустить оболочку администратора СДЗ Dallas Lock;

— перейти на вкладку «Параметры»;

— в панели «Версия» отображается полный номер версии ОО.

Процедура верификации файла прошивки изделия осуществляется при помощи сервисной утилиты, поставляемой на компакт диске в формате файл-образа «KtService.img».

После запуска утилиты нажать кнопку «Проверить прошивку». Далее необходимо выбрать файл прошивки, поставляемый на компакт диске, после чего будет выведена информация о

соответствии или не соответствии прошивки. Подробное описание использования сервисной утилиты см. п.п. 3.2.9 настоящего руководства.

2 СТРУКТУРА СДЗ DALLAS LOCK

СДЗ Dallas Lock состоит из:

— аппаратной части;

— прошивки (программной части).

2.1 Аппаратная часть СДЗ Dallas Lock

Аппаратная часть СДЗ Dallas Lock представляет собой печатную плату:

— PCIe «КТ-500» (ПФНА.501410.003-01) (рисунок 1);

— miniPCIe-HS «КТ-521» (ПФНА.501410.003-02) (рисунок 2);

— M.2 «КТ-550» (ПФНА.501410.003-04) (рисунок 3);

— PCIe «КТ-500 r3» (ПФНА.501410.003-09) (рисунок 4);

— miniPCIe-HS «КТ-521 r3» (ПФНА.501410.003-10) (рисунок 5);

— M.2 «КТ-550 r3» (ПФНА.501410.003-11) (рисунок 6).

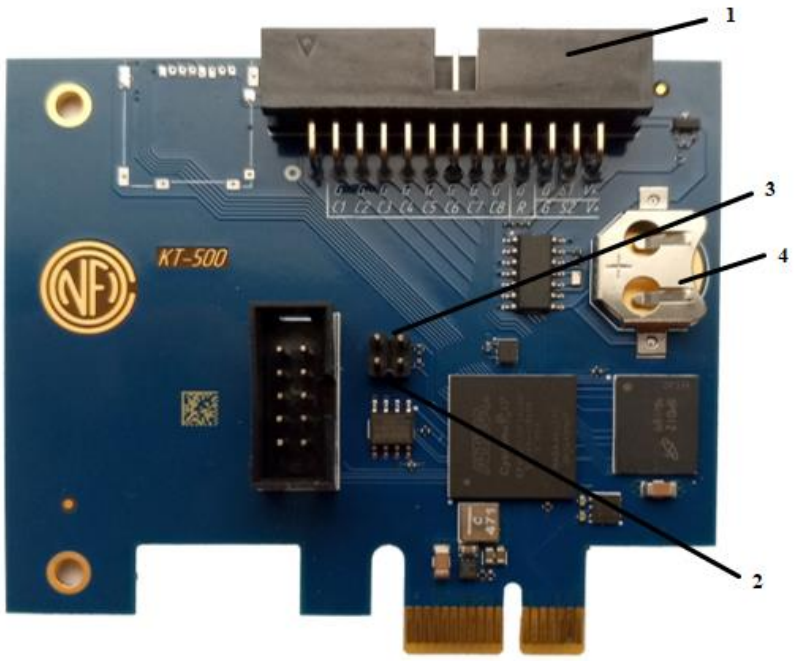


Рисунок 1 — Расположение основных элементов **«КТ-500»**

(1 — Группа штыревых разъемов для подключения датчиков вскрытия корпуса, цепи системного сброса, считывателя Touch Memory (или кабеля для подключения считывателя Touch Memory через разъем RJ11 ПФНА.501410.003-08);
2 — 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 в положении переключателя «ON»;
4 — Разъем для литиевой батареи CR1220/ CR1225 часов реального времени и блока контроля вскрытия корпуса

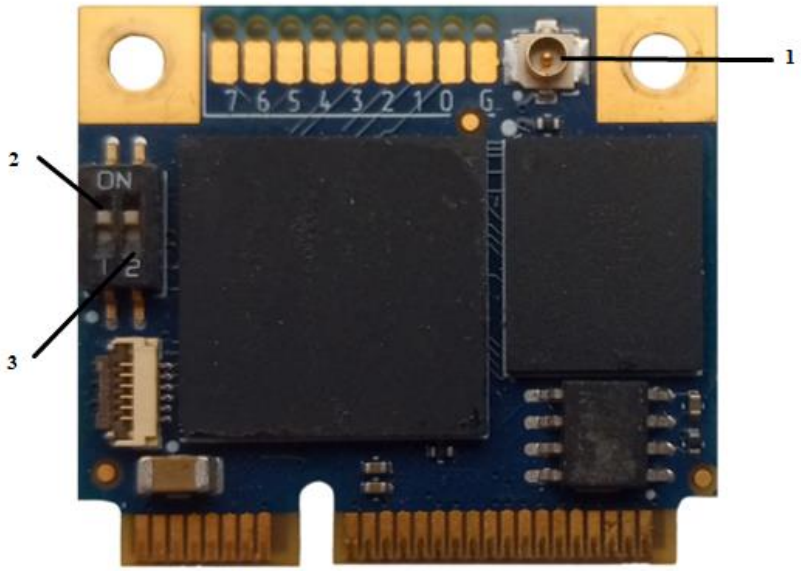


Рисунок 2 — Расположение основных элементов **«КТ-521»**

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

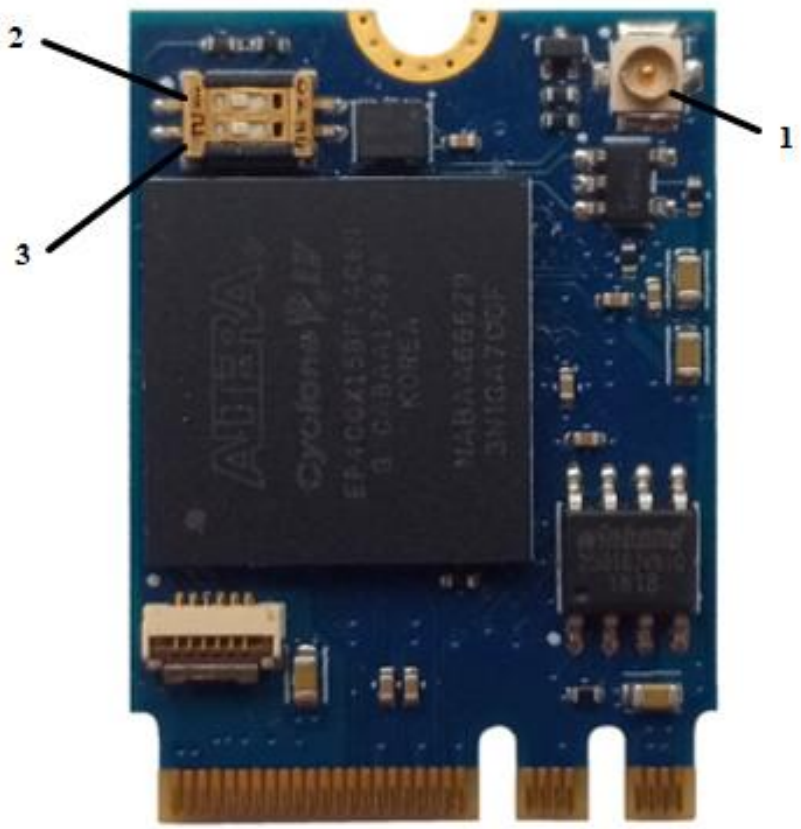


Рисунок 3 — Расположение основных элементов **«КТ-550»**

(1 — Коаксиальный разъем для подключения «сторожевого таймера»;

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

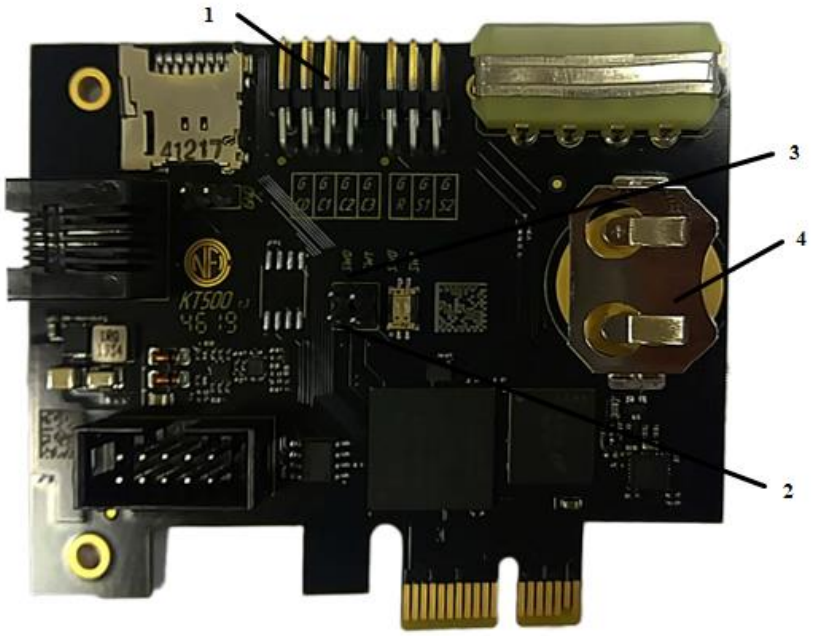


Рисунок 4 — Расположение основных элементов **«КТ-500 r3»**

(1 — Группа штыревых разъемов для подключения датчиков вскрытия корпуса, цепи системного сброса, считывателя Touch Memory (или кабеля для подключения считывателя Touch Memory через разъем RJ11 ПФНА.501410.003-08);
2 — 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 в положении переключателя «ON»;
4 — Разъем для литиевой батареи CR1220/ CR1225 часов реального времени и блока контроля вскрытия корпуса

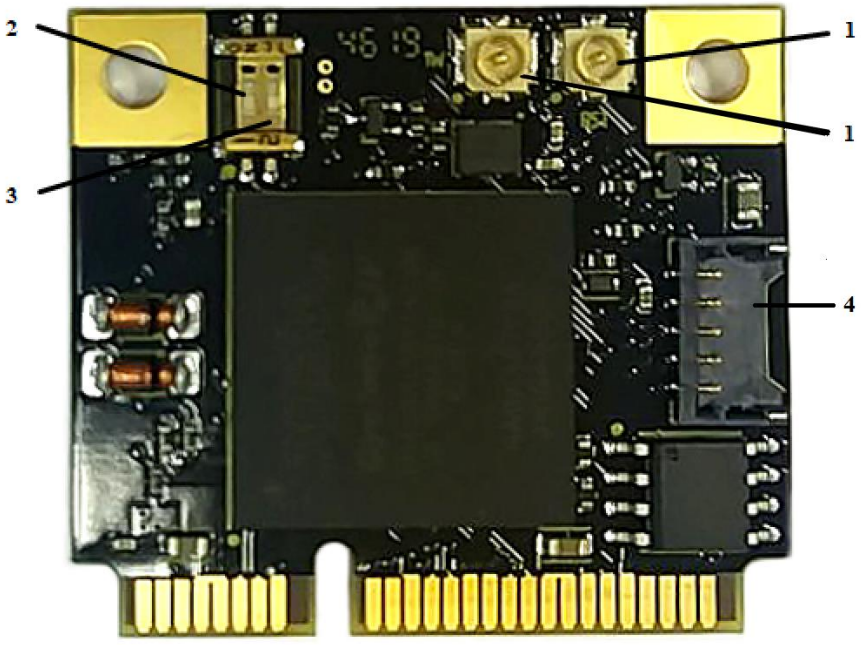


Рисунок 5 — Расположение основных элементов **«КТ-521 r3»**

(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)

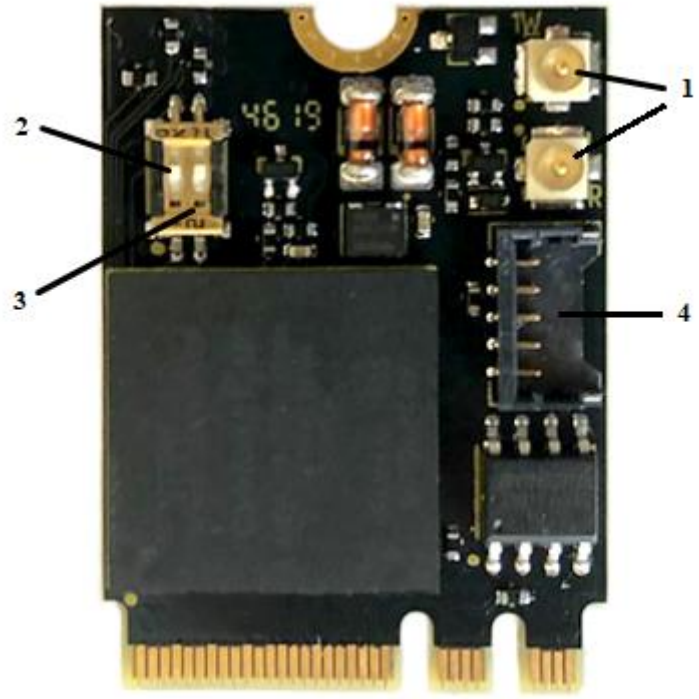


Рисунок 6 — Расположение основных элементов **«КТ-550 r3»**

(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)

2.2 Прошивка (программная часть) СДЗ Dallas Lock

Прошивка (программная часть) СДЗ состоит из следующих компонентов:

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

2.2.1 Загрузчик среды исполнения

Обеспечение получения управления над процессом загрузки компьютера. Его задача — выполнить чтение кода среды исполнения функций безопасности из памяти платы и передать ей управление.

2.2.2 Среда исполнения функций безопасности

Обеспечение работоспособности организационных функций безопасности, для чего среда исполнения предоставляет следующие сервисы:

- запуск оболочки функций безопасности;
- обеспечение доступа к файловым системам ШОС;
- обеспечение доступа к USB-устройствам;
- получение сведений о конфигурации ТС, текущего времени;
- вывод графики на экран ТС;
- обеспечение доступа к энергонезависимой памяти платы для чтения/сохранения параметров и журнала;
- обеспечение доступа к функции перезагрузки/выключения ТС;
- возможность управления манипулятором типа «мышь»;
- поддержка системных плат BIOS и UEFI;
- загрузка ШОС.

2.2.3 Оболочка функций безопасности

Реализует функционал СДЗ Dallas Lock, связанный с основной задачей, и состоит из следующих подсистем:

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

3 УСТАНОВКА И НАСТРОЙКА СДЗ DALLAS LOCK

3.1 Предварительная подготовка

Перед эксплуатацией СДЗ Dallas Lock необходимо внимательно ознакомиться с комплектом документации на данную систему.

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

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

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

- включить режим UEFI Boot (Enabled);
- отключить режим CSM (Disabled);
- отключить режим FastBoot (Disabled);
- в Setup BIOS удалить установленные ключи для SecureBoot и затем установить ключи, расположенные на диске, идущем в комплекте с изделием, в следующем порядке: db.auth, KEK.auth, PK.auth.

Примечание — Для замены ключей для SecureBoot можно воспользоваться утилитой KeyTool.efi.

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

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

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

- отключить режим FastBoot (Disabled).

Примечания

1 Плата СДЗ Dallas Lock по умолчанию загружается в режиме «Только UEFI». Поменять режим загрузки платы СДЗ Dallas Lock можно с помощью сервисной утилиты KtService (см. п.п. 3.2.9).

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

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

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

Уполномоченным администратором производится установка аппаратной части СДЗ Dallas Lock в свободный слот PCI-express / mini PCI-express / M.2 при выключенном питании.

В СДЗ Dallas Lock реализован беспроводной (программный) «сторожевой таймер». При наличии разъемов «Reset» или «Power» рекомендуется подключать «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», 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 (см. рисунок 2, рисунок 3, рисунок 5 и рисунок 6 соответственно), на ТС — к разъему «Reset» («Power»)).

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

Для подключения датчиков вскрытия корпуса (ДВК):

— на платах «КТ-500» используются штыревые разъемы «V+», «S1» и «S2» (рисунок 7);

— на платах «КТ-500 r3» используются штыревые разъемы «G», «S1» и «S2» (рисунок 7);

— на платах «КТ-521 r3» и «КТ-550 r3» необходимо подключить плату RTC (плата часов реального времени)[1] с помощью кабеля (п. 4 рисунок 5 и рисунок 6), после подключить к ней ДВК.

Для корректной работы ДВК и «сторожевого таймера» на платах 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) (рисунок 7);

— на платах «КТ-521 r3» и «КТ-550 r3» используется коаксиальный разъем (п.1 рисунок 5 и рисунок 6).

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

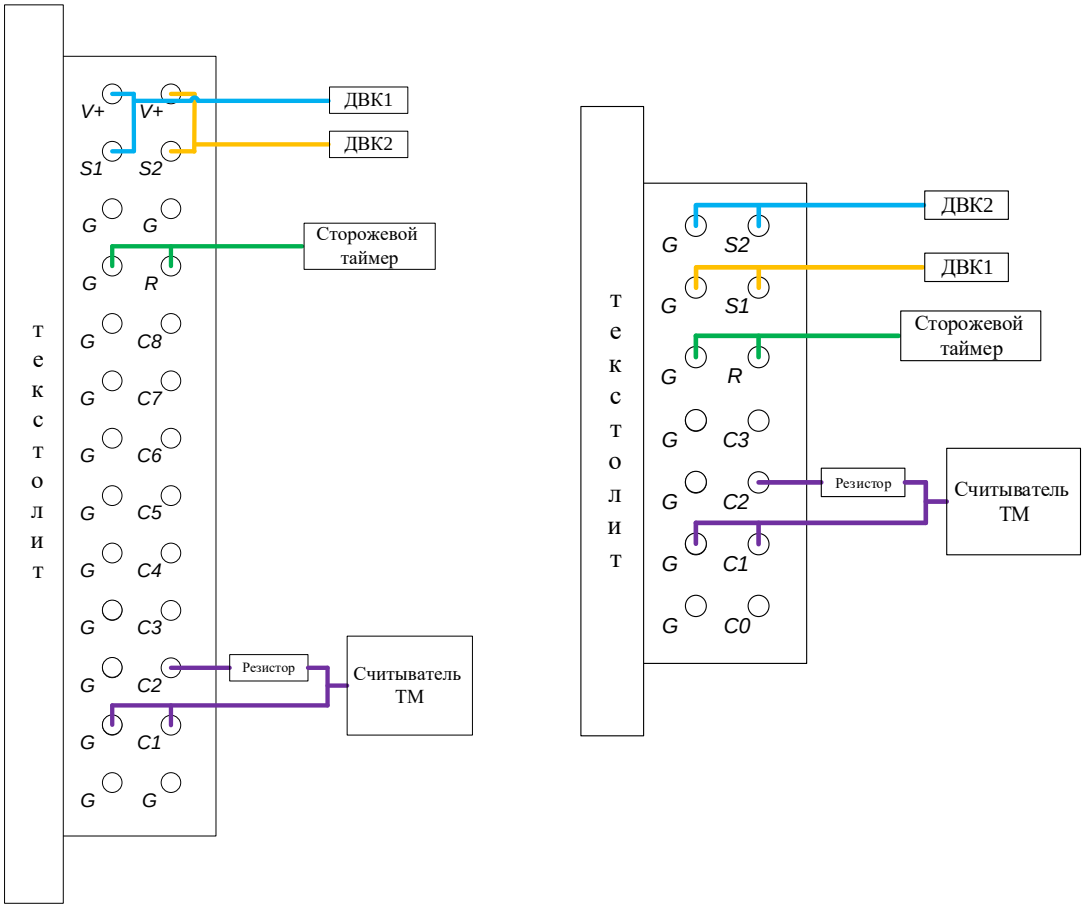


Рисунок 7 — Схема подключения ДВК, сторожевого таймера и считывателя Touch Memory к штыревым разъемам на платах «КТ-500» и «КТ-500 r3» соответственно

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

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

— работы функции автовхода по авторизационным данным из СДЗ Dallas Lock в ШОС, защищенную СЗИ Dallas Lock 8.0;

— работы службы Агента ШОС (см. п.п. Запуск Агента ШОС);

— использования часов плат «КТ-500» и «КТ-500 r3» при регистрации времени событий в журналах СЗИ Dallas Lock 8.0.

3.2 Настройка СДЗ Dallas Lock

После установки платы СДЗ Dallas Lock в слот расширения системной платы ТС включается электропитание системного блока (ноутбука, моноблока), осуществляется включение ТС.

СДЗ Dallas Lock может работать в одном из двух режимов:

— базовый режим работы — доступны гибкие настройки политик авторизации пользователей, работа с локальными и доменными учетными записями пользователей, локальное и удаленное управление платой СДЗ;

— усиленный режим работы[1] — устанавливается принудительная двухфакторная идентификация для всех учетных записей пользователей, возможна работа только с локальными учетными записями пользователей и локальное управление платой СДЗ.

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

Рисунок 8 — Выбор режима работы СДЗ Dallas Lock

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

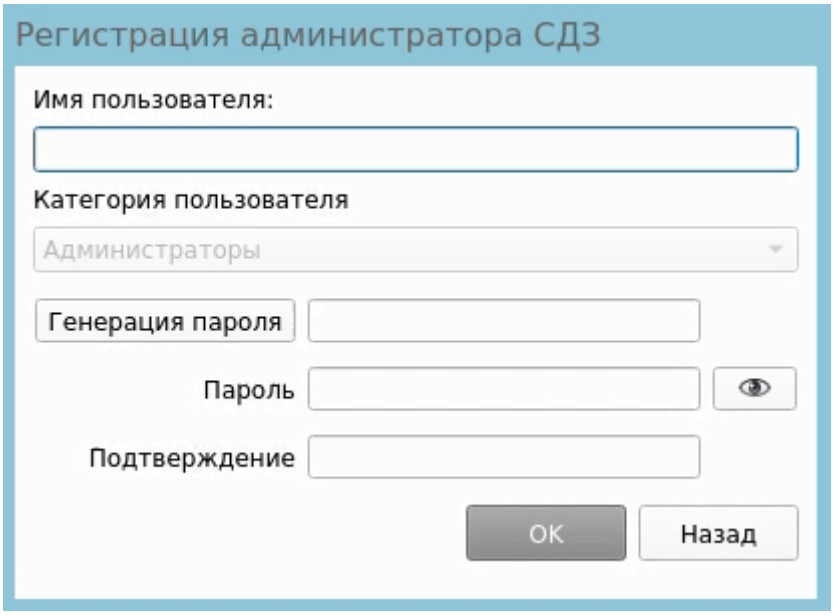


Рисунок 9 — Регистрация администратора СДЗ Dallas Lock

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

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

— первичная регистрация (рисунок 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;

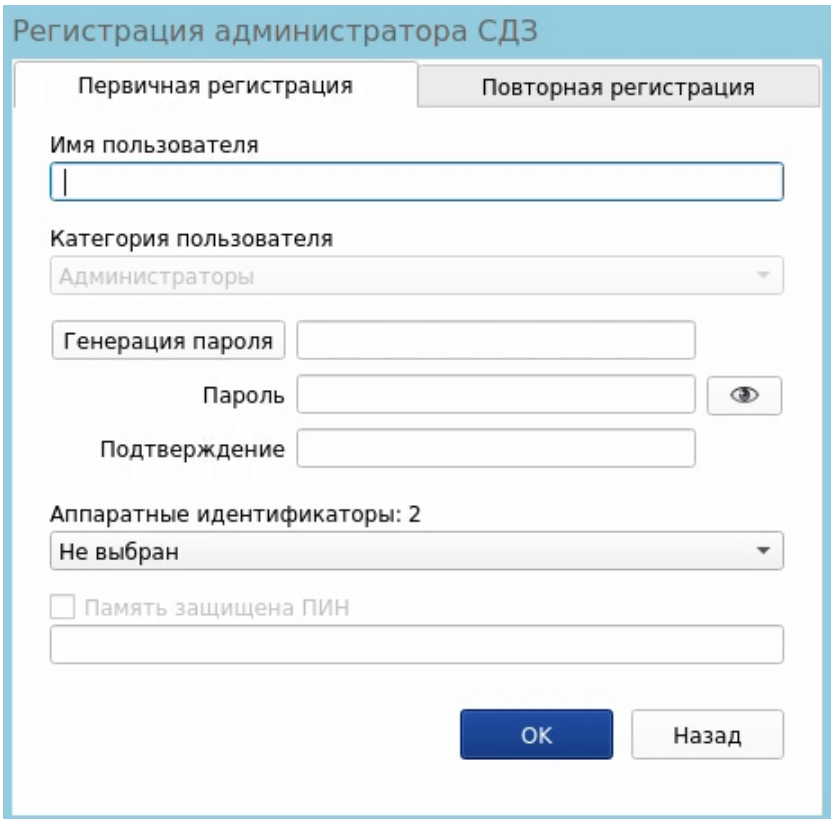


Рисунок 10 — Первичная регистрация администратора СДЗ Dallas Lock

— повторная регистрация (рисунок 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.

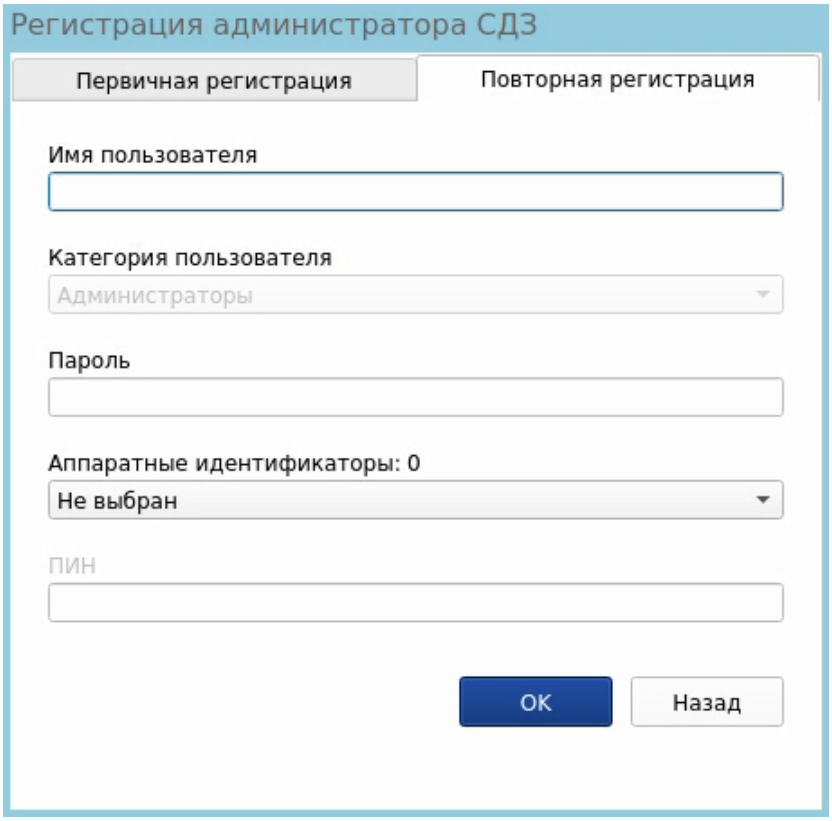


Рисунок 11 — Повторная регистрация администратора СДЗ Dallas Lock

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 (рисунок 12).

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

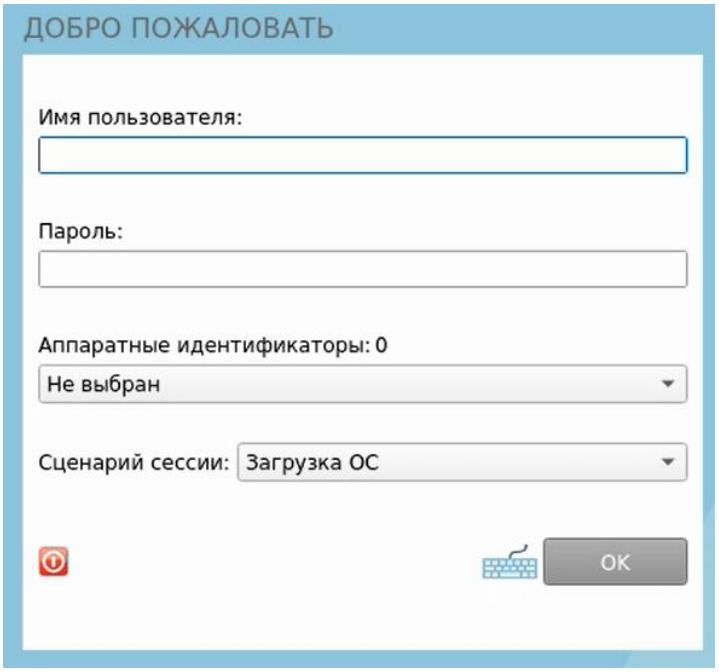


Рисунок 12 — Экран приглашения на вход в систему

Примечание — Если защищенный СДЗ Dallas Lock компьютер введен в Домен безопасности, в левом нижнем углу экрана приглашения на вход, рядом со значком выведено соответствующее сообщение: «Соединение с СБ установлено» или «Соединение с СБ не установлено».

Для входа на защищенный СДЗ Dallas Lock компьютер необходимо:

— предъявить АИ, если он назначен учётной записи пользователя (подробное описание авторизации с использованием АИ описано в документе «Руководство по эксплуатации» ПФНА.501410.003 РЭ);

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

Примечания

1 Ввод имени доменной учётной записи пользователя должен производиться в одном из следующих форматов:

- [dom]\[name], где [dom] — полное или короткое имя домена, [name] — имя учётной записи;
- [name]@[dom], где в качестве значения [dom] используется только полное имя домена.

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

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

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

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

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

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

— выбрать в выпадающем списке допустимую для учётной записи пользователя операцию по работе с системой:

- «Загрузка ОС» — переход к загрузке ШОС;
- «Смена пароля» — переход к смене пароля текущей учётной записи пользователя;
- «Администрирование» — запуск оболочки администратора СДЗ Dallas Lock (действие доступно только для пользователей категорий «Администраторы» и «Аудиторы»);

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

После успешной авторизации осуществляется переход к процедуре контроля целостности объектов, указанных в СДЗ Dallas Lock. При успешном прохождении данной процедуры выводится соответствующее сообщение (рисунок 13) и запуск оболочки администратора (ОА).

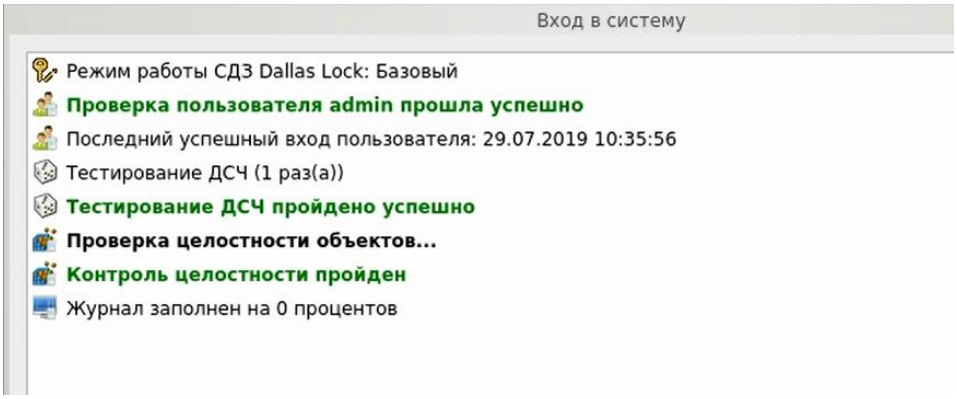


Рисунок 13 — Пример окна сообщения при успешном прохождении контроля целостности

В главном окне оболочки администратора (рисунок 14) расположены вкладки, обеспечивающие доступ к соответствующим разделам:

— «Пользователи» — управление учётными 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.

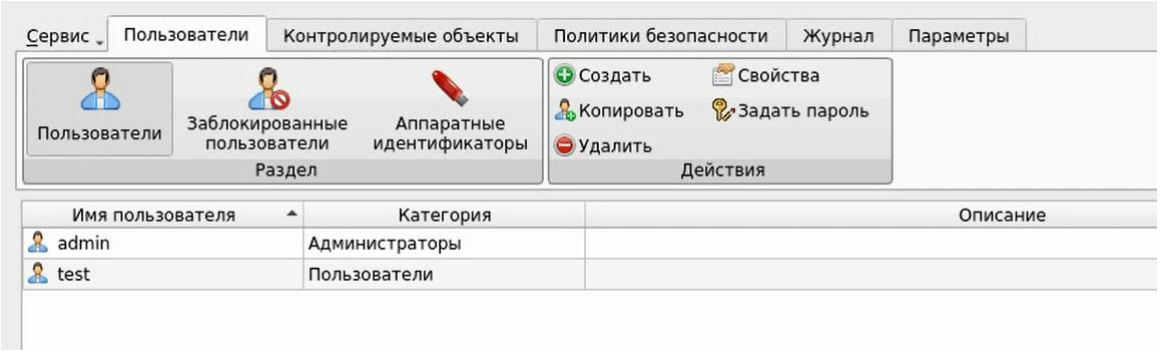


Рисунок 14 — Главное окно. Пользователи

3.2.1 Управление учётными записями пользователей

Раздел «Пользователи»

В разделе **«Пользователи»** в виде таблицы отображаются все учётные 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 учётными записями пользователей:

— «Создать»;

— «Копировать»;

— «Удалить»;

— «Свойства»;

— «Задать пароль».

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

При нажатии кнопки «Свойства» выводится окно редактирования параметров учётной записи пользователя (рисунок 15).

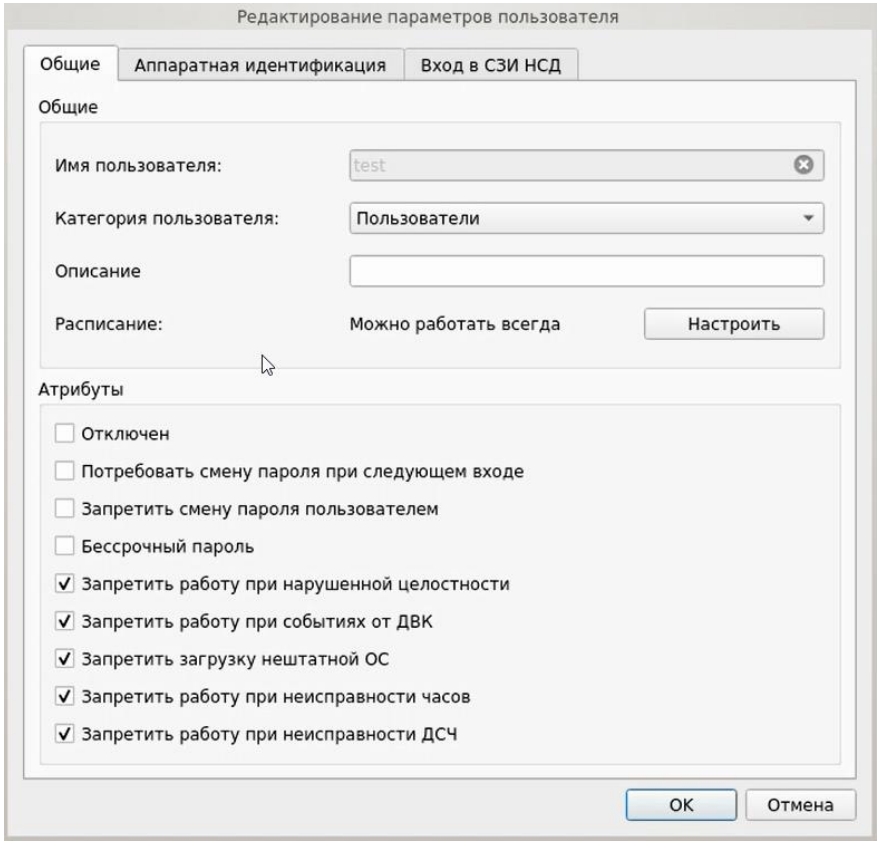


Рисунок 15 — Окно редактирования параметров учётной записи пользователя. Данные учётной записи пользователя

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

— «Категория пользователя» — выбирается из выпадающего списка;

П р и м е ч а н и е — Штатные пользователи, допущенные к работе на защищенной рабочей станции, не должны иметь категорию «Администраторы» или «Аудиторы».

— «Описание» — предназначено для текстового описания учётной записи пользователя (не более 95 символов);

— «Расписание» — установка разрешенного времени входа пользователя в систему

(Подробное описание установки разрешенного времени описано в документе «Руководство по эксплуатации» ПФНА.501410.003 РЭ).

Допустимо присвоение следующих атрибутов учётной записи пользователя:

— «Отключен» — учётная запись пользователя отключается, вход в систему невозможен до снятия атрибута администратором;

— «Потребовать смену пароля при следующем входе» — при входе пользователя в систему принудительно запускается диалоговое окно смены текущего пароля;

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

— «Запретить смену пароля пользователем» — запрет для пользователя на смену своего пароля, в т. ч. и по истечении срока действия;

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

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

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

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

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

Примечание — Данный атрибут 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 загрузку нештатной ОС» — запрет на загрузку ОС с носителя отличного от указанного в поле «Загрузочное устройство» вкладки «Параметры» оболочки администратора;

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

Примечание — Данный атрибут 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 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»** (рисунок 16) возможно назначение аппаратного

идентификатора в следующем порядке:

— предъявить аппаратный идентификатор и выбрать его из списка;

— далее автоматически заполняются поля «Серийный номер» (серийный номер АИ), «Имя пользователя», чекбоксы «Хранить пароль» и «Пароль защищен ПИН» (в соответствии с данными, ранее записанными в память АИ);

— при необходимости нажать кнопку «Очистить» — произойдет очистка поля «Имя пользователя»;

— после нажатия кнопки «Ок» данный идентификатор будет присвоен редактируемой учётной записи пользователя.

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

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

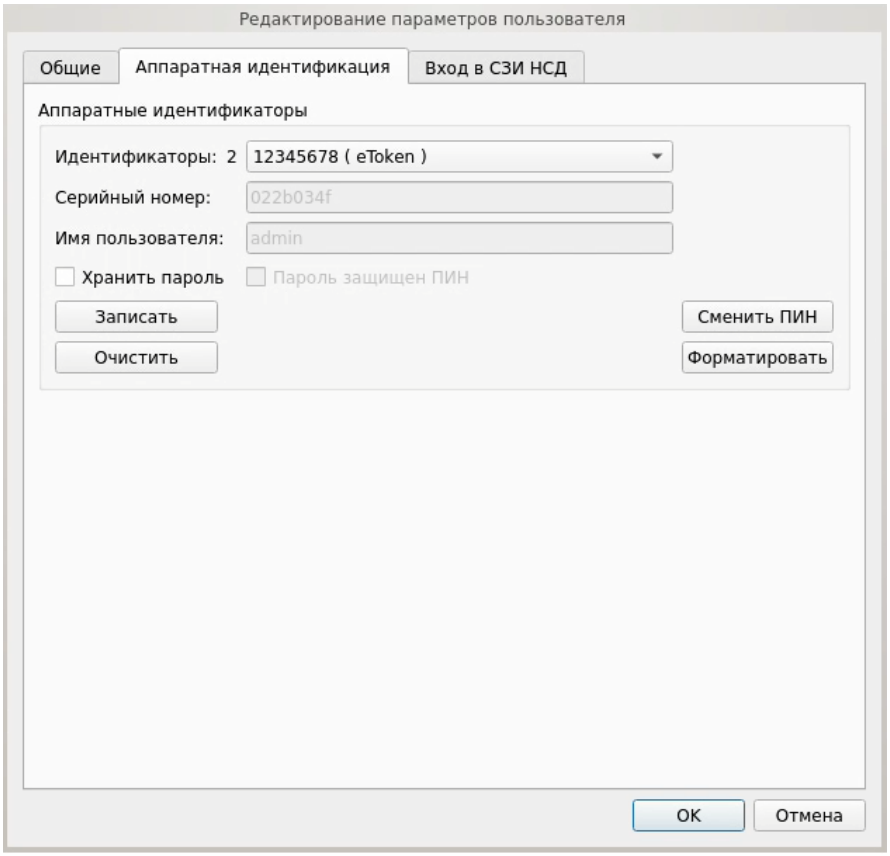


Рисунок 16 — Окно редактирования параметров учётной записи пользователя. Аппаратная идентификация (базовый режим работы)

Примечание — Примечание. В усиленном режиме работы на вкладке «Аппаратная идентификация» отсутствуют чекбокс «Хранить пароль», кнопки «Записать» и «Очистить» (рисунок 17).

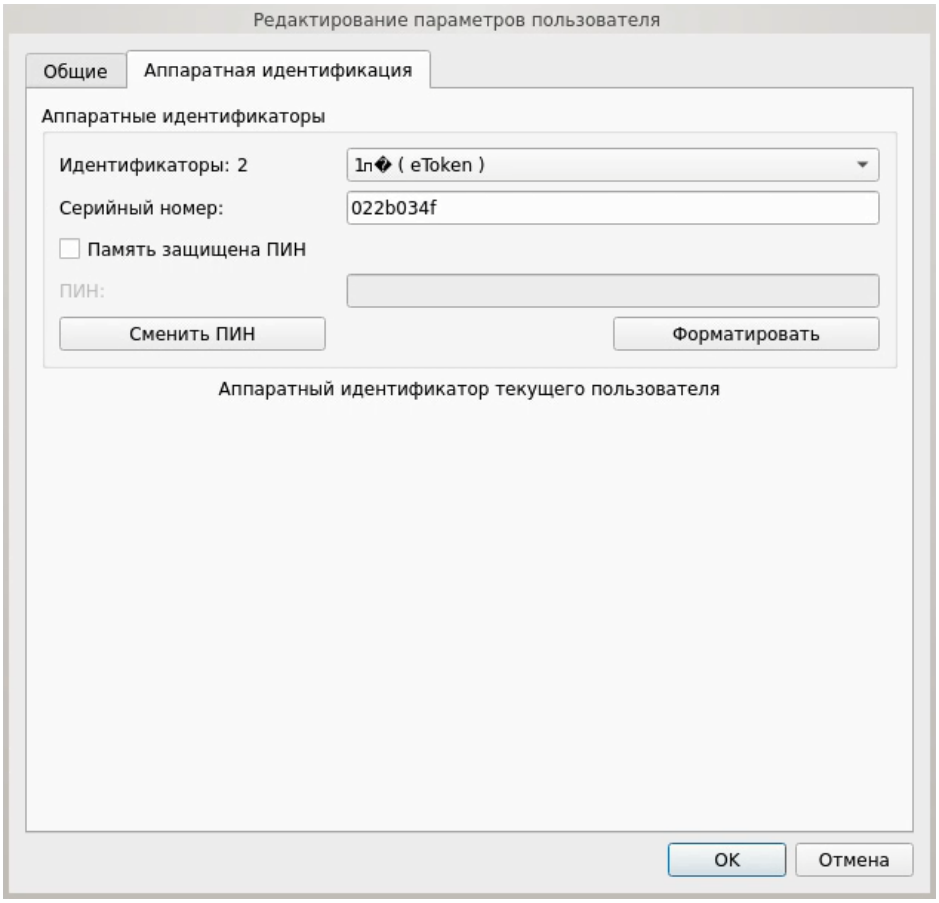


Рисунок 17 — Окно редактирования параметров учётной записи пользователя. Аппаратная идентификация (усиленный режим работы)

При необходимости возможно задать дополнительные параметры аппаратной идентификации:

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

Примечания

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

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

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

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

— «Пароль защищен ПИН» — данный атрибут позволяет хранить пароль в защищенной

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

Примечание — Обязательный атрибут при использовании электронных ключей iButton в качестве аппаратных идентификаторов.

— «Сменить ПИН» — данная кнопка позволяет сменить ранее назначенный ПИН учётной записи пользователя для идентификатора. В окне «Изменение ПИН» (рисунок 18) ввести старый, новый ПИН и повторить ввод нового ПИН;

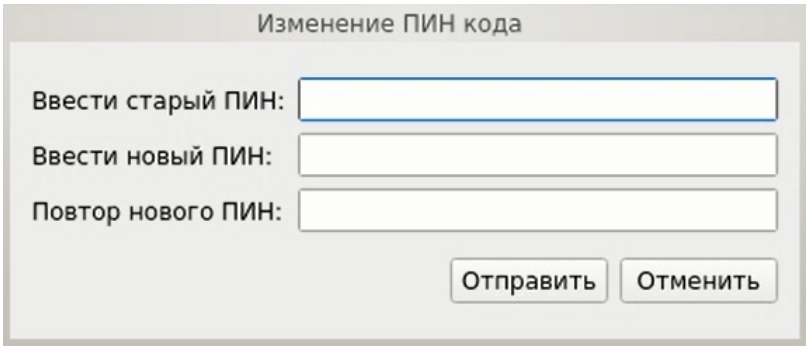


Рисунок 18 — Окно смены ПИН-кода

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

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

В окне «Форматирование токена» (рисунок 19) ввести следующую информацию:

— Старый ПИН администратора;

— Новый ПИН администратора;

— Новый ПИН пользователя;

— Метку токена.

Нажать клавишу «Enter» или кнопку «Отправить».

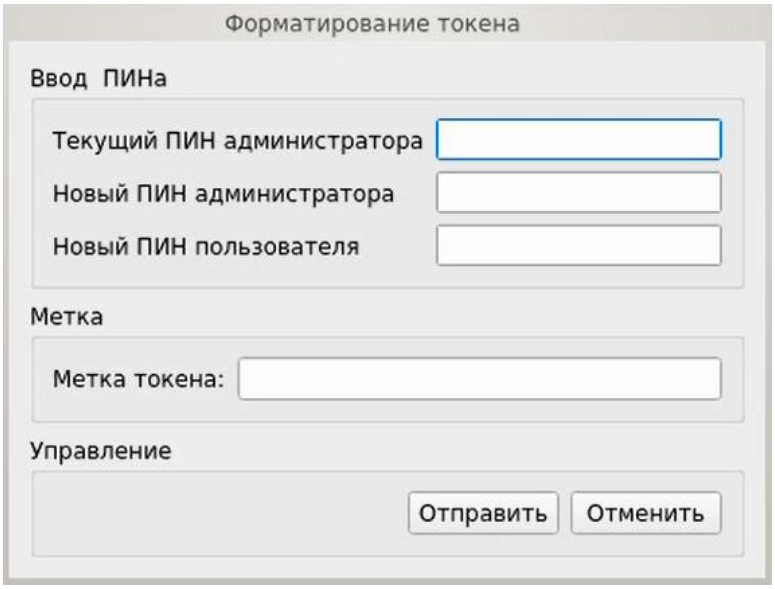


Рисунок 19 — Окно форматирование токена

В базовом режиме функционирования СДЗ имеется дополнительная вкладка **«Вход в СЗИ НСД»** (рисунок 20), позволяющая дополнительно настроить автовход в СЗИ НЗД Dallas Lock, установив соответствующий атрибут. При этом можно выбрать опцию:

— «Авторизационные данные введённые пользователем при входе» — чтобы использовать данные учётные записи пользователя, которые были введены при входе;

— «Предопределенные данные» — чтобы внести данные учётной записи пользователя вручную.

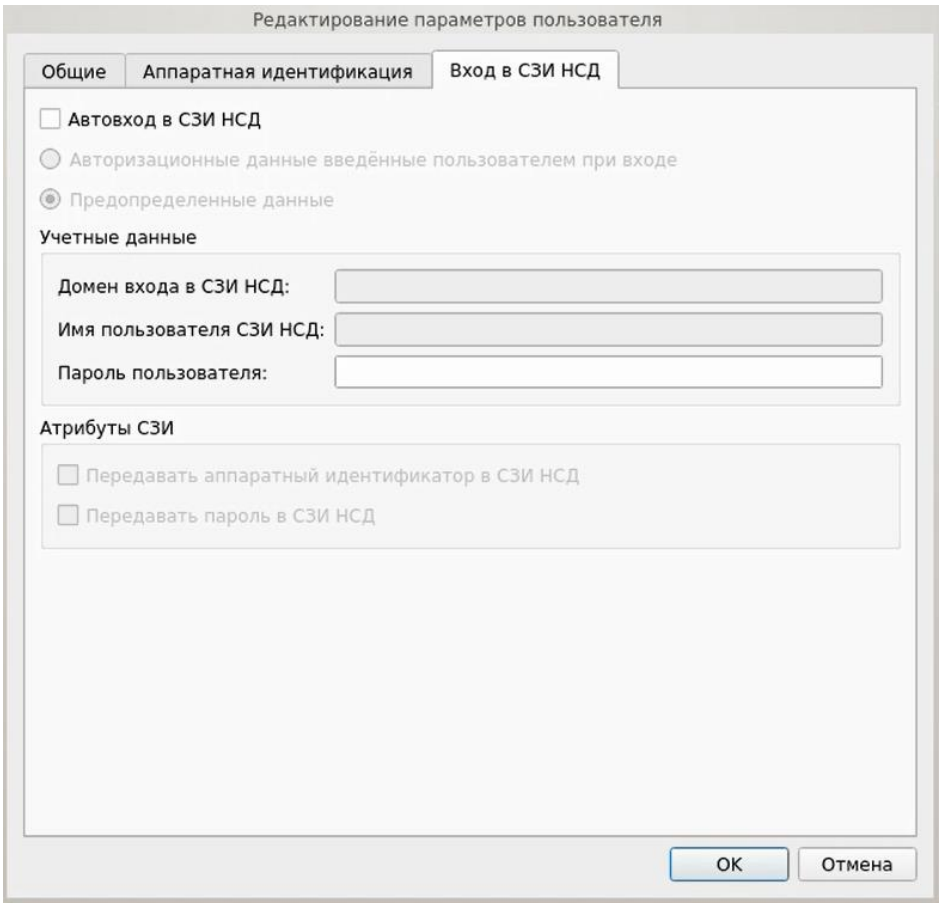


Рисунок 20 — Окно редактирования параметров учётной записи пользователя. Вход в СЗИ НСД

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 учётной записи пользователя производится при нажатии кнопки «ОК».

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

Примечания

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

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

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

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

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

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

При выборе действия «Задать пароль» в появившемся окне ввода пароля (рисунок 21) имеется возможность установить новый пароль учётной записи пользователя.

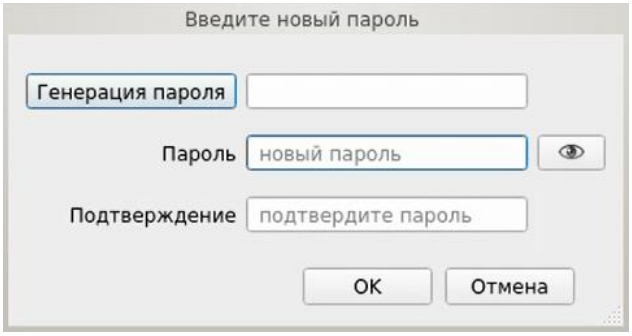


Рисунок 21 — Окно установки пароля учётной записи пользователя

Раздел «Заблокированные пользователи»

Просмотр заблокированных пользователей доступен в разделе «**Заблокированные пользователи**» (см. рисунок 22).

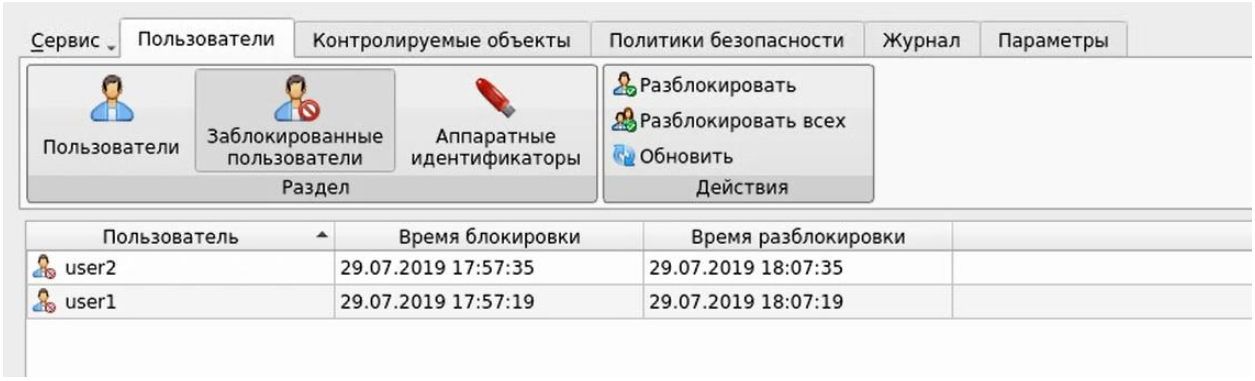


Рисунок 22 — Окно просмотра заблокированных пользователей

Возможны следующие действия с заблокированными учётными записями пользователей:

— «Разблокировать» — разблокировать выбранную учётную запись пользователя;

— «Разблокировать всех» — разблокировать все учётные записи пользователей, находящиеся в списке заблокированных;

— «Обновить» — обновить список заблокированных учётных записей пользователей.

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

Раздел «Аппаратные идентификаторы»

В разделе «**Аппаратные идентификаторы**» отображаются все подключённые аппаратные идентификаторы (см. рисунок 23).

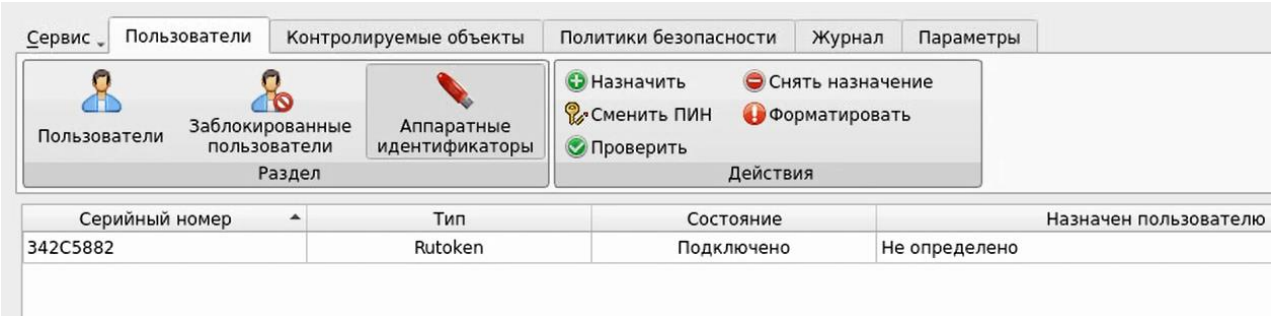


Рисунок 23 — Окно просмотра аппаратных идентификаторов

Для данного раздела доступны следующие действия:

— «Назначить» — назначение пользователю выбранного АИ;

— «Сменить ПИН»;

— «Проверить» — запуск процесса тестирования АИ;

— «Снять назначение»;

— «Форматировать».

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

3.2.2 Контроль целостности

На вкладке **«Контролируемые объекты»** отображаются все контролируемые объекты, зарегистрированные в СДЗ Dallas Lock (рисунок 24).

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».

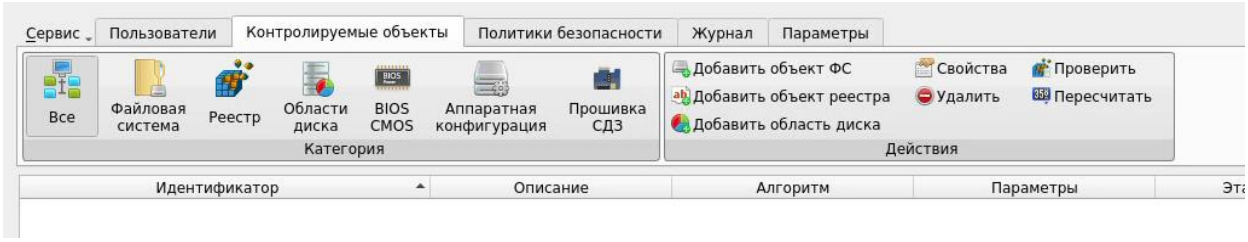


Рисунок 24 — Главное окно. Контролируемые объекты

Возможны следующие действия с контролируемыми файлами:

— «Добавить объект ФС»;

— «Добавить объект реестра»;

— «Добавить область диска»;

— «Свойства»;

— «Удалить»;

— «Проверить»;

— «Пересчитать».

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

Категория «Файловая система»

При нажатии кнопки «Добавить объект ФС» выполняется вывод диалогового окна «Добавить объект файловой системы» (рисунок 25), где доступно редактирование следующих параметров:

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

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

Допустима установка следующих атрибутов:

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

— «Учитывать наличие» — при контроле целостности объекта файловой системы будет проверяться только наличие указанного объекта. Устанавливается автоматически при установке

атрибутов «Учитывать содержимое» и «Учитывать атрибуты»;

— «Учитывать содержимое» — при контроле целостности объекта файловой системы будет проверяться содержимое указанного объекта;

— «Учитывать атрибуты» — при контроле целостности объекта файловой системы будет проверяться неизменность атрибутов указанного объекта.

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

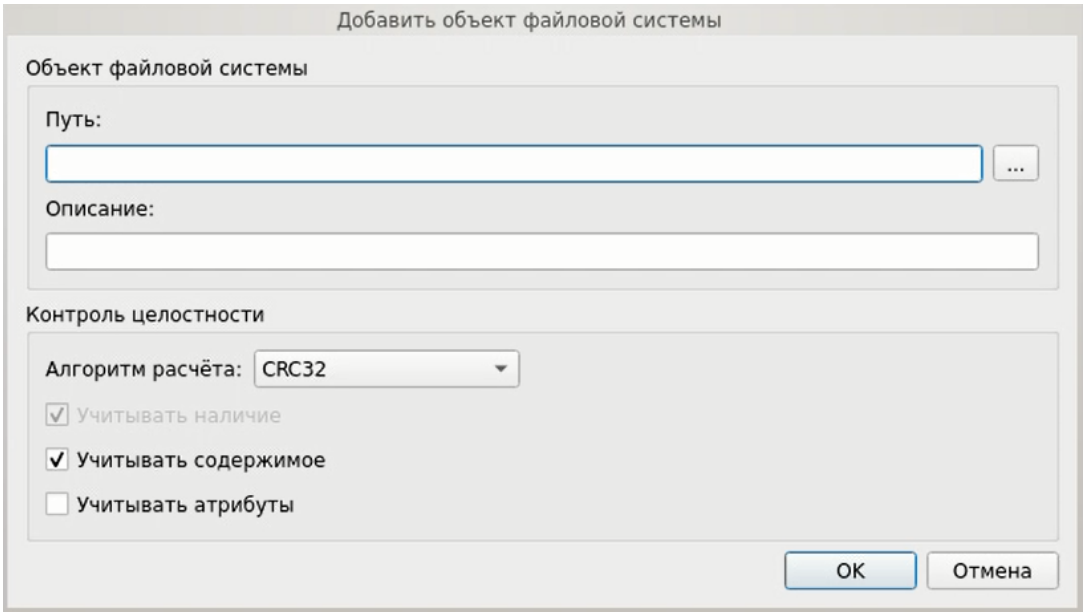


Рисунок 25 — Окно добавления объекта ФС в контролируемые объекты

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.

Категория «Реестр»

При нажатии кнопки «Добавить объект реестра» осуществляется вывод диалогового окна «Добавить объект реестра Windows» (рисунок 26), 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.

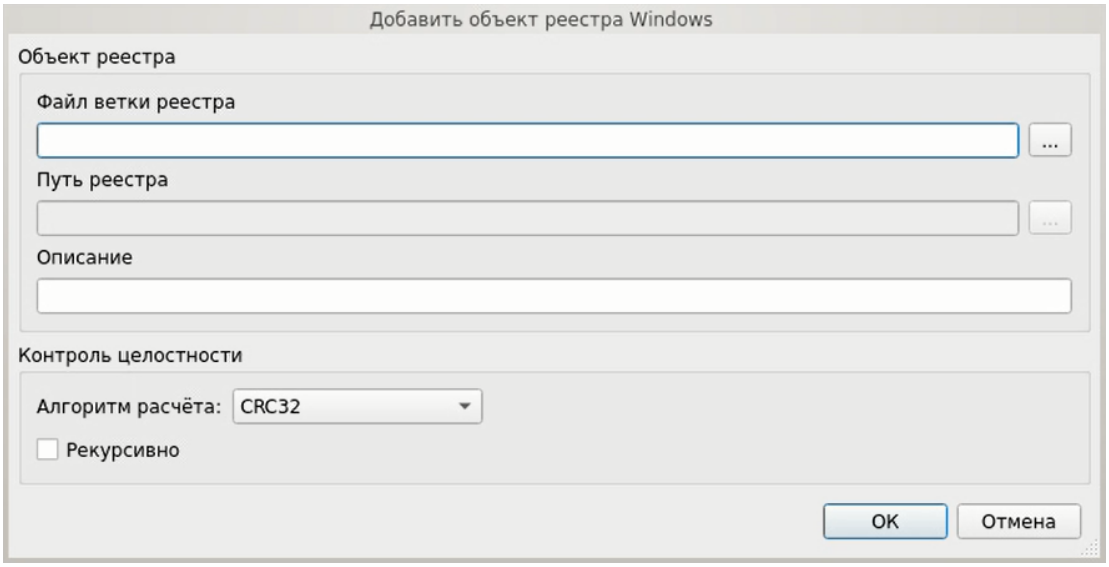


Рисунок 26 — Окно добавления объекта реестра в контролируемые объекты

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».

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.

Категория «Области диска»

Контроль целостности может быть назначен только для локальных дисков.

При нажатии кнопки «Добавить область диска» осуществляется вывод диалогового окна «Добавление области диска» (рисунок 27), 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».

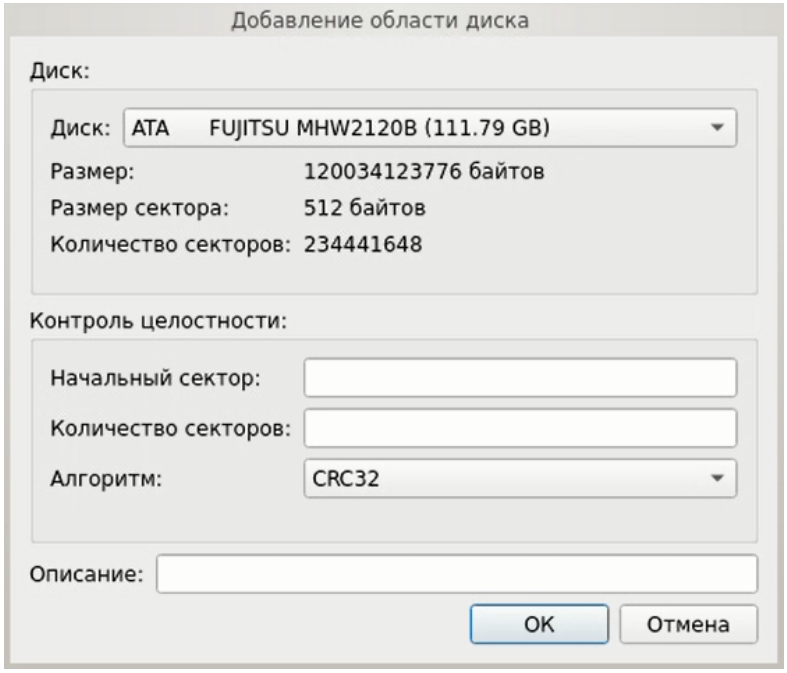


Рисунок 27 — Окно добавления области диска в контролируемые объекты

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.

Категория «BIOS/CMOS»

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

— «Обновить CMOS»;

— «Сохранить».

Для категории «BIOS CMOS» форма просмотра разделена на два блока «BIOS» и «CMOS» (рисунок 28).

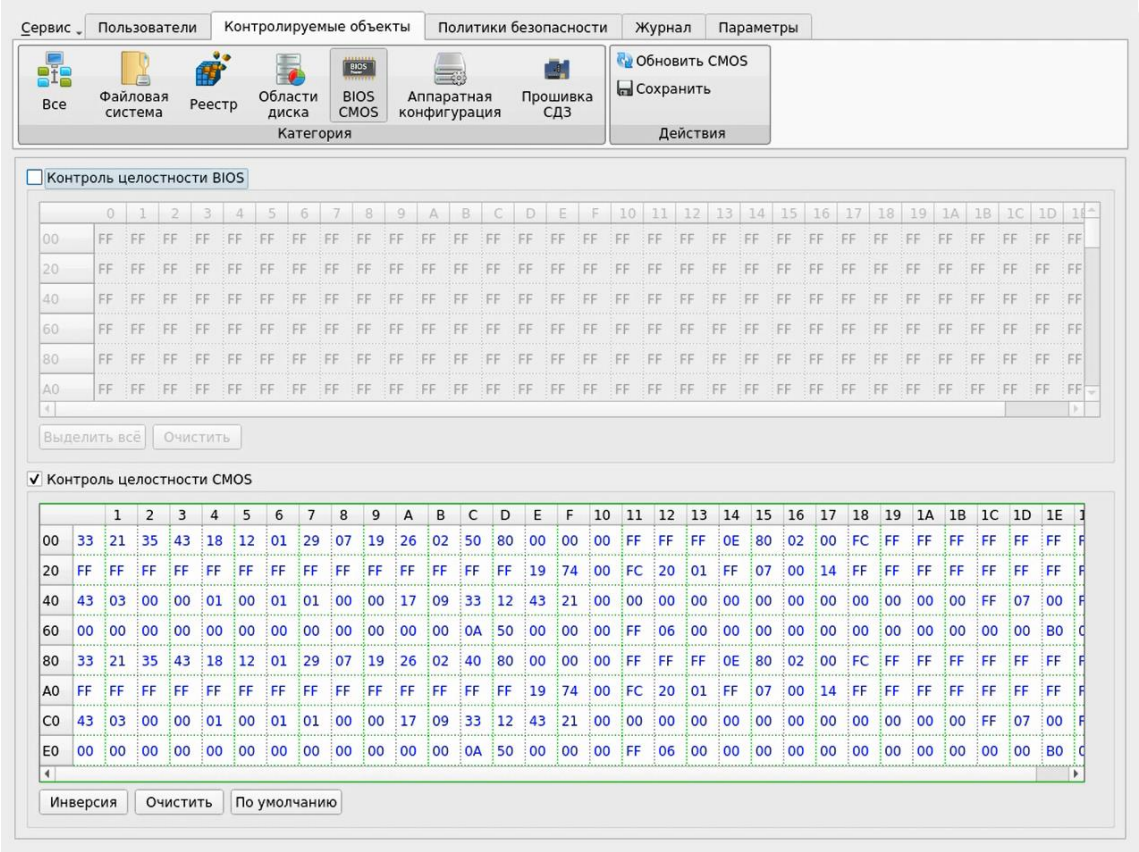


Рисунок 28 — Контроль BIOS CMOS

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

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

Категория «Аппаратурная конфигурация»

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

Для категории «Аппаратная конфигурация» доступны следующие функциональные кнопки:

— «Контролировать все группы» — при нажатии осуществляется инициирование контроля всех групп контролируемых объектов аппаратной конфигурации;

— «Снять контроль со всех групп» — при нажатии осуществляется прекращение контроля всех групп контролируемых объектов аппаратной конфигурации;

— «Обновить конфигурацию» — при нажатии осуществляется обновление списка устройств аппаратной конфигурации ТС;

— «Пересчитать» — при нажатии осуществляется пересчет значений целостности объектов аппаратной конфигурации;

— «Сохранить» — при нажатии осуществляется сохранение списка контролируемых

объектов аппаратной конфигурации.

Для настройки контроля аппаратной конфигурации в основной области доступны соответствующие группам чекбоксы (рисунок 29) «Контролировать группу» и напротив конкретного идентификатора в группе «исключить из контроля»/«включить контроль».

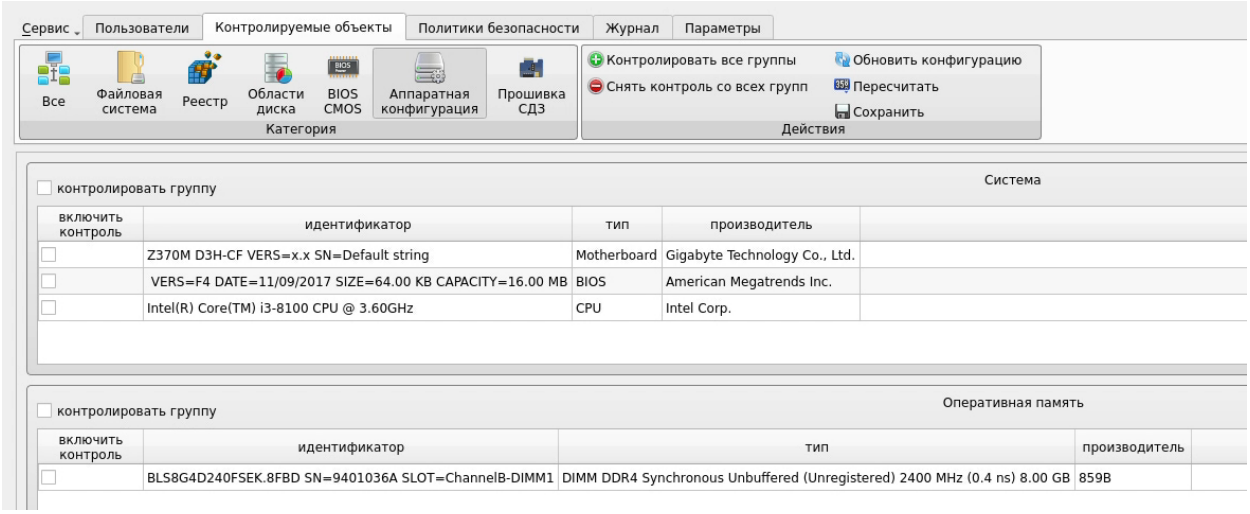


Рисунок 29 — Главное окно. Контролируемые объекты аппаратной конфигурации ТС

Для категории «Аппаратная конфигурация» выводятся списки групп аппаратной конфигурации (таблица 2).

Таблица 2 — Пример списка групп аппаратной конфигурации

Группа	Описание
Система	Отображается информация о материнской плате, BIOS и ЦП
Оперативная память	Отображаются установленные модули оперативной памяти
PCI-Устройства	Отображаются подключённые PCI-устройства
Накопители	Отображаются установленные накопители
USB-Устройства	Отображаются различные устройства, подключённые через USB-порт, например: — аппаратные идентификаторы; — USB-преобразователи; — USB-HID устройства

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

Категория «Прошивка СДЗ»

Для данной категории доступны следующие действия (рисунок 30):

— «Проверить»;

— «Сохранить».

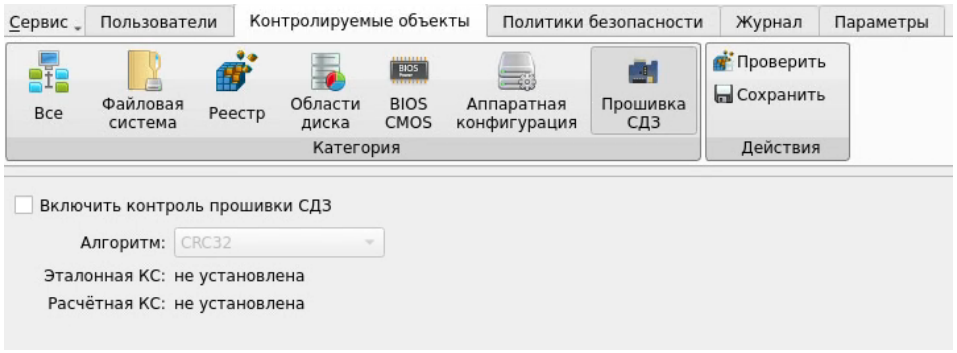


Рисунок 30 — Главное окно. Контроль прошивки СДЗ

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

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

Сохранение установленных данных осуществляется при нажатии кнопки «Сохранить».

3.2.3 Настройка политик безопасности

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

Выделяются следующие категории политик безопасности:

— «Политики авторизации»;

— «Политики паролей»;

— «Политики ДСЧ».

Просмотр параметров и значений конкретной категории политик осуществляется через соответствующие кнопки в панели «Политики» (рисунок 31, рисунок 32, рисунок 33). Описание и возможные значение политик приведены в таблицахТаблица **3**,Таблица **4** и Таблица **5**.

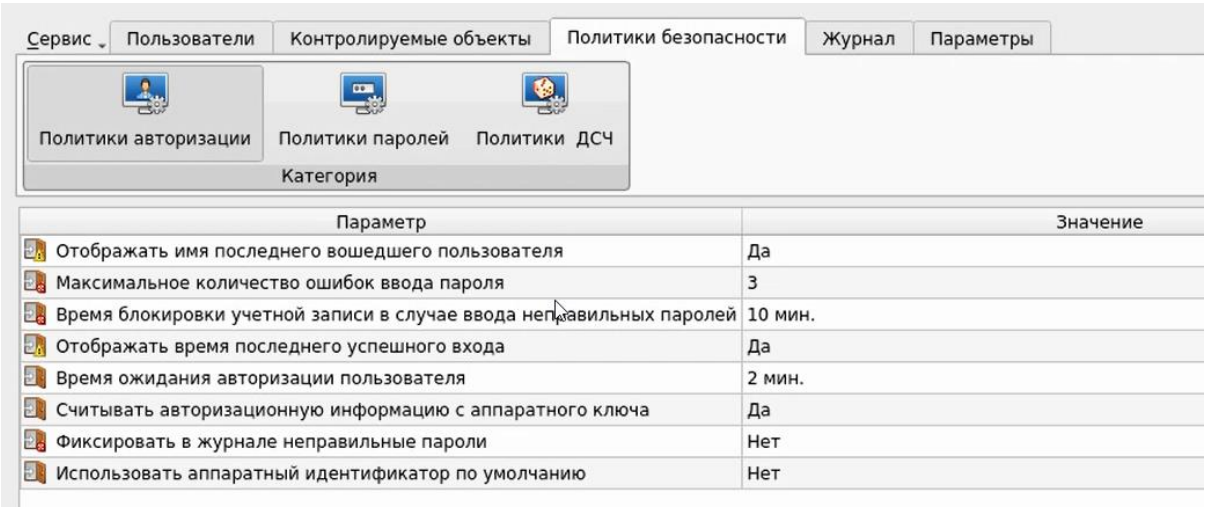


Рисунок 31 — Главное окно. Политики авторизации

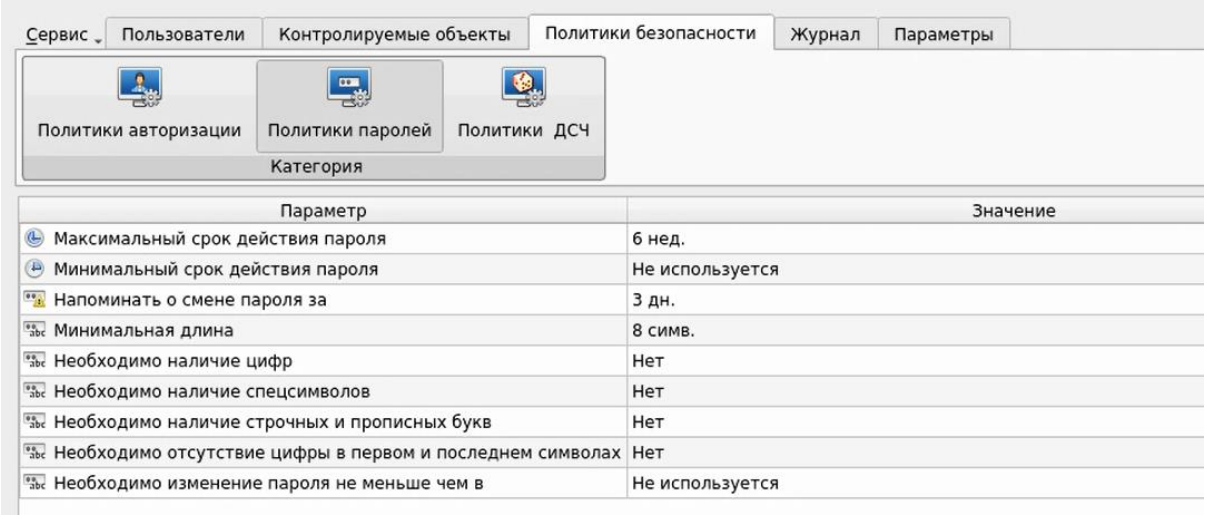


Рисунок 32 — Главное окно. Политики паролей

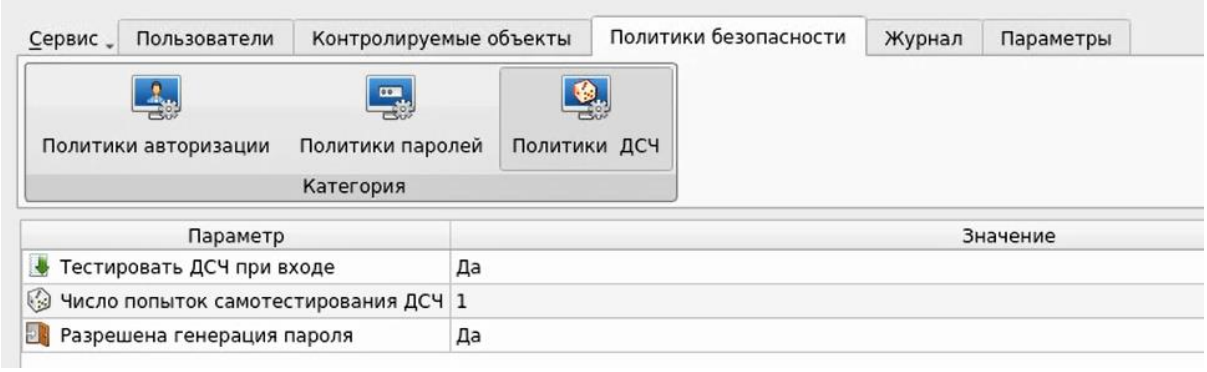


Рисунок 33 — Главное окно. Политики ДСЧ

Редактирование значений параметров политик осуществляется через соответствующие диалоговые окна, вызываемые двойным нажатием левой кнопки мыши на поле таблицы с редактируемой записью. Пример диалогового окна редактирования параметров политики безопасности (рисунок 34).

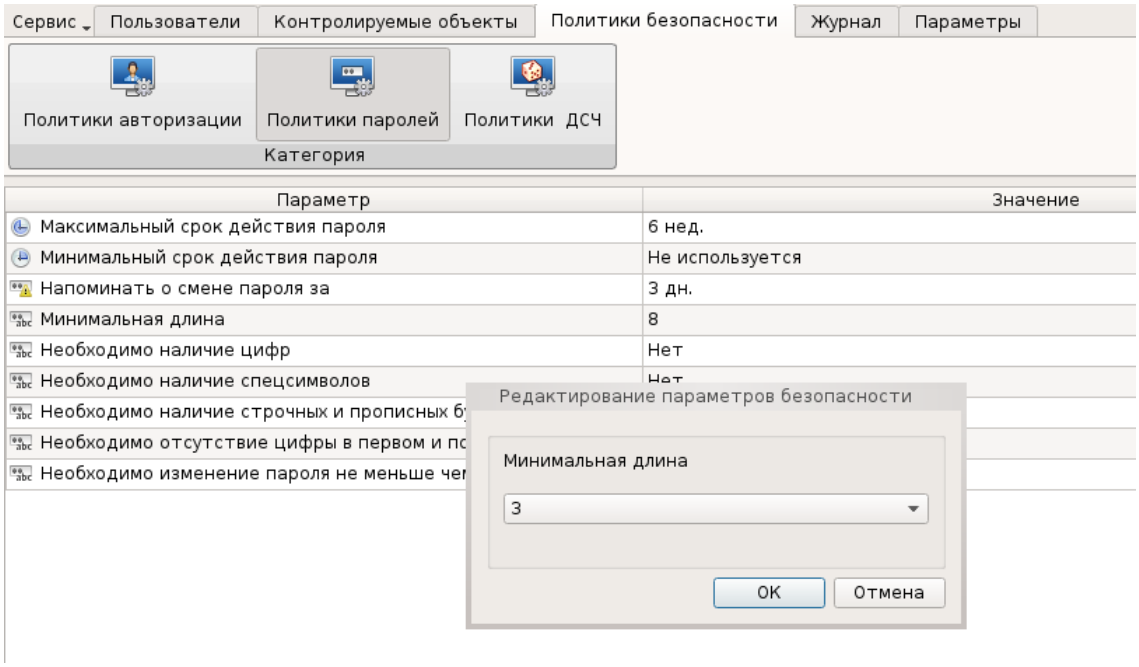


Рисунок 34 — Диалоговое окно редактирования

Таблица 3 — 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 учётной записи пользователя, осуществившего последний успешный вход. При значении «Нет» поле остается пустым
«Максимальное количество ошибок ввода пароля»	Установленное значение регламентирует количество попыток ввода значений пароля. В случае ввода неверного пароля появляется предупреждение. По достижении установленного значения — учётная запись пользователя блокируется на определённое время, устанавливаемое параметром «Время блокировки учётной записи в случае ввода неправильных паролей». Возможное значение параметра: от 1 до 10 и «Не используется» — количество попыток ввода пароля не ограничено
«Время блокировки учётной записи в случае ввода неправильных паролей»	Установленное значение регламентирует время блокировки учётной записи после ввода неверного пароля более допустимого числа раз (определяется параметром «Максимальное количество ошибок ввода пароля»). В данный интервал времени вход невозможен даже при верном вводе пароля. Возможное значение параметра: от 1 мин до 5 ч и «Не используется» — в таком случае разблокировка возможна только администратором
«Отображать время последнего успешного входа»	Возможное значение параметра: «Да/Нет». В значении «Да» при очередном входе пользователя во вовремя выполнения процедуры контроля целостности объектов отображается дата и время последнего успешного входа данного пользователя. В значении «Нет» — не

Параметр политики	Описание
	отображается
«Время ожидания авторизации пользователя»	Время, отводимое на ввод пользователем авторизационных данных (от начала набора данных, до нажатия кнопки «ОК»). Если пользователь не успел завершить ввод авторизационных данных, уже введённые данные очищаются. Возможное значение параметра: от 1 мин до 10 мин и «Не используется» — время ожидания ввода авторизационных данных не ограничено
«Считывать авторизационную информацию из аппаратного ключа»	Возможное значение параметра: «Да/Нет». В значении «Нет» авторизационная информация вводится пользователем с клавиатуры. В значении «Да» авторизационная информация считывается с памяти АИ в соответствии с настройками учётной 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 «Нет» АИ должен быть выбран из предъявленных пользователем самостоятельно. В значении «Да» обнаруженный АИ используется автоматически. Если АИ предъявлено несколько, то используется первый обнаруженный
«Срок действия ключа аутентификации»	Значение данного параметра определяет срок смены ключа аутентификации. Возможное значение параметра: от 1 дн. до 52 нед. и «Не используется» — срок действия не ограничен. Данная политика авторизации доступна только в усиленном режиме работы СДЗ Dallas Lock

Таблица 4 — Список параметров категории «Политики паролей»

Параметр политики	Описание
«Максимальный срок действия пароля»	Параметр устанавливает максимальный срок действия паролей пользователей. По истечении срока действия пользователям автоматически будет предложено сменить пароли. Не распространяется на учётные записи пользователей с установленным атрибутом «Бессрочный пароль». Возможное значение параметра: от 1 дня до 25 недель и «Не используется» — максимальный срок действия пароля не установлен
«Минимальный срок действия пароля»	Параметр определяет минимальный срок действия пароля. Если этот срок ещё не истёк, смена пароля пользователем запрещена.

Параметр политики	Описание
	Возможное значение параметра: от 1 дня до 4 недель, «Не используется» — минимальный срок действия не установлен
«Напоминать о смене пароля за»	Параметр задаёт период до установленного максимального срока действия пароля, в который пользователю будет выводиться сообщение о необходимости смены пароля. Возможное значение параметра: от 1 дня до 2 недель и «Не используется» — сообщение выводиться не будет
«Минимальная длина»	Параметр устанавливает ограничение на минимальную длину пароля. Возможное значение параметра: от 1 до 14 и «Не используется» — устанавливаемый пароль может иметь пустое значение
«Необходимо наличие цифр»	Если данный параметр включен, то при создании пароля в нём должны присутствовать цифры. Возможное значение параметра: «Да/Нет»
«Необходимо наличие спецсимволов»	Если данный параметр включен, то при создании пароля в него должны быть включены специальные символы, такие как "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "_", "-", "+", "{", "}", "[", "]", "\", "|", ":", ";", """, "'", "<", ">", ",", ".", "?", "/", "=" и т. д. Возможное значение параметра: «Да/Нет»
«Необходимо наличие строчных и прописных букв»	Если данный параметр включен, то при создании пароля в него должны быть включены как строчные, так и прописные буквы. Возможное значение параметра: «Да/Нет»
«Необходимо отсутствие цифры в первом и последнем символах»	Если данный параметр включен, то при создании пароля его первый и последний символ не должны являться цифрами. Возможное значение параметра: «Да/Нет»
«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 5 — 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

Параметр политики	Описание
«Разрешена генерация пароля»	Возможное значение параметра: «Да/Нет». В значении «Да» пользователю дается возможность генерации паролей. В значении «Нет» у пользователя нет возможности воспользоваться генерацией пароля.

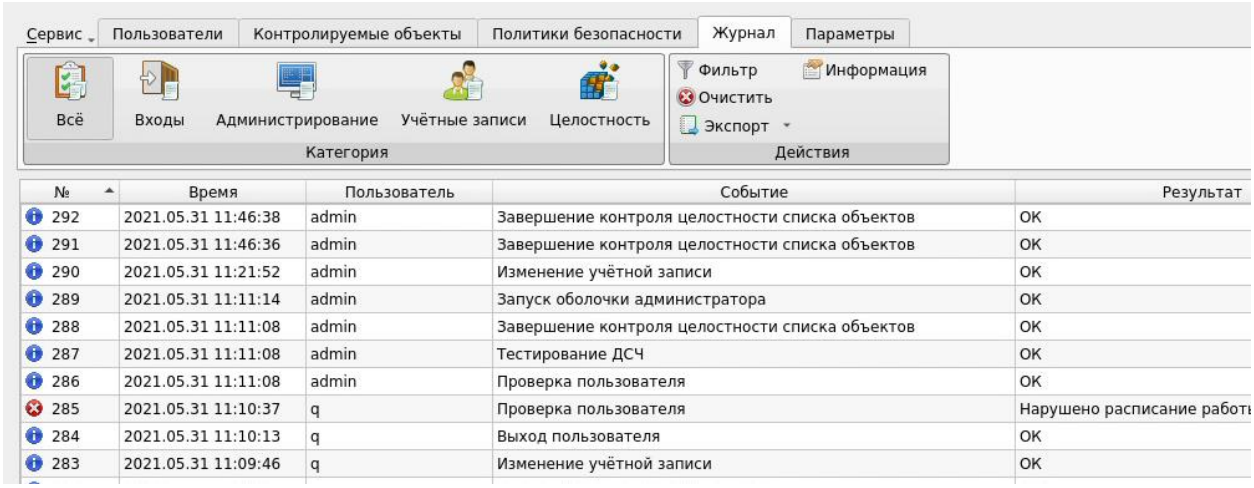
Перечень вариантов параметров политик безопасности предполагается выбирать из соответствующих выпадающих списков или путем выбора одного из вариантов «Да/Нет».

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

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

3.2.4 Регистрация и учёт

В разделе **«Журнал»** в виде таблицы отображаются все события, зарегистрированные в ходе работы СДЗ Dallas Lock (рисунок 35).



№	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

Рисунок 35 — Главное окно. Журнал

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»;

— «Учётные записи»;

— «Целостность».

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

Возможны следующие действия с категориями журнала:

— «Фильтр»;

— «Очистить»;

— «Экспорт»;

— «Информация».

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

При нажатии кнопки «Фильтр» выводится всплывающее меню (рисунок 36) через которое допустимо назначение:

— текстового фильтра;

— интервального фильтра;

— фильтра по значению;

— регулярного выражения;

— автофильтра.

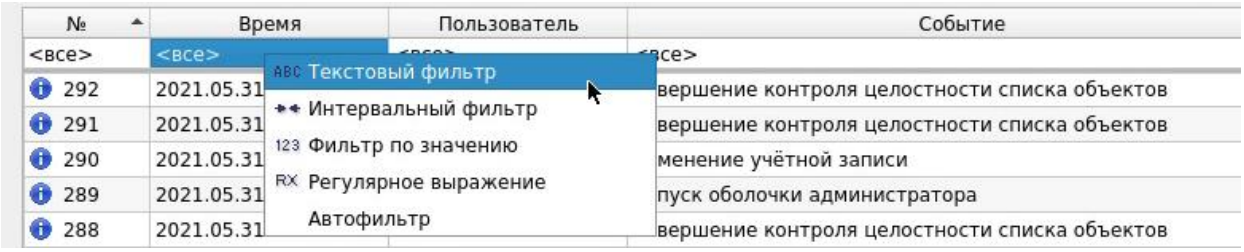


Рисунок 36 — Главное окно. Назначение фильтра

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 (рисунок 37).

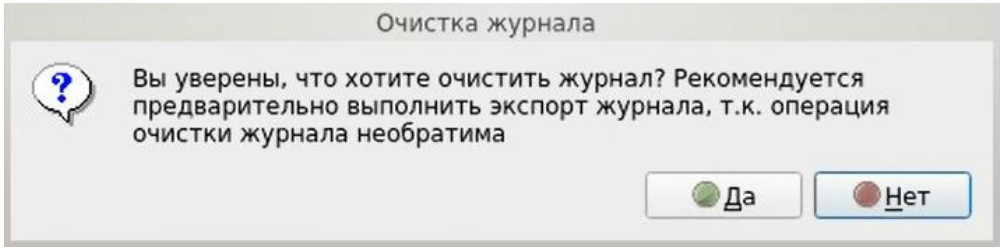


Рисунок 37 — Сообщение «Очистка журнала»

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

Поскольку операция удаления записей журнала необратима, перед очисткой журнала рекомендуется произвести экспорт записей журнала в файл. При нажатии кнопки «Экспорт» из выпадающего списка выбирается формат создаваемого файла (рисунок 38). Данная функция также доступна пользователям категории «Аудиторы».

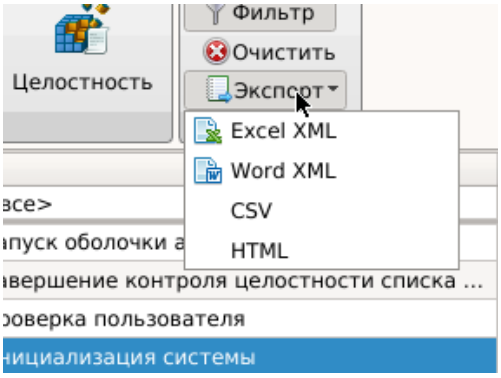


Рисунок 38 — Главное окно. Меню экспорта журнала в файл

При нажатии кнопки «Информация» выводится соответствующее информационное окно для выбранного события (рисунок 39).

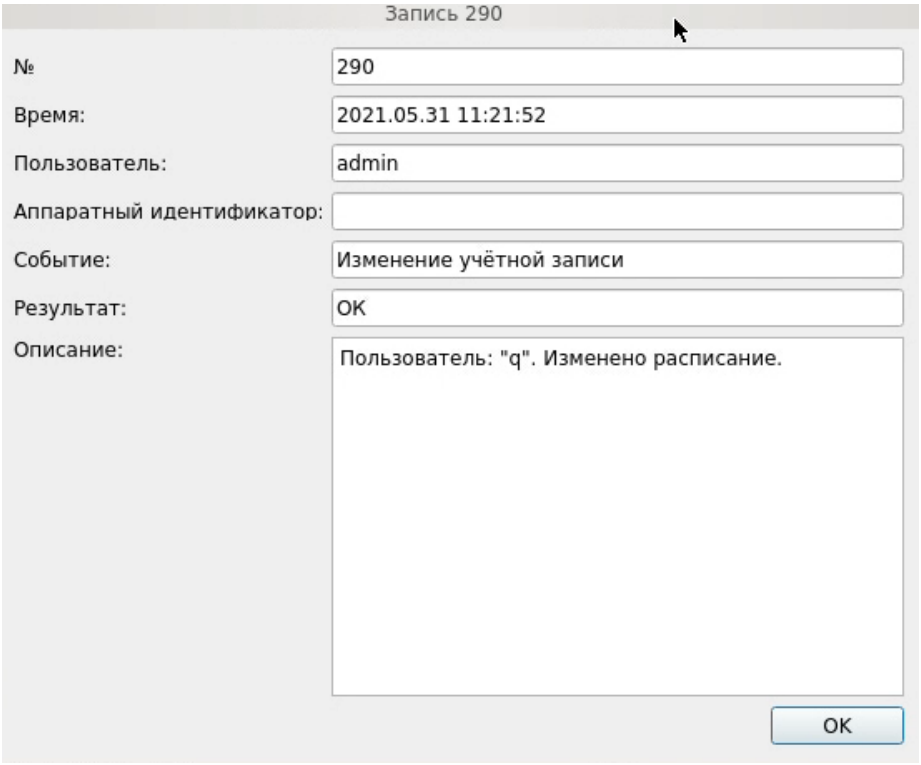


Рисунок 39 — Информационное окно

3.2.5 Управление параметрами платы

В разделе «Параметры» отображаются следующие категории:

— «Плата КТ»;

— «Параметры загрузки»;

— «Параметры сети».

Просмотр параметров и значений конкретной категории осуществляется через соответствующие кнопки в панели «Категория» (рисунок 40, рисунок 43, рисунок 44).

Категория «Плата КТ»

В категории «**Плата КТ**» доступен просмотр и установка следующих значений:

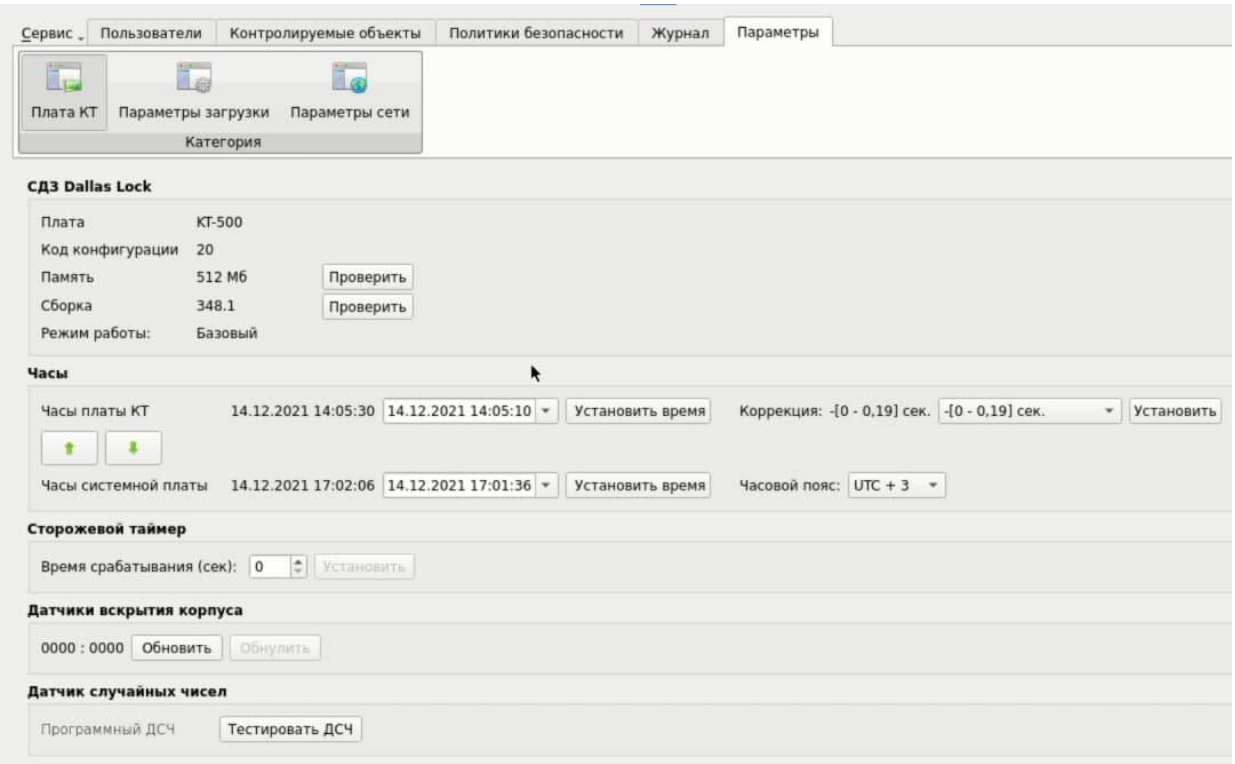


Рисунок 40 — Главное окно. Плата КТ

— «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.

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

Примечание — Параметр «Датчик вскрытия корпуса» 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» (ДСЧ) — 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 (Рисунок 41).

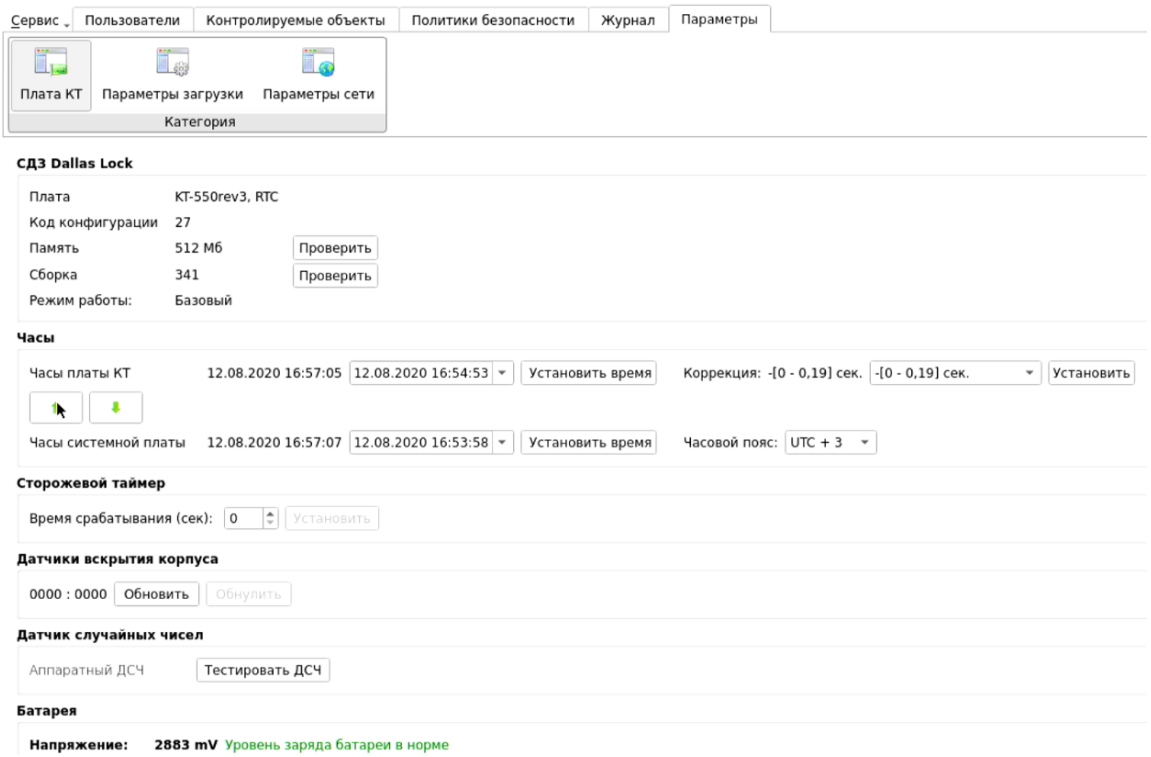


Рисунок 41 — Уровень заряда батареи в норме

Если батарея разряжена, то в полях «Часы» и «Батарея» выводится информационное сообщение «Батарея полностью разряжена!», а указанное напряжение будет равно 0 mV (Рисунок 42):

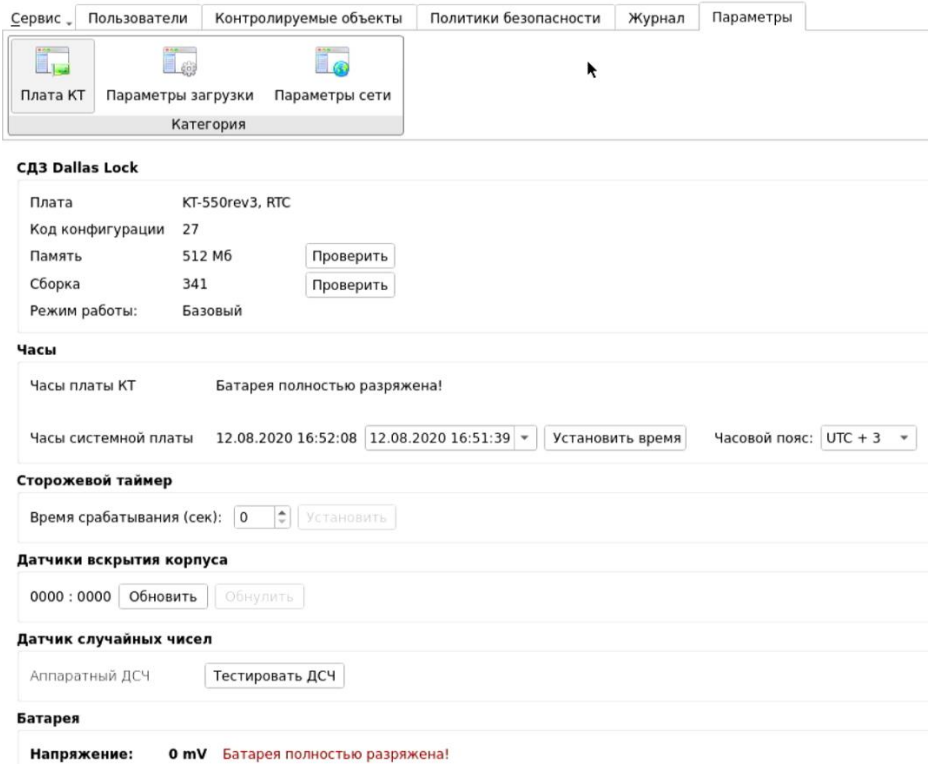


Рисунок 42 — Батарея разряжена

Категория «Параметры загрузки»

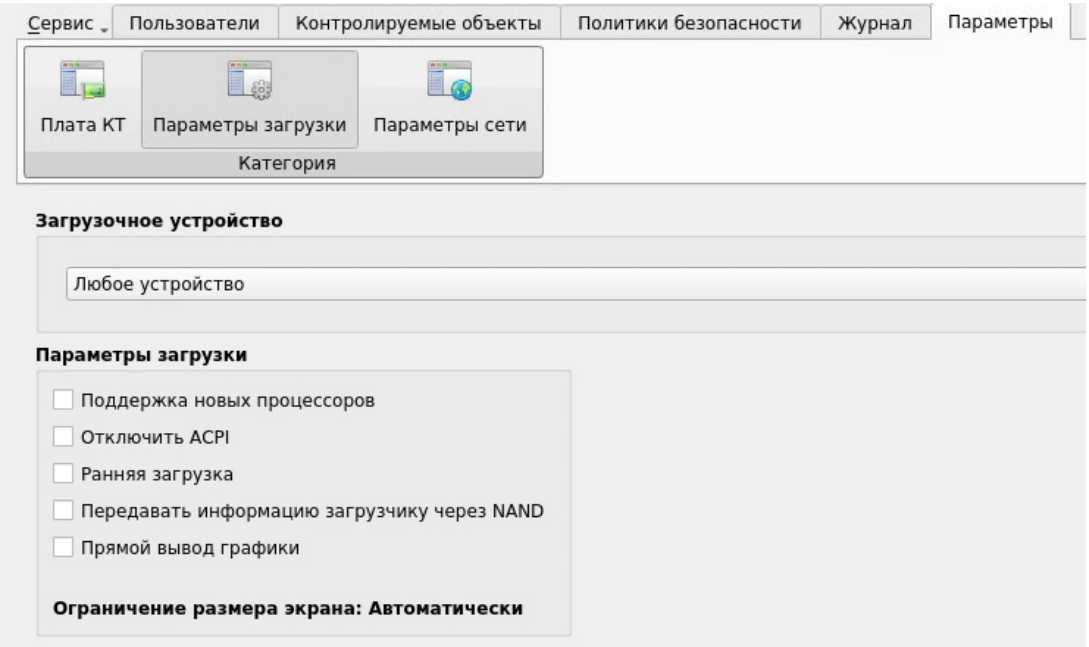


Рисунок 43 — Главное окно. Параметры загрузки

— «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.
- «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» 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.

Категория «Параметры сети»

Рисунок 44 — 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 мак-адрес нужного сетевого адаптера;
- чекбокс «запрашивать динамически» — при установленном чекбоксе во время запуска оболочки функций безопасности сетевые параметры автоматически назначаются DHCP-сервером;
- «IPv4 адрес», «IPv4 маска подсети», «IPv4 шлюз», «Серверы DNS» — сетевые параметры компьютера, которые можно заполнить вручную или автоматически, установив флаг в поле «запрашивать динамически». Также для сервера DNS доступны управляющие кнопки «+» и «-», которые позволяют добавлять и удалять DNS сервера;

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 Домен безопасности, появится сообщения об успешном вводе клиента (рисунок 45). Для завершения операции и перезагрузки клиента СДЗ необходимо нажать кнопку «ОК».

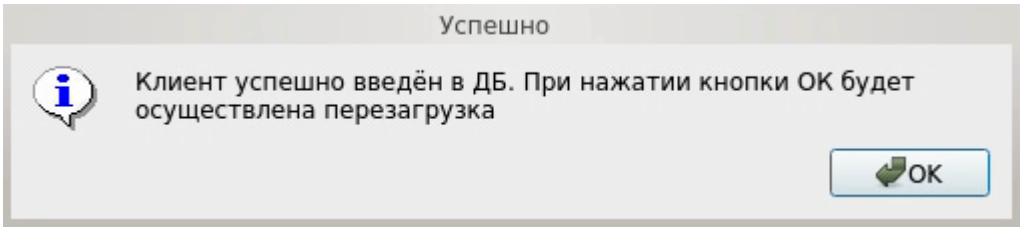


Рисунок 45 — Информационное сообщение о вводе клиента в ДБ

Примечания

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

2 Для удаленной перезагрузки/выключения клиентов СДЗ, находящихся в режиме работы ШОС, необходима установка Агента ШОС (см. п.п. 3.2.8).

В дереве объектов КСБ или консоли ЕЦУ появится новый клиент СДЗ. После чего в категории «Параметры сети» будет доступна только кнопка «Вывести из ДБ» (рисунок 46).

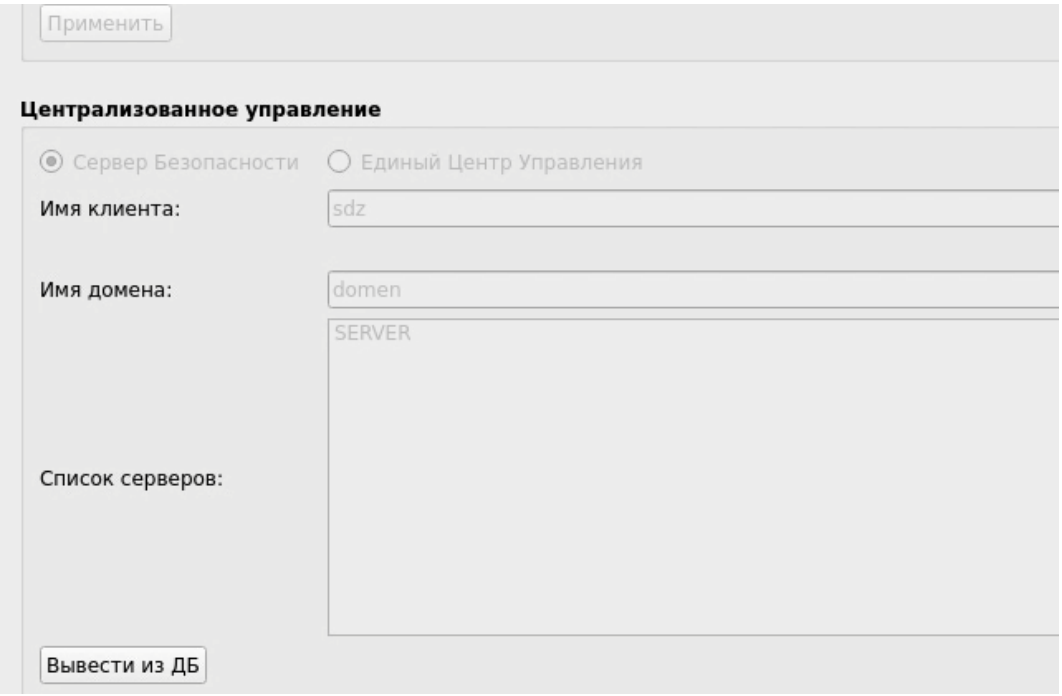


Рисунок 46 — Параметры сети. Кнопка вывода из ДБ

3.2.6 Дополнительные функции СДЗ Dallas Lock

Меню **«Сервис»** позволяет получить доступ к дополнительным функциям СДЗ Dallas Lock (рисунок 47).

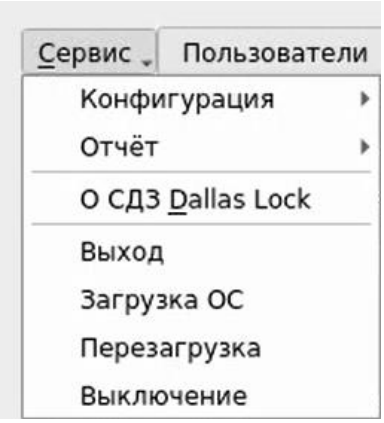


Рисунок 47 — Главное окно. Меню «Сервис»

Действия доступные для конфигурации:

— «Сохранить» — данные об учётных записях пользователей, контролируемых объектах и политиках безопасности сохраняются в специальном файле конфигурации в формате *.xml на различные носители информации;

— «Применить» — применение сохраненных параметров конфигурации;

— «По умолчанию» — восстановление конфигурации СДЗ Dallas Lock по умолчанию.

«Отчёт» — сохранение отчёта в формате *.txt на различные носители информации. Функция сохранения отчёта может использоваться для дальнейшей проверки соответствия этих настроек эталонным значениям.

Доступно формирование отчётов следующих видов:

— отчёт «Права и конфигурация»;

— отчёт «Аппаратная часть».

В отчёте «Права и конфигурации» указываются следующие данные:

— имя пользователя, который создал отчёт;

— дата и время формирования отчёта;

— версия прошивки СДЗ Dallas Lock;

— режим работы СДЗ;

— параметры конфигурации СДЗ Dallas Lock в соответствии с настройками отчёта.

В отчёте «Аппаратная часть» указываются следующие данные:

— имя пользователя, который создал отчёт;

— дата и время формирования отчёта;

— 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 контактных данных производителя. Доступна кнопка «Сменить код тех. поддержки» — ввод кода технической поддержки в случае, когда он не был введён ранее либо был изменён.

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

3.2.7 Завершение работы с ОА

После завершения работы с ОА администратор/аудитор, может выполнить любое из действий:

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

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

— «Перезагрузка» — осуществляется перезагрузка ТС;

— «Выключение» — осуществляется выключение ТС.

Процесс загрузки ШОС осуществляется в следующем порядке:

— производится сохранение всех необходимых данных в энергонезависимой памяти платы СДЗ Dallas Lock;

— производится сохранение на жёстком диске ТС данных, которые могут понадобиться СЗИ, работающей в среде ШОС;

— осуществляется зачистка оперативной памяти ТС, используемой для работы СДЗ Dallas Lock;

— производится блокировка доступа к энергонезависимой памяти платы СДЗ Dallas Lock;

— производится перевод процессора ТС в реальный режим работы;

— осуществляется возврат управления BIOS системной платы ТС.

В случае если в BIOS системной платы ТС изменён порядок загрузки таким образом, что первый загрузочный диск не является тем, на котором установлена ШОС, СДЗ Dallas Lock блокирует

загрузку ОС, и выводится соответствующее предупреждение.

Все значимые события заносятся в журнал СДЗ Dallas Lock: загрузка ОФБ, результат самодиагностики СДЗ Dallas Lock, результат авторизации пользователя, результат контроля целостности, смена пароля, запуск ОА, загрузка ШОС, перезагрузка и выключение ТС.

3.2.8 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 доступна посредством КСБ и осуществляться 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.

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 «generic» и при выключенном режиме ЗПС);
- Astra Linux Special Edition (Смоленск) 1.6 x64 (ограничение: корректная работа Агента ШОС возможна с версией ядра «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 данная процедура проходит в фоновом режиме. По завершению установки выводится сообщение об успешном выполнении процедуры.

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

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:
    a. заголовки файлов для загруженного ядра;
    b. инструменты для разработчиков;
    c. 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» (Рисунок 48).

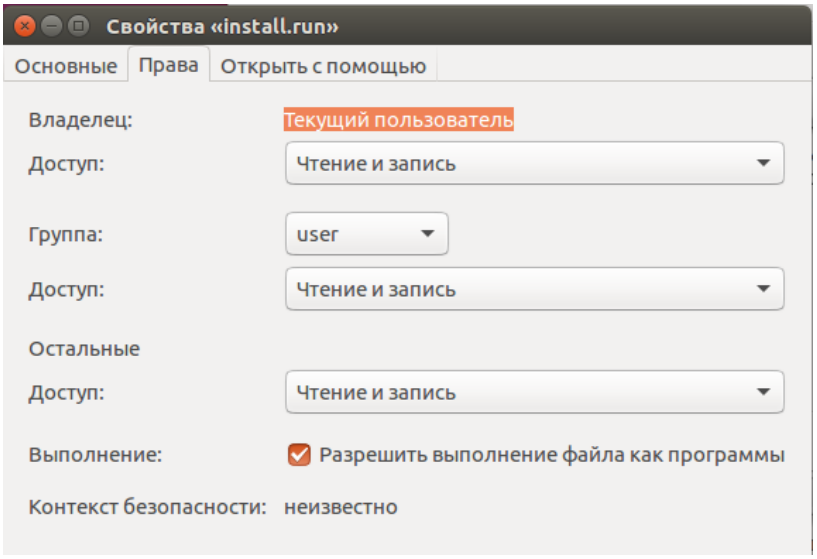


Рисунок 48 — Свойства файла

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 (Рисунок 49).

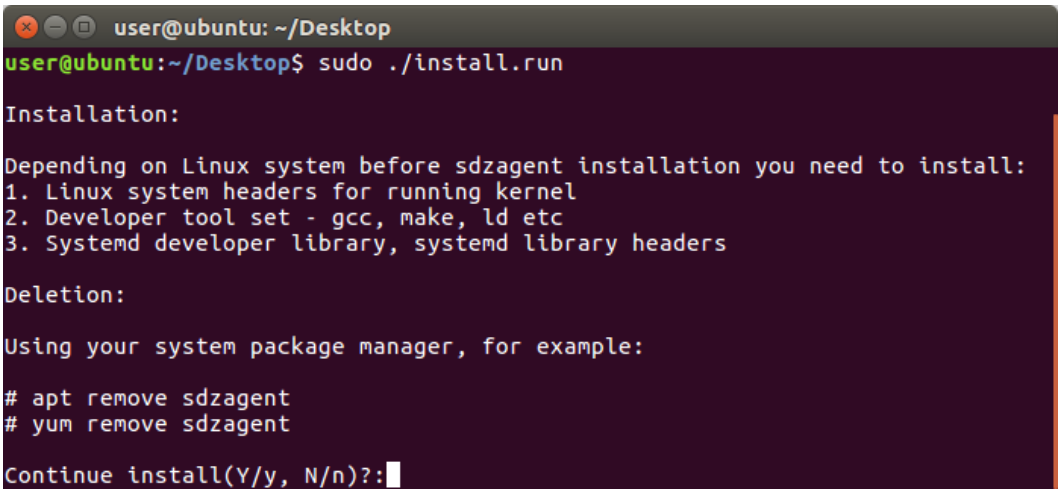


Рисунок 49 — Процесс установки Агента ШОС

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 (таблица 6).

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

Таблица 6 — 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

3.2.9 Восстановление заводских настроек (использование сервисной утилиты)

Восстановление изделия к заводским настройкам возможно при помощи сервисной утилиты СДЗ Dallas Lock (рисунок 50).

Данная утилита позволяет:

— посмотреть информацию о плате;

— применить/обновить прошивку;

— вернуть настройки платы в исходное состояние;

— сменить режим загрузки.

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

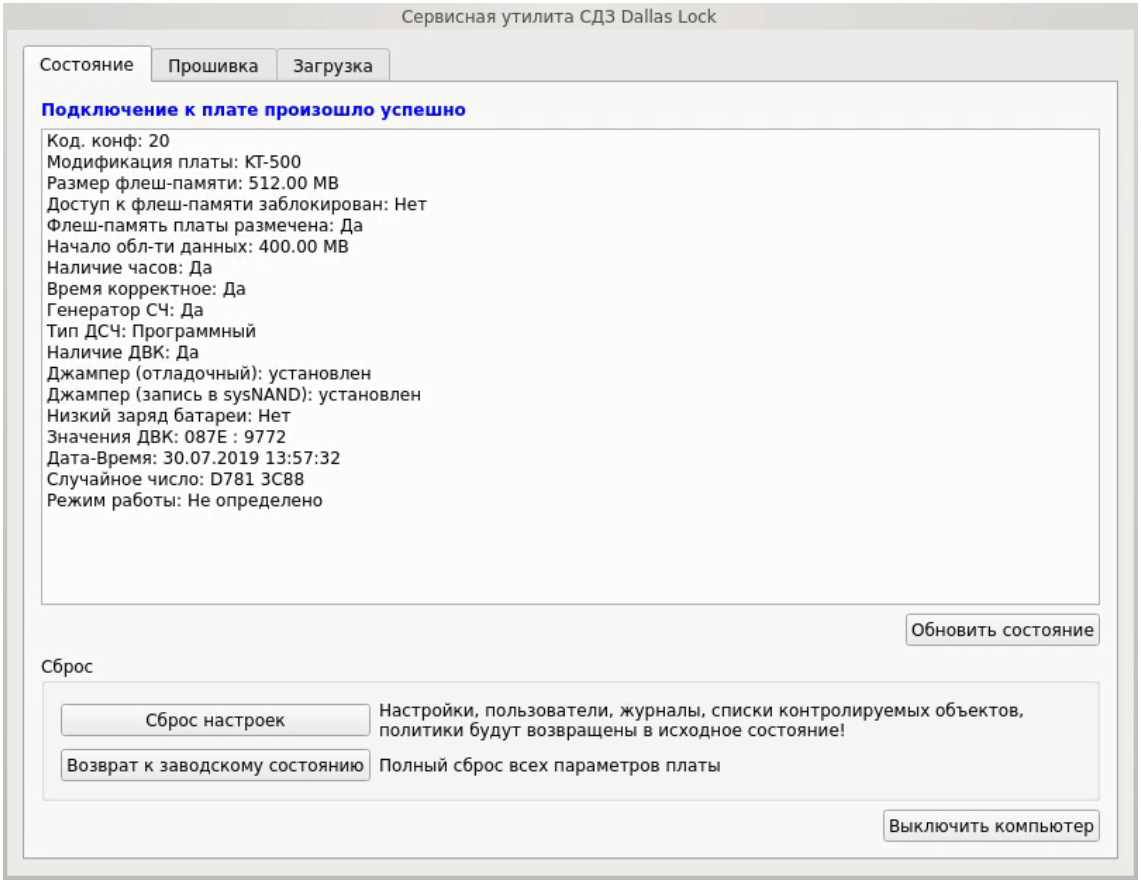


Рисунок 50 — Сервисная утилита

Запуск сервисной утилиты KtService

— 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 «2» и «3» (см. рисунок 1 и рисунок 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» (см. рисунок 2, рисунок 5, рисунок 3 и рисунок 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.

Интерфейс сервисной утилиты

Вкладка «Состояние»:

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

— «Обновить состояние» — происходит обновление таблицы;

— «Сброс 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.

Вкладка «Прошивка» (рисунок 51):

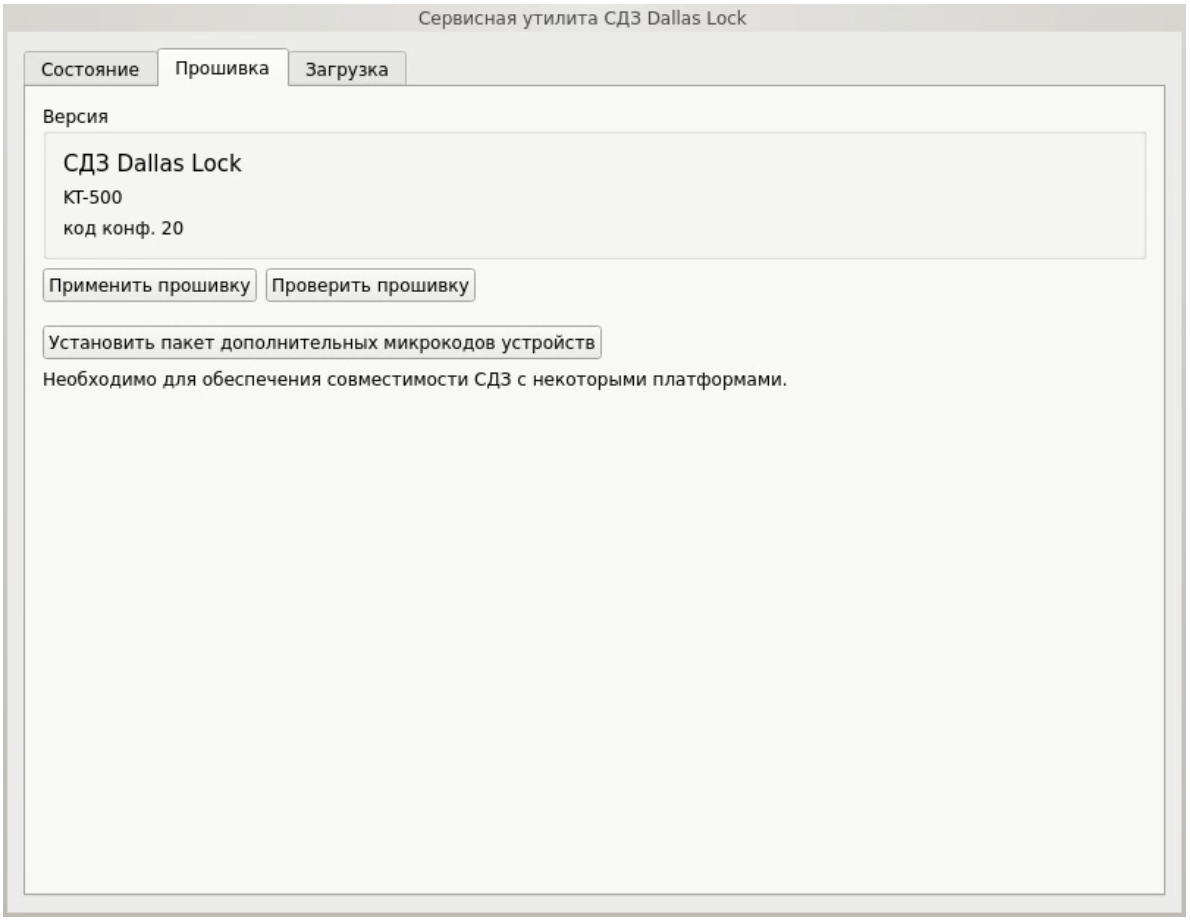


Рисунок 51 — Сервисная утилита. Вкладка «Прошивка»

— «Применить прошивку» — при нажатии появится диалог выбора файла прошивки платы. Требуется выбрать файл с расширением .amfrm. Далее необходимо будет выбрать один из вариантов возможной прошивки и подтвердить установку, после чего она будет применена (подробное описание процедуры обновления описано в п. 3.2.11);

— «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».

Вкладка «Загрузка» (рисунок 52):

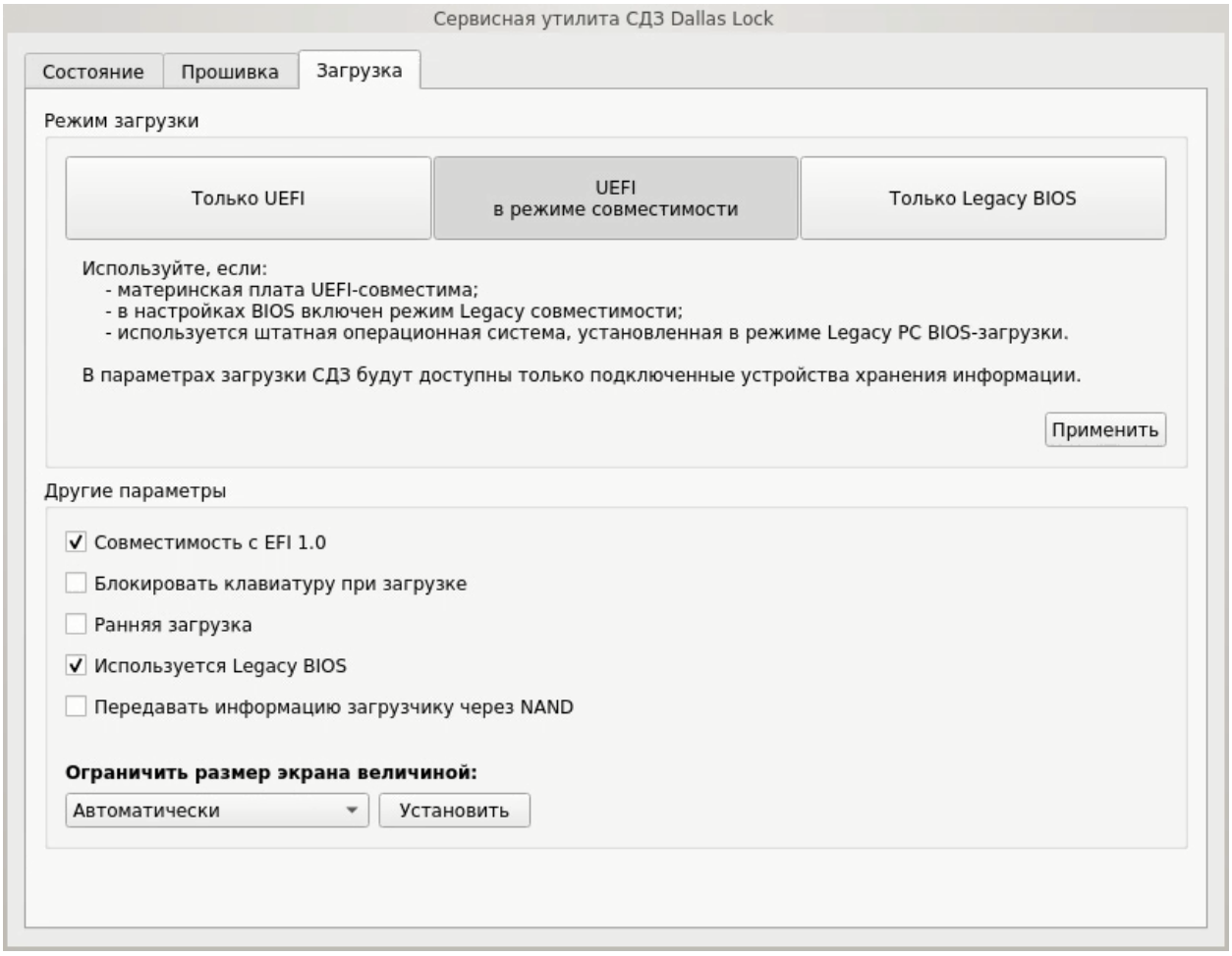


Рисунок 52 — Сервисная утилита. Вкладка «Загрузка»

Доступны следующие режимы загрузки с кратким описанием:

— «Только UEFI»;

— «UEFI в режиме совместимости»;

— «Только Legacy BIOS».

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

Другие параметры загрузки содержат чекбоксы:

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

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

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

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

— «Передавать информацию загрузчику через NAND» — устанавливается для передачи информации в загрузчик среды исполнения прошивки СДЗ через NAND.

3.2.10 Перечень возможных неисправностей в процессе использования изделия

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

3.2.11 Порядок выключения изделия

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

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.

3.2.12 Порядок обновления изделия

Обновление программной части изделия доступно через сервисную утилиту «KtService» на вкладке «Прошивка» (п.п. 3.2.92) и осуществляется следующим образом:

— предприятие-изготовитель доводит до потребителя информацию о выпуске обновлений изделия и устраненных в новых версиях недостатках по электронной почте письмом с вложенным документом, подписанным ЭП;

— потребитель при получении указанной информации выполняет загрузку обновления с сайта предприятия-изготовителя в виде дистрибутива, информация о контрольной сумме которого содержится на сайте предприятия-изготовителя, а также файл электронной подписи;

— перед установкой обновления потребитель выполняет проверку подлинности электронной подписи (согласно инструкции, представленной на сайте предприятия-изготовителя), расчет[1] и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте предприятия-изготовителя;

— в случае успешной проверки электронной подписи и совпадения контрольных сумм, потребитель выполняет установку обновлений. Если проверка электронной подписи и контрольных сумм не пройдена, потребитель не выполняет установку обновлений и обращается к предприятию-изготовителю изделия;

— для установки обновления необходимо запустить сервисную утилиту KtService, после чего убедиться, что разрешена запись в системную область энергонезависимой памяти СДЗ (порядок запуска подробно описан в п.п. 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»,

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

подтвердить установку, после чего она будет применена;

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

- для UEFI-режима (если материнская плата UEFI-совместима и используется ШОС, установленная в режиме UEFI-загрузки): из группы элементов «Режим загрузки» нажать кнопку «Только UEFI», из группы элементов «Другие параметры» установить галочки «Совместимость с EFI 1.0», «Блокировать клавиатуру при загрузке», «Ранняя загрузка» и «Используется Legacy BIOS» при необходимости (см. п.п. 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 галочки «Совместимость с EFI 1.0», «Блокировать клавиатуру при загрузке» и «Ранняя загрузка» при необходимости (см. п.п. 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».

3.3 Действия по реализации функций безопасности среды функционирования

Дополнительных действий по реализации функций безопасности среды функционирования (кроме описанных в п. 3.1) не требуется.

4 ПРОВЕРКА СДЗ DALLAS LOCK

4.1 Идентификация и аутентификация

Проверка данных идентификации и аутентификации субъектов по их именам и паролям (аппаратным идентификаторам) реализуется в следующем порядке:

— выдача приглашения на вход в систему;

— проверка возможности входа пользователя с введенным именем учётной записи;

— при использовании аппаратного идентификатора проверяется правильность введенных данных в соответствии с настройками использования АИ для данной учётной записи пользователя;

— проверяется правильность указанного пользователем пароля;

— проверка установленного атрибута «Отключен» для данной учётной записи;

— проверка допустимого времени работы для пользователя.

Испытания проводятся в следующем порядке:

— последовательно проводится авторизация и вход на рабочую станцию администратором и пользователем как в установленное, так и в неустановленное время работы;

— осуществляются попытки авторизации при вводе неверного имени / пароля / предъявлении стороннего аппаратного идентификатора.

Ожидаемые результаты проверки:

— при успешном выполнении всех проверок происходит дальнейшая загрузка с предоставлением прав доступа, заданных для данной учётной записи пользователя;

— при вводе незарегистрированного имени, неверного пароля или предъявлении стороннего АИ, доступ блокируется;

— события по вводу паролей (как правильных, так и неправильных) регистрируются в журнале входов.

4.2 Регистрация событий

В СДЗ Dallas Lock ведется журнал, регистрирующий следующие категории событий:

— «Входы» — фиксируются все события, связанные с загрузкой компьютера и входом в ОС;

— «Администрирование» — ведется учет событий, связанных с администрированием и результатами этих действий;

— «Учётные записи» — фиксируются действия по изменению учётных записей;

— «Целостность» — ведется учет всех событий, связанных с контролем / пересчетом / завершением контроля целостности.

Испытания проводятся в следующем порядке:

— осуществляется попытка входа с пустым именем пользователя;

— авторизация в СДЗ пользователем admin или auditor;

— проверяется содержимое перечисленных категорий в журнале.

Ожидаемые результаты проверки:

В журнал заносится запись о событии попытки входа с незаданным именем пользователя с

указанием:

— даты и времени;

— субъекта, осуществляющего регистрируемое действие;

— события, произошедшего в результате действий субъекта;

— результат выполнения, включая попытки несанкционированного доступа;

— описания события.

4.3 Администрирование параметров СДЗ Dallas Lock

Проверка изоляции функций интерфейса администратора СДЗ Dallas Lock в сравнении с другими пользователями такого же интерфейса.

Испытания проводятся в следующем порядке:

— осуществляется вход на рабочую станцию администратором;

— администратором назначаются соответствующие политики безопасности на определенные полномочия пользователю;

— осуществляется вход пользователя;

— сравниваются функциональные возможности интерфейса СДЗ Dallas Lock пользователя и администратора;

— осуществляется попытка получить доступ к функциям оболочки управления интерфейса СДЗ Dallas Lock с повышением назначенных полномочий.

Ожидаемые результаты проверки:

— пользователю обеспечена доступность функционала интерфейса СДЗ Dallas Lock в соответствии с его полномочиями и его логическая изолированность от других таких же интерфейсов;

— невозможность получения доступа пользователей к функционалу интерфейса администратора.

4.4 Контроль целостности компонентов ТС

1. Проверяется наличие средств контроля целостности данных, а именно объектов файловой системы, реестра Windows, областей дисков, BIOS/CMOS.

Испытания проводятся в следующем порядке:

— осуществляется вход на рабочую станцию администратором;

— на вкладке «Контролируемые объекты» проверяется доступность кнопок для добавления в список объектов с контролируемой целостностью объектов файловой системы, реестра Windows, областей дисков.

— в окне редактирования параметров пользователя проверяется наличие атрибута «запретить работу при нарушенной целостности», состояние которого определяет возможность загрузки ОС при обнаружении нарушения целостности.

Ожидаемые результаты проверки:

— выполнение вышеперечисленных шагов возможно;

— установлено наличие функции контроля целостности загружаемой операционной системы;

— установлено наличие возможности блокирования загрузки операционной системы при нарушении целостности загружаемой программной среды.

2. Проверяется наличие и работа средств контроля состава компонентов аппаратного обеспечения ТС.

Испытания проводятся в следующем порядке:

— осуществляется вход на рабочую станцию администратором;

— в параметрах пользователя auditor включается атрибут «запретить работу при нарушенной целостности», если он отключен;

— подключается USB-накопитель к ТС;

— в группе «USB-устройства» раздела «Аппаратная конфигурация» вкладки «Контролируемые объекты» установить контроль на подключенный USB-накопитель;

— вернуться в окно авторизации;

— отключить подключенный ранее USB-накопитель;

— выбрать действие «Загрузка» и авторизоваться в СДЗ пользователем auditor.

Ожидаемые результаты проверки:

— выполнение вышеперечисленных шагов возможно;

— установлено, что в ходе контроля целостности обнаружено изменение контролируемой аппаратной конфигурации, загрузка ШОС невозможна.

5 СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

В процессе установки, настройки и проверки СДЗ Dallas Lock системному программисту выводятся сообщения об удачно или неудачно выполненной операции.