УТВЕРЖДЕН
ПФНА.501410.004 РЭ-ЛУ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА

Dallas Lock

(версия изделия 1.0.17)

Руководство по эксплуатации

ПФНА.501410.004 РЭ

АННОТАЦИЯ

Данное руководство по эксплуатации распространяется на изделие «Средство доверенной загрузки уровня базовой системы ввода-вывода «Dallas Lock» ПФНА.501410.004 (далее — СДЗ УБ Dallas Lock, СДЗ УБ, изделие).

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

Руководство состоит из 4 разделов и включает в себя:

- раздел 1: общее описание назначения, технические характеристики и возможности СДЗ УБ Dallas Lock, состав изделия, а также устройство и работа механизмов СДЗ УБ Dallas Lock;
- раздел 2: сведения, необходимые для установки и эксплуатации изделия, подготовки его к работе;
- раздел 3: описание задач по администрированию изделия, описание пользовательского интерфейса оболочки администратора СДЗ УБ Dallas Lock и функциональных возможностей, доступных администратору изделия;
- раздел 4: сведения о хранении и транспортировании изделия.

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

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

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

АИ	аппаратный идентификатор
ЕЦУ	Единый центр управления «Dallas Lock»
КС	контрольная сумма
НШОС	нештатная операционная система
ОС	операционная система
ПИН (ПИН-код)	пароль, предоставляющий доступ к защищенной памяти АИ
ПО	программное обеспечение
СДЗ УБ	средство доверенной загрузки уровня базовой системы ввода-вывода
СЗИ НСД	средство защиты информации от несанкционированного доступа
ТС	техническое средство
ШОС	штатная операционная система

1 ОПИСАНИЕ И НАЗНАЧЕНИЕ

1.1 Назначение и технические характеристики

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

Обозначение изделия: ПФНА.501410.004.

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

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

Изделие предназначено для использования в составе различных технических средств (далее — ТС), в том числе на ноутбуках, моноблоках и серверах.

Изделие функционирует как на автономных ТС, так и на компьютерах в составе локальной вычислительной сети.

Изделие может быть использовано как в сетях с доменной организацией, так и в одноранговых сетях.

СДЗ УБ Dallas Lock позволяет контролировать целостность реестра ОС Windows.

СДЗ УБ Dallas Lock поддерживает следующие виды аппаратных идентификаторов (далее — АИ):

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

СДЗ УБ 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 СВТ и (или) состава компонентов аппаратного обеспечения СВТ в ИС;
- нарушение целостности СДЗ УБ Dallas Lock, обход нарушителем компонентов СДЗ УБ Dallas Lock;
- несанкционированное изменение конфигурации СДЗ УБ Dallas Lock;
- преодоление или обход функций безопасности СДЗ УБ Dallas Lock;
- получение остаточной информации СДЗ УБ Dallas Lock из памяти ТС после завершения работы СДЗ УБ Dallas Lock;
- получение доступа к ресурсам СДЗ УБ Dallas Lock из программной среды ТС после завершения работы СДЗ УБ Dallas Lock;
- сбои и ошибки в процессе функционирования СДЗ УБ Dallas Lock.

СДЗ УБ Dallas Lock реализует следующие функции безопасности:

- разграничение доступа к управлению СДЗ УБ Dallas Lock;
- управление работой СДЗ УБ Dallas Lock;
- управление параметрами СДЗ УБ Dallas Lock;

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

- аудит безопасности СДЗ УБ Dallas Lock;
- идентификация и аутентификация;
- тестирование СДЗ УБ Dallas Lock, контроль целостности ПО и параметров СДЗ УБ Dallas Lock;
- контроль компонентов ТС;
- блокирование загрузки ОС средством доверенной загрузки;
- сигнализация СДЗ УБ Dallas Lock;
- обеспечение безопасности после завершения работы СДЗ УБ Dallas Lock.

СДЗ УБ Dallas Lock предоставляет следующие возможности:

1. Изделие реализует поддержку определенных ролей (категорий учетных записей пользователей — администратор, аудитор, пользователь).
2. Изделие реализует оповещение о событиях безопасности администратора.
3. Изделие обеспечивает возможность регистрировать в каждой записи аудита следующую информацию:
   - уникальный ID записи;
   - дату и время события, идентификатор субъекта, тип события и результат события (успешный или неуспешный);
   - описание события.
4. Изделие осуществляет регистрацию следующих событий, относящихся к безопасности ТС и самого изделия, в соответствующем журнале аудита:
   - события, связанные с процессом аутентификации;
   - события, связанные с управлением и конфигурацией;
   - события, связанные с изменениями учетных записей пользователя;
   - события, связанные с контролем целостности;
   - в случае возникновения события, не попадающего ни под одну из категорий, в журнал должно регистрироваться событие «Неизвестное событие».
5. Изделие реализует функции просмотра, фильтрации, очистки и экспорта журналов аудита.
6. Изделие реализует просмотр информации о записи журнала аудита.
7. В изделии реализован контроль заполнения журнала аудита.
8. В изделии реализован контроль целостности путем мониторинга неизменности следующих контролируемых объектов:
   - объекты файловой системы (далее — ФС);
   - реестр;
   - области диска;
   - содержимое энергонезависимой памяти CMOS;
   - таблицы SMBIOS (с возможностью задать маску, определяющую состав контролируемых байтов);
   - таблицы BIOS;
   - аппаратная конфигурация;
   - программное обеспечение СДЗ УБ Dallas Lock.
9. В изделии предоставляется выбор алгоритма расчета контрольной суммы из CRC32, ГОСТ Р 34.11-94, MD5 для объектов ФС, реестра, областей жесткого диска, программного обеспечения СДЗ УБ Dallas Lock.
10. В изделии обеспечена автоматическая проверка целостности контролируемых объектов, осуществляемая после авторизации пользователя в изделии и по запросу уполномоченного пользователя, основываясь на идентификационной информации компонентов: «идентификатор», «тип», «производитель», «статус» для верификации неизменности состава аппаратного обеспечения ТС. Реализован вывод результатов контроля загрузчика ШОС в окно проверок после авторизации пользователя.
11. В изделии реализован механизм тестирования (самотестирования) критичных функций безопасности:
    - контроль целостности;
    - идентификация и аутентификация;
    - создание, удаление учетной записи пользователя;
    - аудит событий безопасности.

12. В изделии реализован механизм парольной и аппаратной аутентификации.

13. В изделии реализована возможность регулирования политики паролей.

14. В изделии реализована возможность отображения имени последнего вошедшего пользователя.

15. Изделие блокирует учетную запись пользователя при превышении количества попыток авторизации, предусмотренных политикой безопасности.

16. Изделие осуществляет оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему.

17. Изделие осуществляет идентификацию и аутентификацию пользователя с помощью имени учетной записи и пароля и/или аппаратного идентификатора до выполнения действий по загрузке операционной системы или до выполнения действий администратора по управлению изделием. При успешной проверке идентификатора и аутентификационных данных в случае отсутствия ошибок пользователю разрешаются дальнейшие действия в системе.

18. Изделие предоставляет возможность использования при авторизации пользователя как идентификационной, так и аутентификационной информации, записанной на аппаратном идентификаторе пользователя.

19. В изделии осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

20. В изделии предоставлена возможность сохранения конфигурации с данными об учетных записях пользователей, контролируемых объектах и политиках безопасности в специальном файле конфигурации в формате *.xml на различные носители информации.

21. В изделии реализована возможность настройки запрета доступа учетной записи пользователя при возникновении следующих категорий событий:

- при нарушении целостности;
- при работе в неразрешенное время входа;
- при блокировке этой учетной записи;
- при отключении этой учетной записи.

22. В изделии реализовано блокирование загрузки ОС при:

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

23. В изделии реализована функция назначения загрузочного устройства, с которого и только с которого будет происходить загрузка ОС, либо возможность выбора в качестве загрузочного устройства «Любое устройство». В изделии реализована возможность менять загрузочное устройство. Реализована возможность обновления списка доступных для выбора загрузочных устройств.

24. В изделии реализована возможность предоставлять надежные метки времени путем установки значений, взятых из часов системной платы.

25. В изделии реализована очистка оперативной памяти ТС при перезагрузке с целью исключения возможности доступа к ресурсам изделия и памяти ТС после завершения работы изделия.

26. В изделии реализована возможность централизованного управления в составе домена безопасности в качестве клиента Единого центра управления «Dallas Lock» (далее — ЕЦУ). Обеспечиваются:

- возможность ввода/вывода клиента в/из домена безопасности;
- сбор журналов аудита в единую систему хранения ЕЦУ или базу данных;
- отображение текущего статуса/состояния клиента СДЗ УБ Dallas Lock;
- синхронизация политик/учетных записей;
- выполнение заданий от ЕЦУ (получение отчетов, сохранение и применение конфигураций на клиенте, тестирование функций СДЗ УБ Dallas Lock);

- включение/выключение/перезагрузка клиента;
- разблокировка учетных записей;
- сигнализация о событиях НСД в реальном времени;
- запись в память токенов информации о пользователе в формате, поддерживаемом СДЗ УБ Dallas Lock.

1.2 Состав изделия

СДЗ УБ Dallas Lock состоит из следующих основных компонентов:

1. Загрузчик среды исполнения.

Обеспечение получения управления над процессом загрузки компьютера. Задача загрузчика среды исполнения — загрузить ШОС или выполнить чтение кода среды исполнения функций безопасности с накопителя ПЭВМ и передать ей управление.

2. Среда исполнения функций безопасности.

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

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

3. Оболочка функций безопасности.

Оболочка функций безопасности реализует полезные функциональные возможности СДЗ УБ Dallas Lock, связанные с основной задачей, и состоит из следующих подсистем:

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

Изделие поставляется в составе, указанном в Таблице 1.

Таблица 1

№	Наименование	Обозначение	Кол-во шт.	Примечание
1	USB-flash накопитель		1	
2	Программное обеспечение «Средство доверенной загрузки уровня базовой системы ввода-вывода «Dallas Lock»	ПФНА.501410.004	1	На USB-flash накопителе
3	Описание применения	ПФНА.501410.004 31	1	-/-
4	Руководство оператора (пользователя)	ПФНА.501410.004 34	1	-/-
5	Руководство по эксплуатации	ПФНА.501410.004 РЭ	1	-/-
6	Инструкция по использованию ЕЦУ	ПФНА.501410.004 И3	1	-/-
7	Программа подсчета контрольных сумм		1	-/-

8	Формуляр	ПФНА.501410.004 ФО	1	Печатный вариант
9	Краткое руководство пользователя		1	-/-
10	Копия сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00		1	-/-
11	Идентификатор СЗИ		1	Вклеен в раздел 7 формуляра на изделие
12	Упаковка		1	

При поставке более чем одного изделия комплектность определяется договором.
Поставка модуля «Единый центр управления Dallas Lock» (файлы uccInst.exe, uccInst, uccAgentInst.exe и uccAgentInst) определяется договором.

1.3 Устройство и работа

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

Среда исполнения функций безопасности запускает оболочку функций безопасности.

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

Оболочка функций безопасности СДЗ УБ Dallas Lock отображает окно авторизации.

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

1.4 Маркировка и упаковка

Маркировка СДЗ УБ Dallas Lock производится в соответствии с требованиями Технических условий ПФНА.501410.004 ТУ, а также документом «Технология производства, маркировка и упаковка» ПФНА.501410.004 И2 и включает в себя маркировку упаковочной коробки для USB-flash накопителя, маркировку USB-flash накопителя и маркировку формуляра.

Маркировка формуляра ПФНА.501410.004 ФО содержит:

- лицензионный номер изделия;
- год, месяц, число упаковки (указаны в разделе 7 «Свидетельство об упаковке и маркировке» в поле «Дата упаковки» печатной копии Формуляра ПФНА.501410.004 ФО, поставляемого в составе комплекта СДЗ УБ Dallas Lock);
- идентификатор СЗИ (вклеен в раздел 7 «Свидетельство об упаковке и маркировке» в поле «Маркирован идентификатором» печатной копии Формуляра ПФНА.501410.004 ФО, поставляемого в составе комплекта СДЗ УБ Dallas Lock);
- соответствующие подписи и печати.

Маркировка упаковочной коробки с USB-flash накопителем с СДЗ УБ Dallas Lock соответствует требованиям технической документации предприятия-производителя, наносится печатным способом и содержит заводской номер изделия.

Маркировка USB-flash накопителя с СДЗ УБ Dallas Lock соответствует требованиям технической документации предприятия-производителя, наносится печатным способом и содержит идентификатор СЗИ.

Упаковка изделия обеспечивает защиту и сохранность при транспортировании и хранении изделия

согласно требованиям раздела 6 Технических условий ПФНА.501410.004 ТУ.

2 УСТАНОВКА И УДАЛЕНИЕ ИЗДЕЛИЯ

2.1 Эксплуатационные ограничения и технические требования

Изделие функционирует независимо от ШОС, поэтому требования к операционной системе не предъявляются.

СДЗ УБ Dallas Lock исправно работает на ТС (персональные и портативные компьютеры, серверы). Минимальные аппаратные требования к ТС для установки СДЗ УБ Dallas Lock:

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

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

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

2.2 Меры безопасности при подготовке изделия к установке

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

Перед установкой изделия необходимо осмотреть USB-flash накопитель с изделием на отсутствие механических повреждений. При их наличии изделие к эксплуатации не допускается.

2.3 Ограничения по эксплуатации

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

Перед началом эксплуатации необходимо активировать опцию: «Пароли: минимальная длина» (значение — не менее 8 символов).

2.4 Ограничения по установке

Установку изделия необходимо производить в соответствии с количеством защищаемых АРМ, указанном в разделе 6 «Свидетельство о приемке» в графе «Количество защищаемых АРМ» в формуляре ПФНА.501410.004 ФО.

Дополнительная установка СДЗ УБ (сверх указанного количества) допускается только при переносе СДЗ УБ на другое ТС или его восстановлении.

В процессе эксплуатации изделия рекомендовано использовать сертифицированные обновления по результатам испытаний, вызванных внесением изменений в СДЗ УБ.

Доступ к сертифицированным обновлениям по результатам испытаний, вызванных внесением изменений в СДЗ УБ, возможен только в рамках действующего технического сопровождения.

В процессе эксплуатации СДЗ УБ запрещается:

- коммерческое тиражирование СДЗ УБ;
- модификация, декомпиляция или дизассемблирование СДЗ УБ;
- обработка USB-flash накопителя с СДЗ УБ системными программами и утилитами, работающими на низком уровне.

2.5 Предварительная подготовка

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

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

1. Для UEFI-режима (материнская плата UEFI-совместима и используется ШОС, установленная в режиме UEFI-загрузки):
   - включить режим UEFI Boot (Enabled);
   - отключить режим CSM (Disabled);
   - отключить режим FastBoot (Disabled);
   - в Setup BIOS удалить установленные ключи для SecureBoot и затем установить ключи, расположенные на USB-flash накопителе, в следующем порядке: db.auth, KEK.auth, PK.auth.

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

2. Для Combo-режима (если материнская плата UEFI-совместима):
   - проверить, что режим CSM включен (Enabled);
   - отключить режим FastBoot (Disabled).

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

Также в настройках Setup BIOS необходимо установить загрузку с жесткого диска (загрузчика) с ШОС и необходимо отключить загрузку через сетевую карту PXE Option ROM.

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

Для установки СДЗ УБ Dallas Lock необходимо вставить в USB-порт ТС USB-flash накопитель с изделием.

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

Примечание. Дальнейшая установка СДЗ УБ по умолчанию производится с использованием PartitionTool — программы для управления разделами диска.

Возможна ручная разметка диска. Для этого необходимо до начала установки осуществить следующие действия:

1. Создать раздел на диске не менее 500 Мб с использованием вспомогательных средств (например, gparted, ntfsresize и др.).
2. При создании раздела указать:
   GUID раздела: 42465331-3BA3-10F1-802A-4861696B7521
   UUID раздела: 42465331-3ba3-10f3-802a-4863696b7523
3. Отформатировать данный раздел в файловую систему FAT32 и назначить файловую метку тому — VBUILD_ROOT.
4. Перезагрузить ТС.

Далее перейти к процессу установки СДЗ УБ, описанному в разделе «Установка изделия».

2.6 Установка изделия

Для установки СДЗ УБ Dallas Lock необходимо подключить установочный USB-flash накопитель и произвести загрузку с подключенного установочного USB-flash накопителя (через Boot menu или установить USB-flash накопитель первым в boot order). После загрузки с установочного USB-flash накопителя на экране ТС будет отображено меню инсталлятора СДЗ УБ Dallas Lock (Рис. 1).

Рис. 1. Меню инсталлятора СДЗ УБ Dallas Lock

Перед началом установки СДЗ УБ Dallas Lock необходимо провести следующие тесты для проверки совместимости изделия с ТС:

- Read/write test — проверяет возможность вычитки и записи капсулы BIOS в микросхему; в случае успешного прохождения теста на экране отобразится сообщение «Read/write test: Success»; необходимо нажать любую клавишу для перезагрузки ТС.
- Read/patch test —проверяет возможность патчинга BIOS; в случае успешного прохождения теста на экране отобразится сообщение «Read/patch test: Success»; необходимо нажать любую клавишу для перезагрузки ТС.

Примечание. В случае провала любого из тестов необходимо зафиксировать результат и обратиться в службу технической поддержки. Лог файлы хранятся на инсталляционном накопителе в папках: \logs\[дата время].

В случае успешного прохождения тестов можно переходить к процедуре установки СДЗ УБ. Для этого необходимо в меню инсталлятора выбрать пункт «Install». Процедура установки осуществляется в два этапа:

- Осуществляется проверка разметки диска. Если диск не размечен предварительно вручную, то осуществляется автоматическая переразметка целевого диска с помощью программы PartitionTool, которая осуществляет поиск участка памяти, в который будет осуществляться сохранение всей служебной информации в процессе функционирования изделия. После данного этапа осуществляется автоматическая перезагрузка ТС.
- Чтение инсталлятором информации с BIOS ТС и сохранение прочитанных данных в dump, который в свою очередь сохраняет эти данные на установочный USB-flash накопитель в соответствующем каталоге. Далее осуществляется анализ dump с целью поиска участка, куда будет установлен UEFI-драйвер СДЗ УБ Dallas Lock. После нахождения участка начинается процесс модификации dump BIOS. Формируется новый dump со встроенным UEFI-драйвером СДЗ УБ Dallas Lock. После формирования нового dump осуществляется его запись в BIOS. В конце процесса установки осуществляется проверка верификации ТС.

При успешном окончании процедуры установки на экране ТС будет отображена надпись «Install: Success». Для дальнейшей работы необходимо нажать любую клавишу на клавиатуре для перезагрузки ТС и извлечь из ТС установочный USB-flash накопитель.

После перезагрузки ТС на экране будет отображено окно регистрации учетной записи администратора СДЗ УБ Dallas Lock (рис. 6).

2.7 Удаление изделия

Для удаления СДЗ УБ Dallas Lock нужно выполнить следующие действия:

1. Подключить к ТС инсталляционный USB-flash накопитель, с которого производилась установка СДЗ УБ Dallas Lock.
2. В оболочке администратора во вкладке «Сервис» выбрать пункт меню «О СДЗ Dallas Lock». Откроется окно с информацией о СДЗ УБ Dallas Lock (Рис. 2).

Рис. 2. Окно с информацией СДЗ УБ Dallas Lock

3. В открывшемся окне нажать кнопку «Удалить СДЗ». Откроется окно подтверждения удаления СДЗ УБ Dallas Lock (Рис. 3).

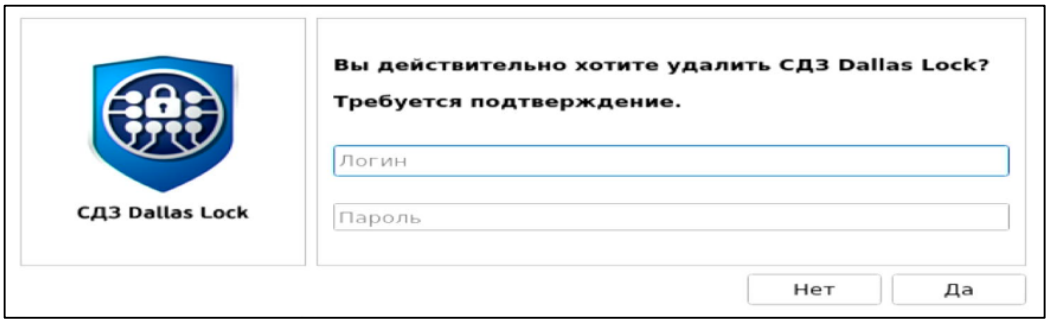


Рис. 3. Окно с информацией СДЗ УБ Dallas Lock

4. В открывшемся окне необходимо ввести данные учетной записи администратора, после чего нажать кнопку «Да».
5. Если к ТС не был подключен инсталляционный USB-flash накопитель, то изделие выдаст сообщение о том, что необходимо его подключить к ТС (Рис. 4).

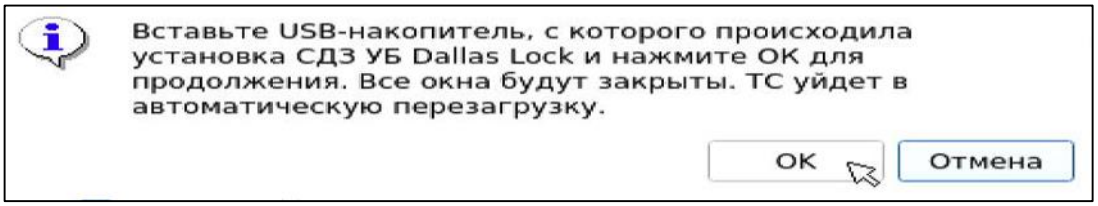


Рис. 4. Оповещение о том, что необходимо подключить инсталляционный USB-flash накопитель

6. Начнется процесс удаления СДЗ УБ Dallas Lock.
7. После успешного завершения процесса удаления на экране отобразится сообщение «Uninstall: Success».

Примечание. Для аварийного удаления СДЗ УБ Dallas Lock необходимо подключить к ТС инсталляционный USB-flash накопитель и запустить ТС. При загрузке ТС необходимо зажать комбинацию клавиш «Ctrl+Shift+Insert», после чего управление будет передано инсталляционному USB-flash накопителю. На экране отобразится меню аварийного удаления СДЗ УБ Dallas Lock (Рис. 5).

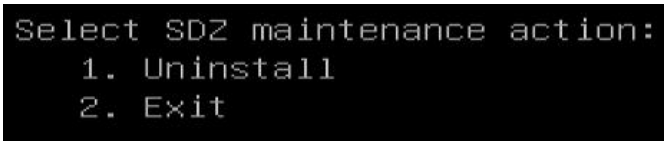


Рис. 5. Меню аварийного удаления

Для запуска аварийного удаления необходимо выбрать пункт меню «1. Uninstall». Начнется процесс аварийного удаления СДЗ УБ Dallas Lock. После успешного завершения процесса аварийного удаления на экране ТС появится сообщение «Uninstall: Success». Удаление завершено.

3 ИСПОЛЬЗОВАНИЕ ПО НАЗНАЧЕНИЮ

В настоящем руководстве по эксплуатации рассматриваются возможные действия пользователей СДЗ УБ Dallas Lock с правами аудитора и администратора. Возможные действия пользователя СДЗ УБ Dallas Lock изложены в Руководстве оператора ПФНА.501410.004 34.

3.1 Вход на защищенное ТС

При первом включении ТС с установленным СДЗ УБ Dallas Lock производится предварительная настройка СДЗ УБ (первичная инициализация).

После включения ТС появляется окно регистрации учетной записи администратора СДЗ УБ Dallas Lock (рис. 6), в котором необходимо обязательно указать имя пользователя и задать пароль к его учетной записи. После успешной регистрации учетных данных производится перезагрузка ТС.

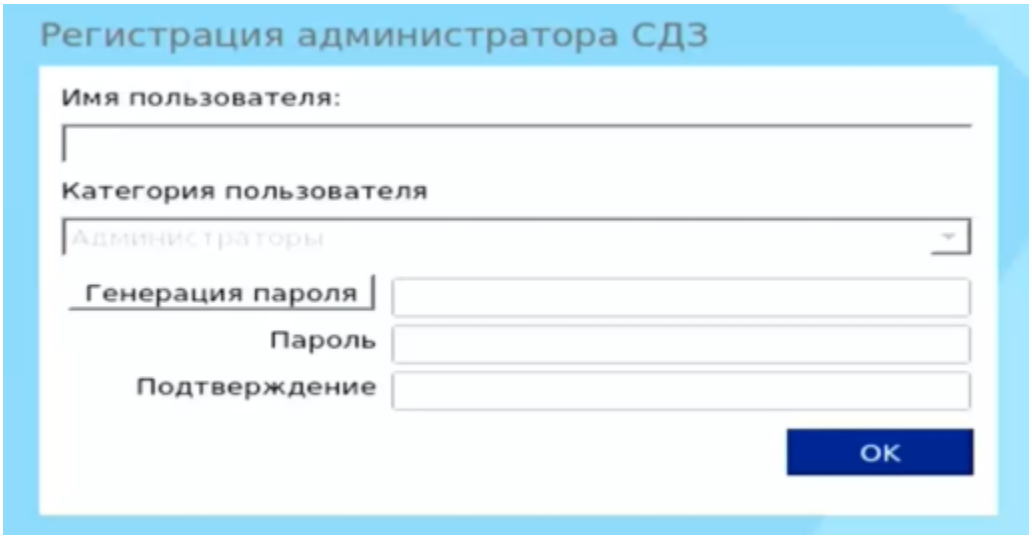


Рис. 6. Регистрация администратора СДЗ УБ Dallas Lock

После первичной регистрации администратора осуществляется автоматическая перезагрузка ТС.

После перезагрузки компьютера с установленной СДЗ УБ Dallas Lock появляется экран приглашения на вход в систему (рис. 7).

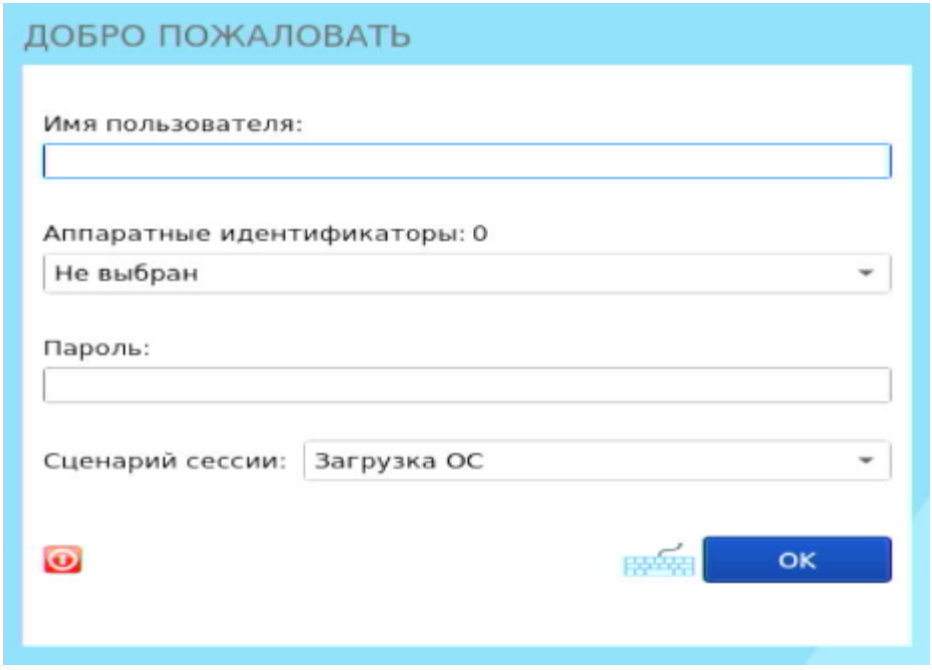


Рис. 7. Экран приглашения на вход в систему

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

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

Для входа на защищенный СДЗ УБ Dallas Lock компьютер необходимо:

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

Процедура авторизации с использованием АИ возможна одним из следующих способов:

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

Примечание. В случае предъявления не сопоставленного данной учетной записи пользователя АИ при попытке авторизации будет выведено соответствующее сообщение (рис. 8).

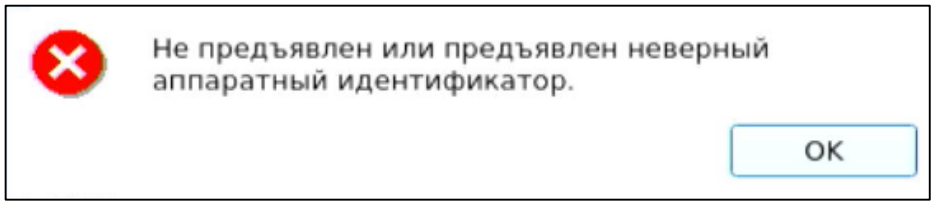


Рис. 8. Окно сообщения при предъявлении неверного АИ

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

2. Используя клавиатуру, ввести в поле «Имя пользователя» имя учетной записи, под которой пользователь зарегистрирован в СДЗ УБ Dallas Lock. В зависимости от настроек политики авторизации СДЗ УБ Dallas Lock в этом поле может оставаться имя учетной записи пользователя, выполнившего вход последним.

Примечание. Ввод имени доменной учетной записи пользователя должен производиться в одном из следующих форматов:

- [dom]\[name], где [dom] — полное или короткое имя домена, [name] — имя учетной записи;
- [name]@[dom], где [dom] — только полное имя домена.

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

Примечание. Для корректной работы доменной авторизации необходима настройка обратной зоны DNS, обслуживающего СДЗ УБ Dallas Lock, чтобы полученные СДЗ УБ Dallas Lock от DHCP-сервера IP-адреса DNS-серверов могли быть преобразованы в полное DNS-имя, из которого можно получить полный доменный суффикс для учетной записи. Например, СДЗ УБ получает IP-адрес 192.168.0.100 и IP-адрес DNS-сервера 192.168.0.1. DNS-сервер должен быть настроен таким образом, чтобы результатом запроса преобразования адреса 192.168.0.1 в имя было dns.dl.local. Таким образом, будет создана возможность авторизовываться пользователям по короткому суффиксу (user@dl) в полном доменном имени (user@dl.local).

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

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

4. Выбрать в выпадающем списке поля «Сценарий сессии» допустимую для учетной записи пользователя операцию по работе с системой:
   - «Загрузка ОС» — переход к загрузке ШОС;
   - «Смена пароля» — переход к смене пароля текущей учетной записи пользователя;
   - «Администрирование» — запуск оболочки администратора СДЗ УБ Dallas Lock (действие доступно только для пользователей категорий «Администратор» и «Аудитор»).
5. Нажать клавишу «Enter» или кнопку «ОК» на экранной форме.

В СДЗ УБ Dallas Lock сначала проверяется возможность входа пользователя с данным именем. В случае отсутствия в СДЗ УБ Dallas Lock учетной записи пользователя с указанным именем выводится соответствующее сообщение (рис. 9), осуществляется возврат к окну авторизации.

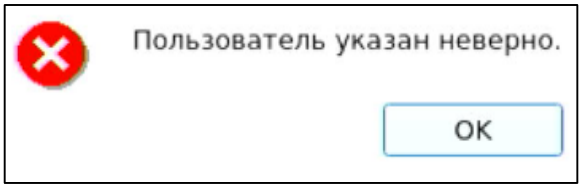


Рис. 9. Окно сообщения при неверном указании имени пользователя

Далее проверяется правильность указанного пользователем пароля. В случае успеха разрешается вход в систему, иначе выводится соответствующее сообщение (рис. 10), осуществляется возврат к окну авторизации.

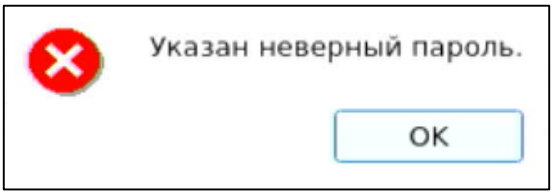


Рис. 10. Окно сообщения при неверном указании пароля учетной записи пользователя

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

При превышении количества попыток ввода пароля, предусмотренных политикой авторизации СДЗ УБ Dallas Lock, происходит автоматическая блокировка учетной записи пользователя на определенное время (задается политикой авторизации) или навсегда (до явной разблокировки администратором), если политике «Время блокировки учетной записи в случае ввода неправильных паролей» (см. «Настройка авторизации в СДЗ УБ Dallas Lock») присвоено значение «Не используется». Выводится соответствующее сообщение (рис. 11).

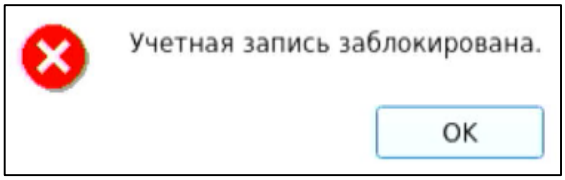


Рис. 11. Окно сообщения блокировки учетной записи пользователя

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

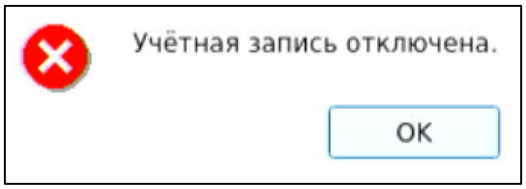


Рис. 12. Окно сообщения при попытке входа отключенного пользователя

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

В случае если не выбран аппаратный идентификатор, выводится соответствующее сообщение (рис. 13).

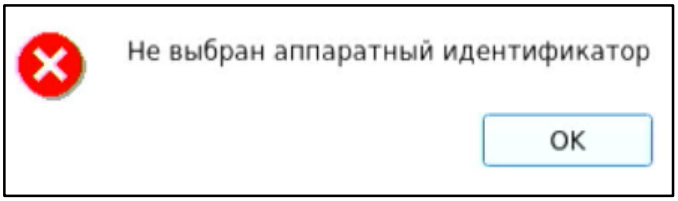


Рис. 13. Окно сообщения при попытке входа с невыбранным аппаратным идентификатором

Если память выбранного аппаратного идентификатора защищена ПИН-кодом, ПИН-код не введен или введен неверно, то выводится диалоговое окно с соответствующей ошибкой (рис. 14), осуществляется возврат к окну авторизации.

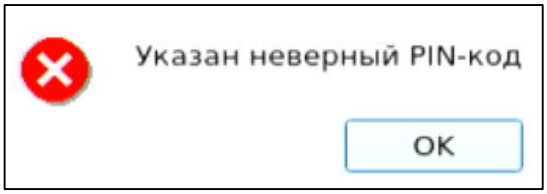


Рис. 14. Окно сообщения при неверном указании ПИН-кода аппаратного идентификатора

Далее осуществляется проверка допустимого времени работы согласно установленному для учетной записи пользователя расписанию. Если осуществляется попытка авторизации пользователя в неустановленное для него время работы, выводится соответствующее сообщение (рис. 15), осуществляется возврат к окну авторизации.

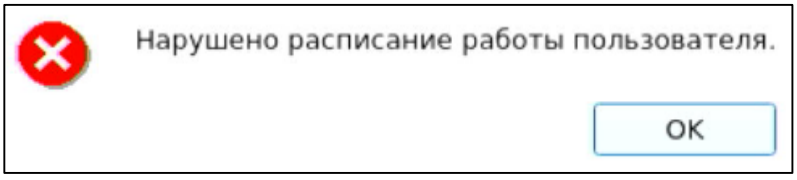


Рис. 15. Окно сообщения при попытке входа в неустановленное время работы

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

После успешной авторизации происходит переход к процедуре контроля целостности объектов, указанных в СДЗ УБ Dallas Lock. При успешном прохождении данной процедуры выводится соответствующее сообщение. При входе пользователей с полномочиями аудитора или администратора в окне контроля целостности помимо результата отображается ход выполнения процедуры контроля целостности объектов (рис. 16).

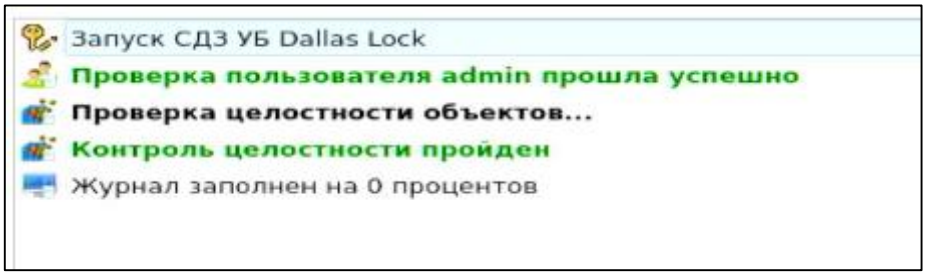


Рис. 16. Пример окна сообщения при успешном прохождении контроля целостности

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

В случае неуспешного прохождения процедуры контроля целостности при входе пользователя, учетной записи которого установлен атрибут «Запретить работу при нарушении целостности» (см. «Управление учетными записями пользователей»), выводится соответствующее сообщение (рис. 17). В окне доступны следующие действия:

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

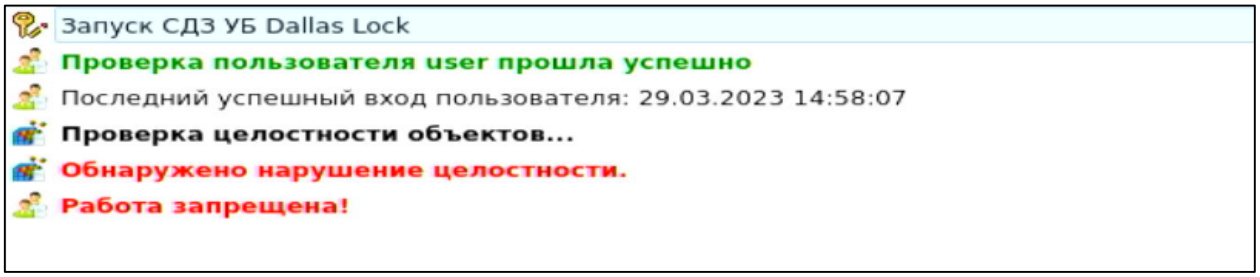


Рис. 17. Пример окна сообщения при неуспешном прохождении контроля целостности при входе непривилегированного пользователя

Если пользователю разрешено работать в системе с нарушенной целостностью контролируемых объектов, осуществляется вывод соответствующего сообщения (рис. 18), и вход в систему продолжается при нажатии кнопки «Далее». Осуществляется работа в соответствии с выбранным действием («Загрузка ОС», «Смена пароля» или «Администрирование»).

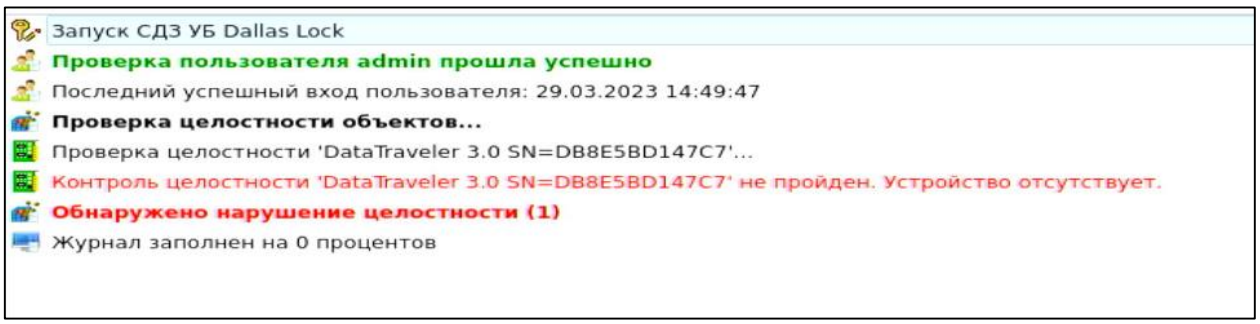


Рис. 18. Пример окна сообщения при неуспешном прохождении контроля целостности при входе пользователя

При успешном выполнении процесса контроля целостности производится переход к этапу проверки срока действия пароля для учетной записи пользователя. Загрузка ШОС и администрирование не доступны для учетной записи с истекшим сроком действия пароля. В случае истечения срока действия пароля проверяется разрешение для пользователя на смену своего пароля в соответствии с установленным атрибутом в настройках учетной записи пользователя «Запретить смену пароля пользователем». Если атрибут не установлен, выводится соответствующее сообщение о

необходимости изменения пароля (рис. 19) и происходит переход к процедуре смены пароля (см. «Смена пароля»).

Рис. 19. Сообщение о необходимости изменения пароля учетной записи

В случае, когда разрешение на смену пароля отсутствует, выводится сообщение о ошибке (рис. 20) и производится возврат к окну авторизации.

Рис. 20. Сообщение об истечении срока действия пароля

При попытке загрузки НШОС пользователем, у которого включен атрибут «Запретить загрузку нештатной ОС», изделие не позволяет осуществить загрузку НШОС. После такой попытки ТС уходит в перезагрузку. После перезагрузки ТС появляется окно с оповещением о том, что зафиксирована попытка загрузки нештатной ОС (Рис. 21).

Рис. 21. Окно сообщения при несанкционированной попытке загрузки нештатной ОС

При повторной попытке авторизации при условии, что у пользователя, которым осуществляется авторизация, включен атрибут «Запретить загрузку нештатной ОС», выдается соответствующее сообщение об обнаружении попытки недоверенной загрузки (Рис. 22). Для восстановления возможности загрузки ШОС необходимо обратиться к администратору.

Рис. 22. Окно предупреждения о попытке недоверенной загрузки ОС

Внимание! После события недоверенной загрузки повторная авторизация доступна только администратору безопасности и пользователям, у которых выключен атрибут «Запретить загрузку нештатной ОС».

Для предоставления пользователям, у которых включен атрибут «Запретить загрузку нештатной ОС», возможности авторизации администратор безопасности должен авторизоваться в изделии по сценарию «Администрирование». После авторизации в окне проверок администратору будет выведено сообщение о попытке недоверенной загрузки НШОС (Рис. 23). Это действие снимает запрет авторизации пользователей с включенным атрибутом «Запретить загрузку нештатной ОС».

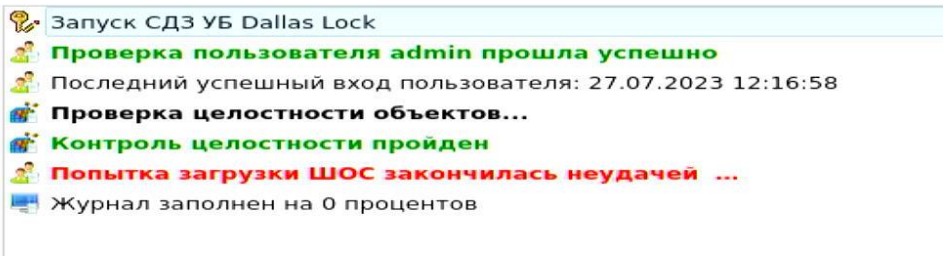


Рис. 23. Окно проверок. Запись «Попытка загрузки ШОС закончилась неудачей…»

Примечание. Попытки недоверенной загрузки регистрируются в журнале событий безопасности с описаниями «Обнаружена попытка недоверенной загрузки» или «Загрузочное устройство отсутствует, либо неисправно».
Запись «Загрузочное устройство отсутствует, либо неисправно» попадает в журнал один раз до момента сброса запрета путем авторизации пользователя с ролью администратора.

Запись «Обнаружена попытка недоверенной загрузки» заносится в журнал каждый раз при попытке загрузки ШОС пользователем, у которого включен атрибут «Запретить загрузку нештатной ОС», с момента срабатывания механизма и до его сброса путем авторизации пользователя с ролью администратора.

3.2 Смена пароля

При выборе действия «Смена пароля» осуществляется переход к диалоговому окну процедуры смены пароля учетной записи пользователя (рис. 24).

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

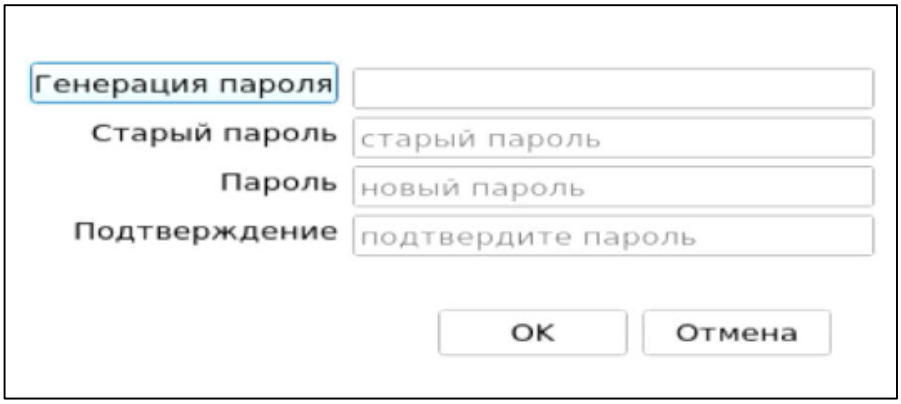


Рис. 24. Диалоговое окно смены текущего пароля учетной записи пользователя

Указанное действие недоступно, если администратором установлен атрибут в свойствах учетной записи пользователя «Запретить смену пароля пользователем». В этом случае при попытке смены пароля пользователем выдается соответствующее сообщение о действующем запрете (рис. 25).

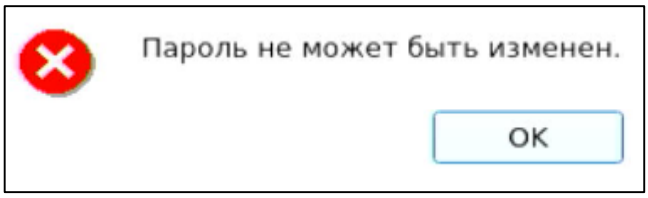


Рис. 25. Окно сообщения при запрете смены пароля пользователем

Для смены пароля необходимо корректно:

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

Также пользователь имеет возможность воспользоваться генератором паролей.

При несоответствии пароля требованиям политики сложности паролей выводится соответствующее сообщение (рис. 26 либо рис. 27), смена пароля не производится, осуществляется возврат к окну смены пароля.

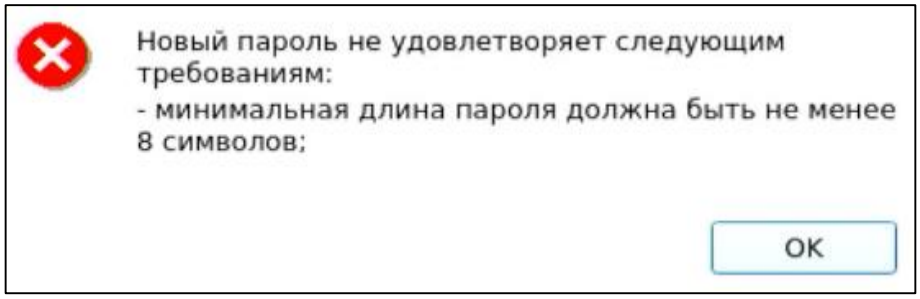


Рис. 26. Сообщение при несоответствии длины пароля учетной записи пользователя политике сложности паролей

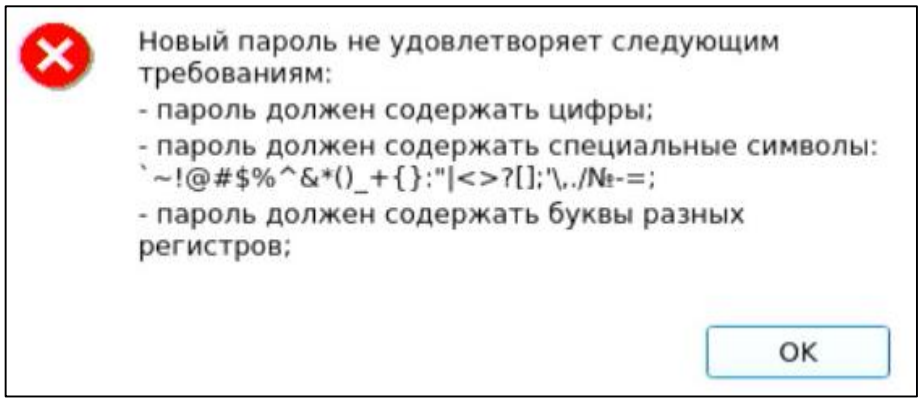


Рис. 27. Сообщение при несоответствии сложности пароля учетной записи пользователя политике сложности паролей

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

Если значения пароля в поле ввода и в поле повтора не совпадают, выводится соответствующее сообщение и осуществляется возврат к окну смены пароля (рис. 28).

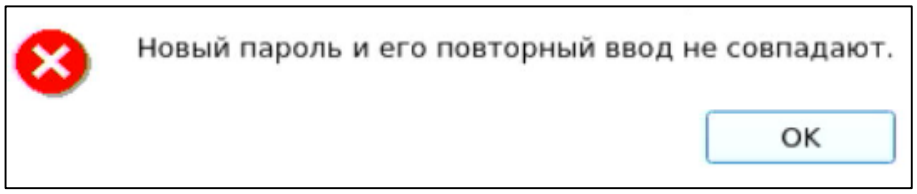


Рис. 28. Сообщение при несовпадении паролей

Дополнительная кнопка (выделена на Рис. 29) изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет неактивно.

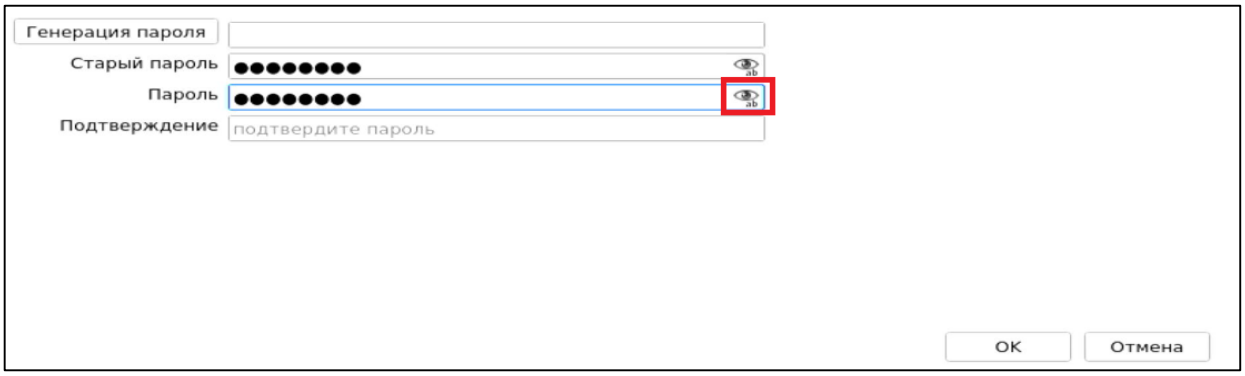


Рис. 29. Кнопка изменения скрытых символов на явные

При успешной смене текущего пароля учетной записи пользователя выводится соответствующее сообщение (рис. 30) и осуществляется возврат в окно авторизации.

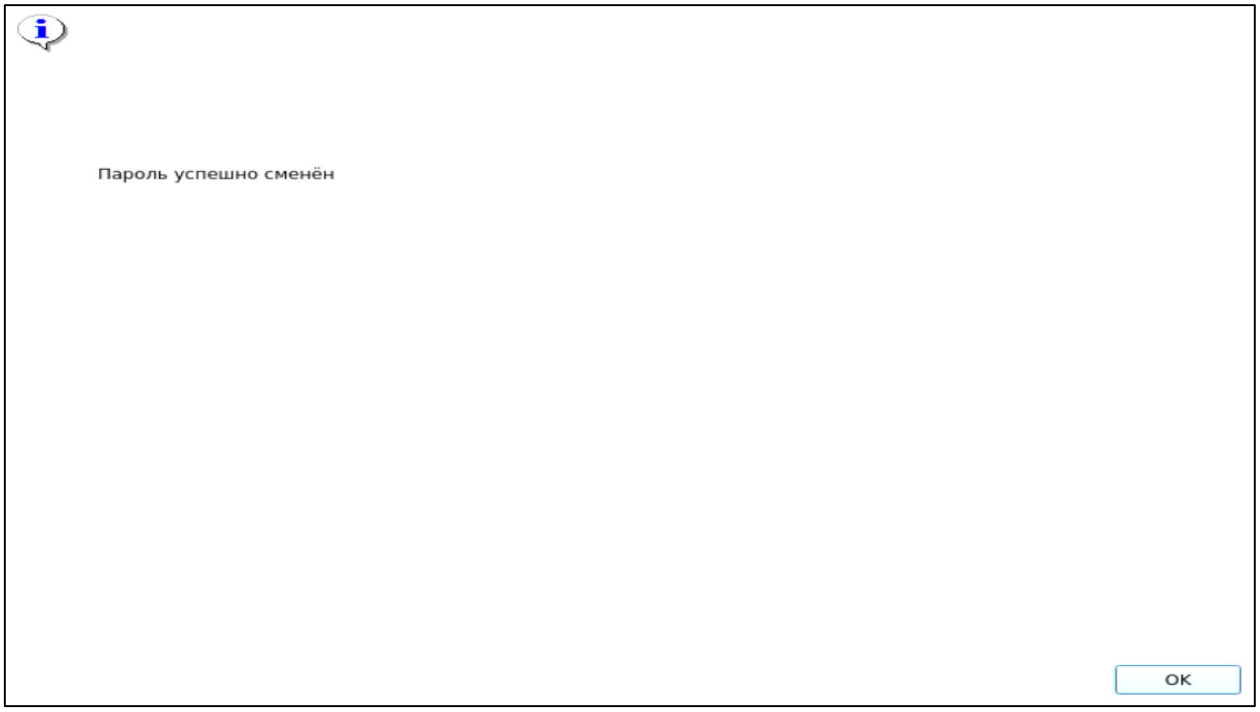


Рис. 30. Сообщение при успешной смене текущего пароля учетной записи пользователя

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

3.3 Администрирование СДЗ УБ Dallas Lock

Внимание! В процессе работы с оболочкой администратора исключено подключение и отключение USB-устройств.

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

В главном окне оболочки администратора (рис. 31) расположены вкладки, обеспечивающие доступ к соответствующим разделам:

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

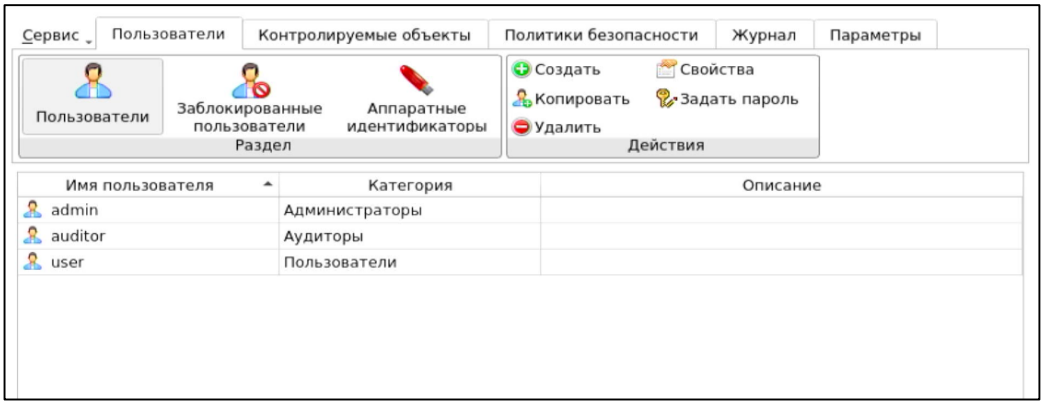


Рис. 31. Главное окно. Пользователи

При попытке запуска оболочки администратора пользователем, не входящим в категорию «Аудитор» или «Администратор», выводится соответствующее сообщение (рис. 32).

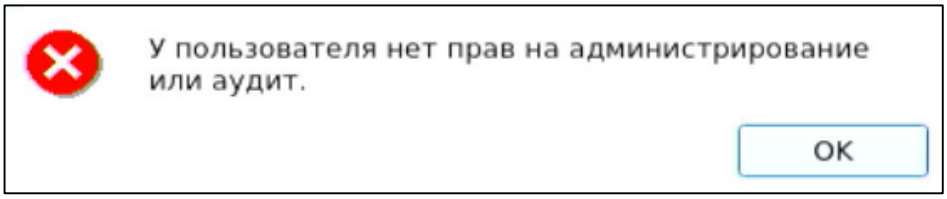


Рис. 32. Сообщение при запрете на администрирование или аудит СДЗ УБ Dallas Lock

3.3.1 Управление учетными записями пользователей

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

Возможны следующие действия с учетными записями пользователей:

- «Создать»;
- «Копировать»;
- «Удалить»;
- «Свойства»;
- «Задать пароль».

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

При нажатии кнопки «Свойства» выводится окно редактирования параметров учетной записи выбранного пользователя (рис. 33).

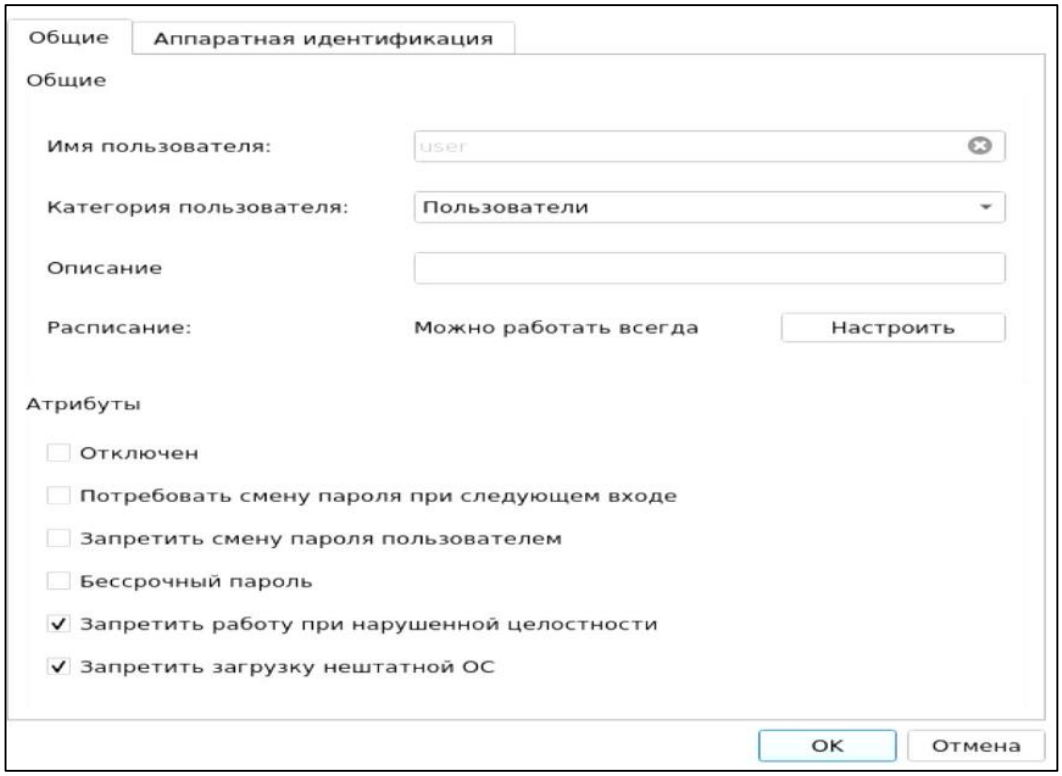


Рис. 33. Окно редактирования параметров учетной записи пользователя. Данные пользователя

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

- «Категория пользователя» — выбирается из выпадающего списка;

Примечание. Штатные пользователи, допущенные к работе на защищенном компьютере, не должны иметь категорию «Администраторы» или «Аудиторы».

- «Описание» — предназначено для текстового описания учетной записи пользователя (не более 95 символов);
- «Расписание» — установка разрешенного времени входа пользователя в систему (Рис. 34).

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

Для быстрой настройки предусмотрены дополнительные кнопки:

- «Разрешить все» — разрешено любое время для работы;
- «Запретить все» — запрещено любое время для работы;
- «Рабочее время» — устанавливается стандартный график работы (пн–пт, 09:00–18:00).

Также имеется возможность указать период действия учетной записи в нижней части окна «Период действия учетной записи».

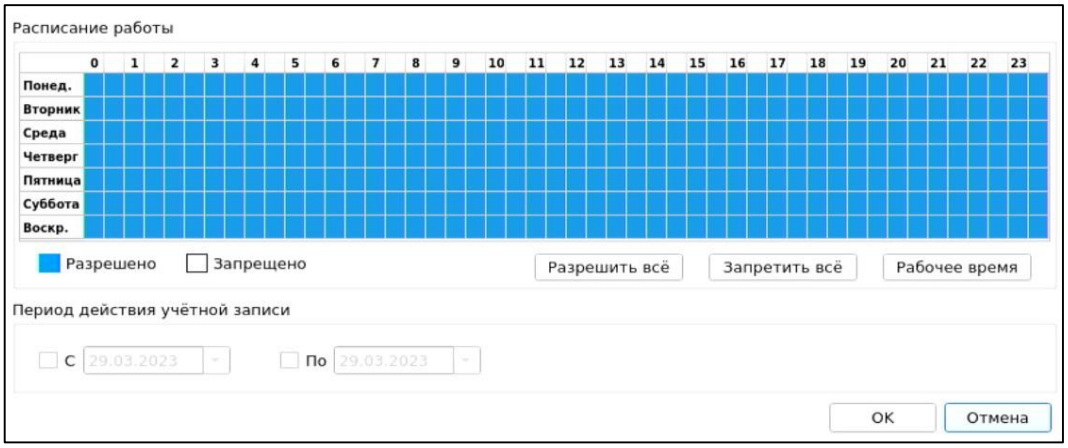


Рис. 34. Окно редактирования разрешенного времени работы в системе

Допустимо присвоение следующих атрибутов учетной записи пользователя (рис. 33):

- «Отключен» — учетная запись пользователя отключается, вход в систему невозможен до снятия атрибута администратором.
- «Потребовать смену пароля при следующем входе» — при входе пользователя в систему принудительно запускается диалоговое окно смены текущего пароля. Чекбокс данного атрибута отсутствует в окне редактирования доменной учетной записи пользователя.
- «Запретить смену пароля пользователем» — запрет для пользователя на смену своего пароля, в том числе и по истечении срока действия.

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

- «Бессрочный пароль» — на учетную запись пользователя не распространяется действие политики безопасности, которая устанавливает максимальный срок действия пароля. Установка данного атрибута не запрещает смену пароля учетной записи пользователем в любое время. Чекбокс данного атрибута отсутствует в окне редактирования доменной учетной записи пользователя.
- «Запретить работу при нарушенной целостности» — вход в систему пользователем при неуспешном прохождении процедуры контроля целостности объектов и компонентов ТС запрещается.
- «Запретить загрузку нештатной ОС» — запрет на загрузку ОС с носителя, отличающегося от указанного в поле «Загрузочное устройство» вкладки «Параметры» оболочки администратора.

На вкладке «Аппаратная идентификация» (рис. 35) возможно назначение АИ в следующем порядке:

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

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

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

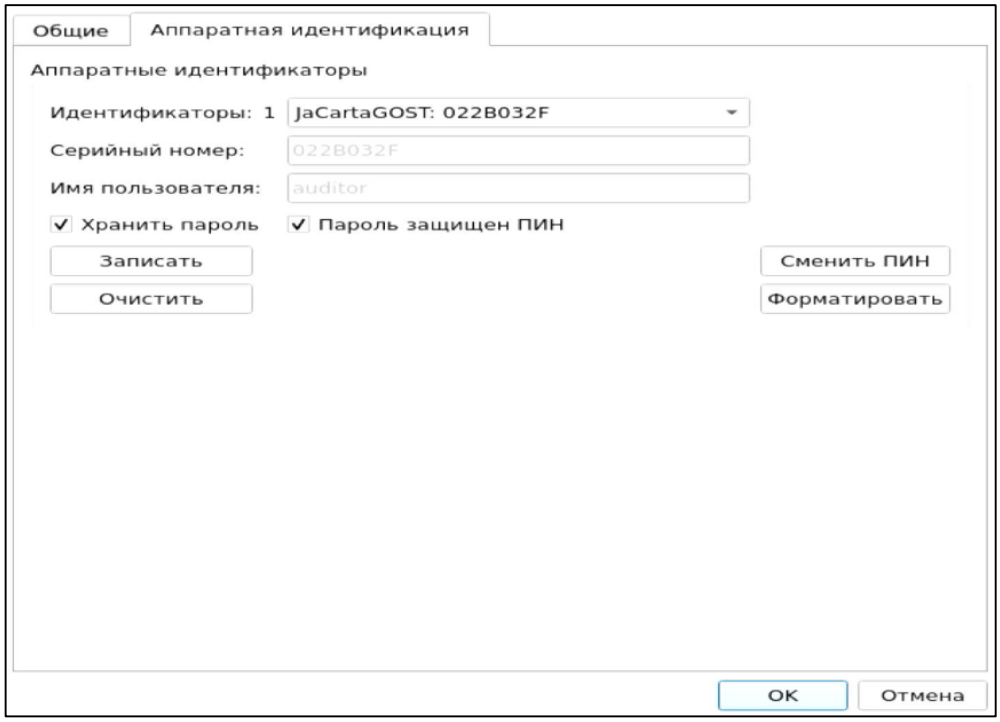


Рис. 35. Окно редактирования параметров учетной записи пользователя. Аппаратная идентификация

При необходимости возможно задать дополнительные параметры аппаратной идентификации:

- «Записать» — данная кнопка позволяет записывать в незащищенную и защищенную память АИ идентификационную и аутентификационную информацию (имя учетной записи пользователя, пароль). В этом случае в окне авторизации в соответствующие поля будет подставлена записанная информация, поля будут недоступны для редактирования. Запись только идентификационной информации (имя пользователя) осуществляется по нажатию кнопки без присвоения остальных возможных атрибутов. При успешной записи в поле «Имя пользователя» отобразится имя текущей учетной записи пользователя, поле будет недоступно для редактирования.

Примечание. Следует учитывать, что запись информации осуществляется не на все модели АИ.

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

Примечание. Хранение пароля в незащищенной памяти АИ с точки зрения информационной безопасности нежелательно.

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

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

- «Сменить ПИН» — данная кнопка позволяет сменить ранее назначенный ПИН-код учетной

записи пользователя для АИ. В окне «Изменение ПИН-кода» (рис. 36) ввести старый, новый ПИН-код и повторить ввод нового ПИН-кода.

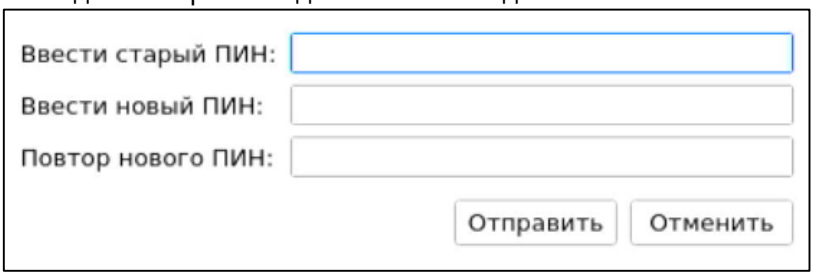


Рис. 36. Окно смены ПИН-кода

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

- «Форматировать» — данная кнопка позволяет провести форматирование АИ и очистить всю ранее записанную идентификационную и аутентификационную информацию (рис. 37).

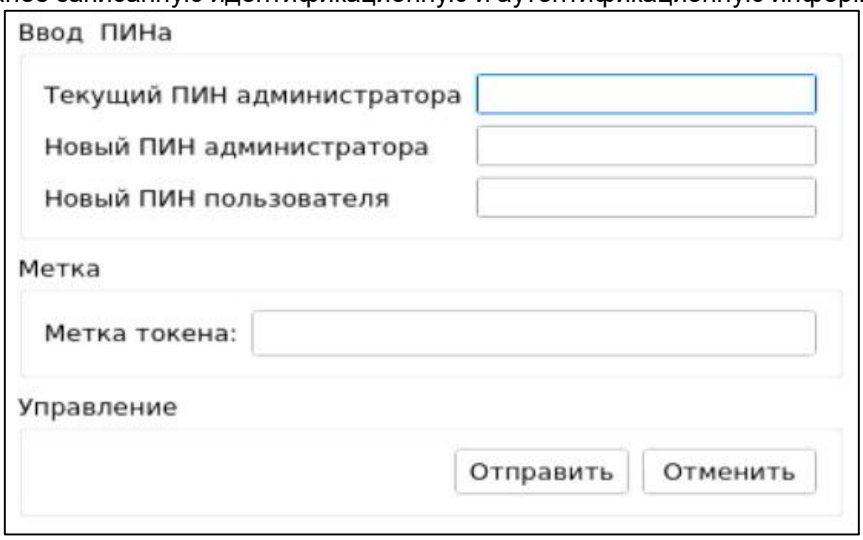


Рис. 37. Окно форматирования токена

В окне «Форматирование токена» необходимо ввести следующую информацию:

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

Нажать кнопку «Отправить».

При нажатии кнопки «Создать» выводится окно создания новой учетной записи пользователя. Процедура создания новой учетной записи пользователя аналогична редактированию параметров учетной записи пользователя, но начинается с ввода имени учетной записи пользователя (рис. 38) и по окончании настройки выводится окно «Ввод пароля» (аналогично рис. 39), в котором необходимо установить пароль для учетной записи пользователя.

Примечание. Требования к имени учетной записи пользователя:

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

Рис. 38. Окно ввода имени пользователя новой учетной записи

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

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

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

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

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

При выборе действия «Задать пароль» в появившемся окне ввода пароля (рис. 39) имеется возможность установить новый пароль учетной записи пользователя.

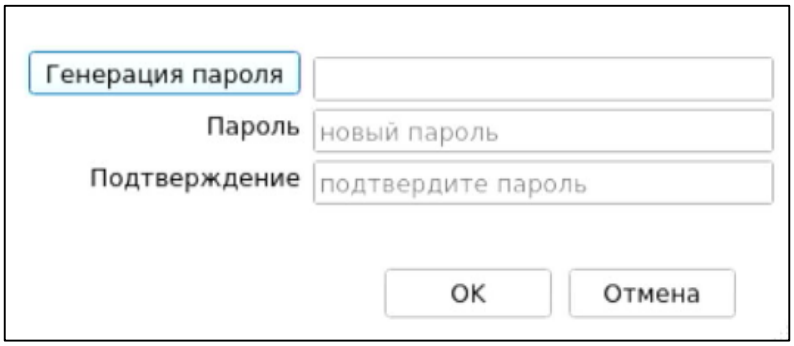


Рис. 39. Окно установки пароля для учетной записи пользователю

Заблокированные пользователи

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

Разблокировка учетной записи пользователя осуществляется автоматически по истечении указанного времени блокировки или после явной разблокировки администратором в разделе «Заблокированные пользователи» (рис. 40). В таком случае у пользователя появляется возможность осуществить вход в систему снова.

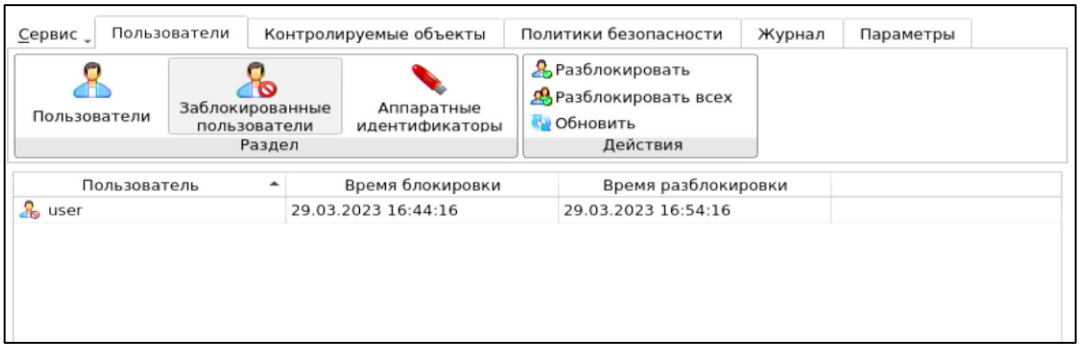


Рис. 40. Окно «Заблокированные пользователи»

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

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

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

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

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

Управление аппаратными идентификаторами

Управление АИ пользователей осуществляется в разделе «Аппаратные идентификаторы» (рис. 41).

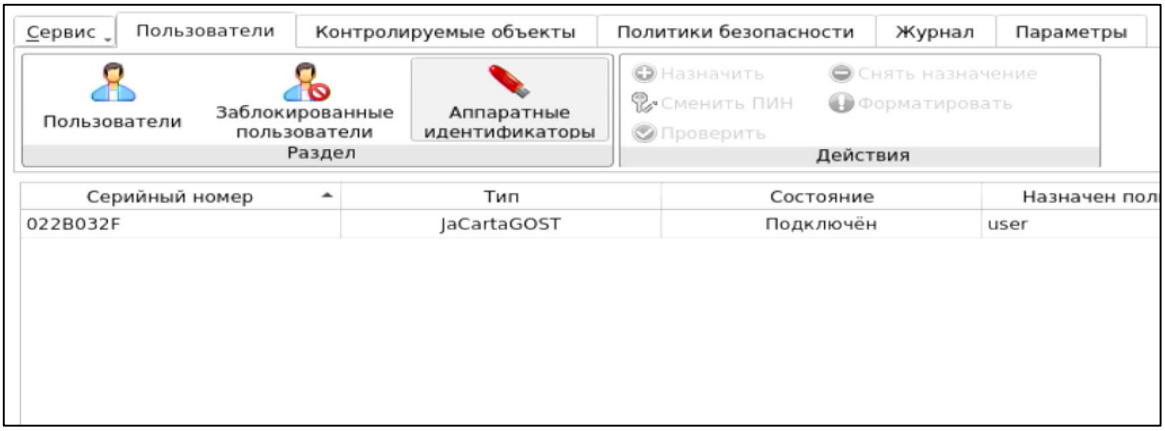


Рис. 41. Окно «Аппаратные идентификаторы»

Для назначения АИ пользователю необходимо нажать кнопку «Назначить» в блоке «Действия», в появившемся диалоговом окне выбрать пользователя и при необходимости установить флаг в поле напротив «Память защищена ПИН» — в этом случае необходимо также указать ПИН АИ (рис. 42).

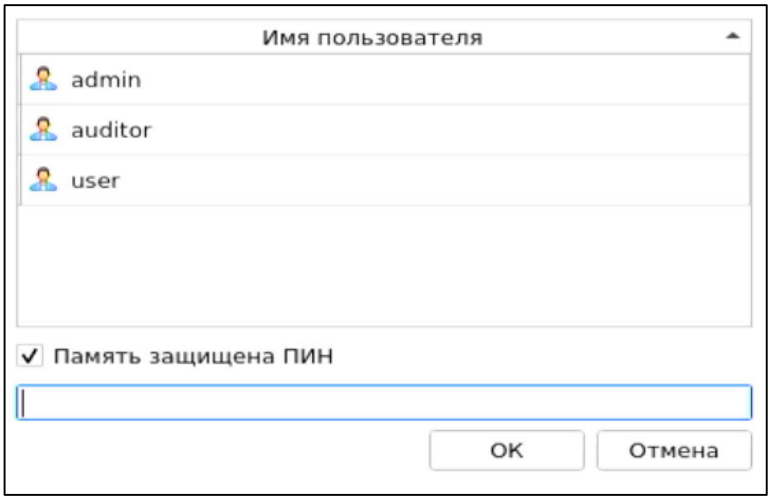


Рис. 42. Диалоговое окно «Назначение аппаратного идентификатора»

По нажатию кнопки «Проверить» запускается процесс тестирования АИ. Для старта тестирования необходимо в открывшемся окне в поле «Пинкод» ввести ПИН АИ и нажать кнопку «ОК» (Рис. 43). Начнется процедура проверки. По завершении тестирования появится соответствующее сообщение (рис. 44).

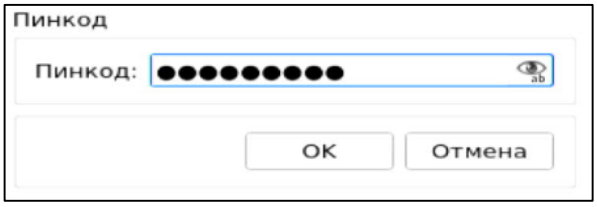


Рис. 43. Окно ввода ПИН АИ

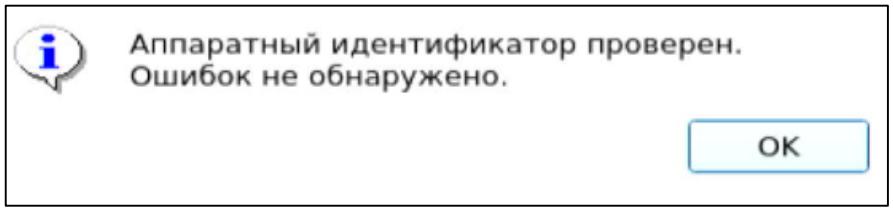


Рис. 44. Сообщение о завершении тестирования АИ

Примечание. Для JaCarta и Рутокен Lite процесс проверки памяти может занимать около 5–10 минут.

Для форматирования АИ необходимо нажать кнопку «Форматировать» в блоке «Действия» и в диалоговом окне ввести соответствующие данные (рис. 45).

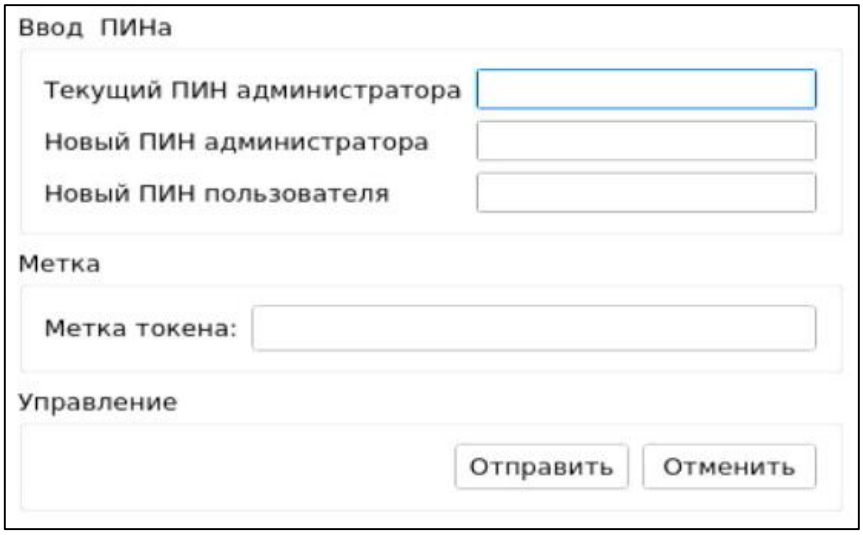


Рис. 45. Окно «Форматирование токена»

3.3.2 Контроль целостности

В разделе «Контролируемые объекты» в виде таблицы отображаются все контролируемые объекты, зарегистрированные в СДЗ УБ Dallas Lock (рис. 46).

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»;
- «ПО СДЗ УБ».

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

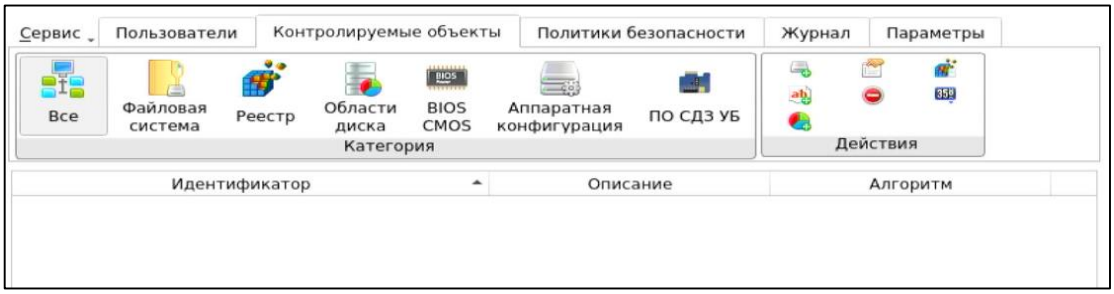


Рис. 46. Главное окно. Контролируемые объекты

Возможны следующие действия с контролируемыми объектами:

- Кнопка « » — добавить объект ФС, при нажатии открывается окно «Объект файловой системы»;
- Кнопка « » — добавить объект реестра, при нажатии открывается окно «Объект реестра»;
- Кнопка « » — добавить область диска, при нажатии открывается окно, где необходимо указать параметры контролируемой области диска;
- Кнопка « » — при нажатии отображаются свойства контролируемого объекта;
- Кнопка « » — при нажатии выбранный контролируемый объект удаляется;

- Кнопка « » — при нажатии осуществляется проверка расчетных КС контролируемых объектов;
- Кнопка « » — при нажатии осуществляется пересчет эталонных КС контролируемых объектов.

Контроль целостности объектов файловой системы

При нажатии кнопки « » выполняется вывод диалогового окна «Объект файловой системы» (рис. 47), где доступно редактирование следующих параметров:

- «Путь» — путь к файлу или каталогу (директории) контролируемого объекта. Задается при добавлении объекта ФС, в дальнейшем не может быть изменен.
- «Описание» — поле предназначено для текстового описания контролируемого объекта.

Допустима установка следующих атрибутов:

- «Алгоритм расчета» — из выпадающего списка выбирается алгоритм расчета контрольной суммы объекта файловой системы.
- «Учитывать наличие» — при контроле целостности объекта файловой системы будет проверяться только наличие указанного объекта. Устанавливается автоматически при установке атрибутов «Учитывать содержимое» и «Учитывать атрибуты».
- «Учитывать содержимое» — при контроле целостности объекта файловой системы будет проверяться содержимое указанного объекта.
- «Учитывать атрибуты» — при контроле целостности объекта файловой системы будет проверяться неизменность атрибутов указанного объекта.

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

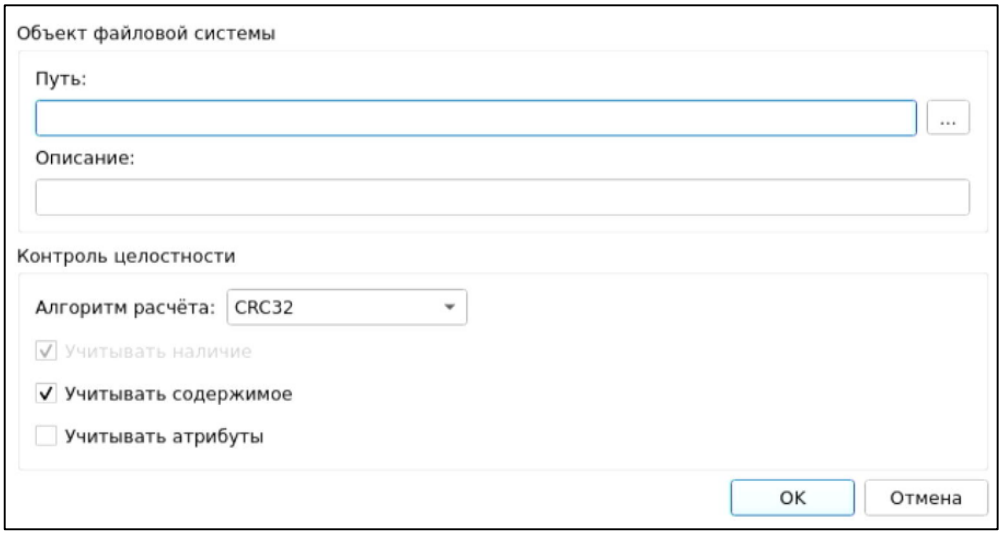


Рис. 47. Окно добавления объекта ФС в контролируемые объекты

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 «Проверить» выполняется обновление расчетных КС списка контролируемых объектов ФС.

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

Контроль целостности объектов реестра Windows

При нажатии кнопки « » осуществляется вывод диалогового окна «Объект реестра» (рис. 48), где доступно редактирование следующих параметров:

- «Файл ветки реестра» — выбирается путь к файлу реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен.
- «Путь реестра» — выбирается путь к контролируемому объекту в указанном выше файле реестра. Задается при добавлении объекта, в дальнейшем не может быть изменен.
- «Описание» — поле предназначено для текстового описания контролируемого объекта.

Допустима установка следующих атрибутов:

- «Алгоритм расчета» — из выпадающего списка выбирается алгоритм расчета контрольной суммы объекта реестра.
- «Рекурсивно» — при контроле целостности объекта реестра типа «Ключ» будут также контролироваться все подключи реестра. Не применимо для объектов реестра типа «Значение».

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

Рис. 48. Окно добавления объекта реестра в контролируемые объекты

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

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

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

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

Контроль целостности областей жесткого диска

Контроль целостности может быть назначен только для локальных дисков.

При нажатии кнопки «  » осуществляется вывод диалогового окна (рис. 49), где доступно редактирование следующих параметров:

- «Диск:» — из выпадающего списка выбирается жесткий диск, подключенный к ТС. При выборе диска в соответствующих полях автоматически отображается его размер, размер сектора и количество секторов. Задается при добавлении объекта, в дальнейшем не может быть изменен.
- «Описание» — поле предназначено для текстового описания контролируемого объекта.

Допустима установка следующих атрибутов:

- «Начальный сектор» — задается начальный сектор области жесткого диска;
- «Количество секторов» — задается количество секторов жесткого диска, подлежащих контролю целостности;
- «Алгоритм» — из выпадающего списка выбирается алгоритм расчета контрольных сумм при контроле целостности области жесткого диска.

Сохранение введенных данных осуществляется при нажатии кнопки «ОК».

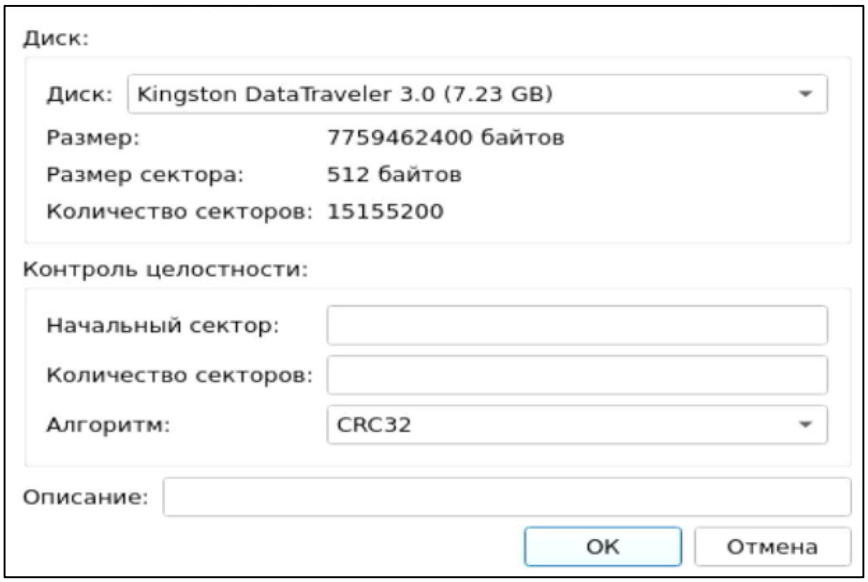


Рис. 49. Окно добавления области диска в контролируемые объекты

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 «Проверить» осуществляется обновление списка контролируемых областей жесткого диска.

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

Контроль целостности BIOS/CMOS

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

- «Обновить CMOS»;
- «Сохранить».

Для категории «BIOS CMOS» форма просмотра разделена на три блока «BIOS», «SMBIOS» и «CMOS» (рис. 50). Блоки «BIOS», «SMBIOS» и «CMOS» представляют из себя три таблицы значений, в которых цветом можно выделять ячейки, для которых нужно назначить контроль, при этом установив чекбоксы «Контроль целостности BIOS», «Контроль целостности SMBIOS» и «Контроль целостности CMOS».

В блоках «BIOS» и «SMBIOS» предусмотрены кнопки «Выделить все» и «Очистить». В блоке «CMOS» это кнопки «Инверсия», которая заменяет назначение целостности для каждой ячейки на обратное значение, «Очистить» и «По умолчанию» (Рис. 51). На выделенные цветом ячейки назначен контроль целостности (Рис. 52). Если ячейки красного цвета — контроль целостности для них не пройден.

Примечание. При первичной настройке контроля целостности BIOS необходимо убедиться, что после перезагрузки АРМ значение не изменилось. В случае изменения значений в каких-либо контролируемых адресах, необходимо исключить данные адреса из маски контроля.

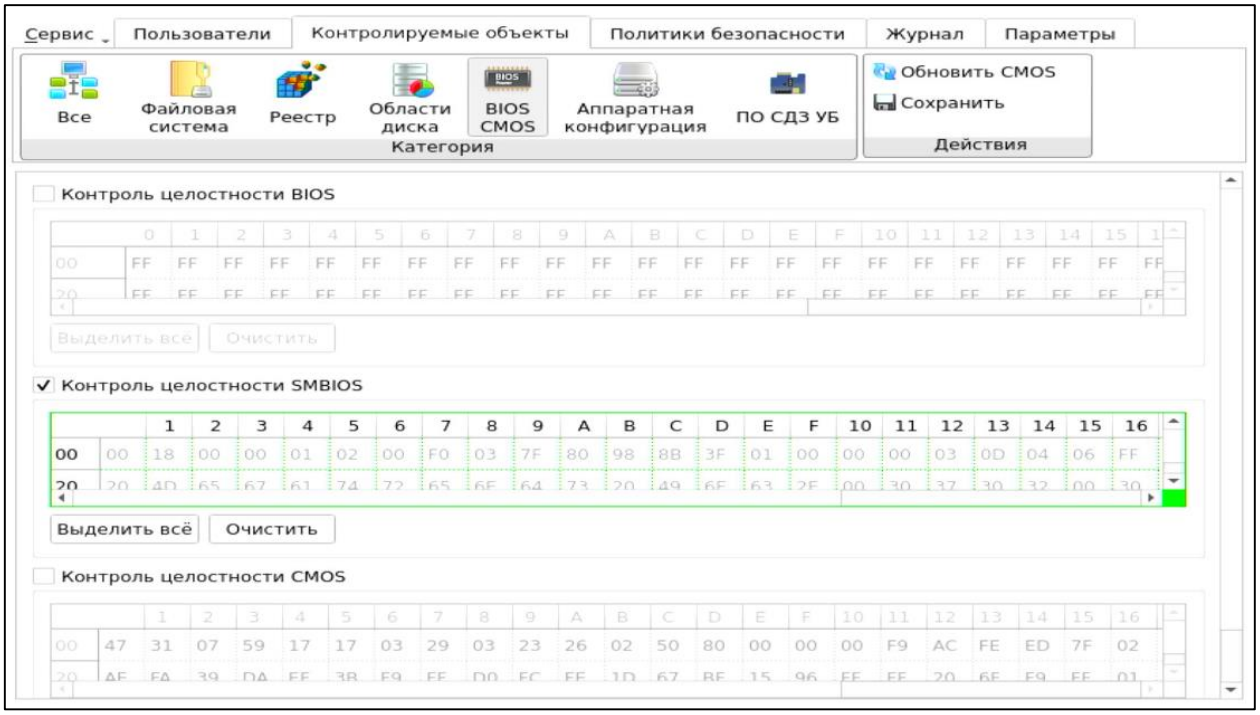


Рис. 50. Контроль BIOS, SMBIOS и CMOS

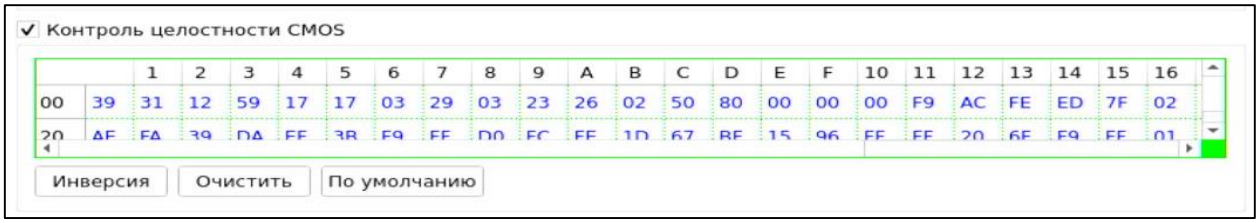


Рис. 51. Кнопки «Инверсия», «Очистить» и «По умолчанию» в блоке «CMOS»

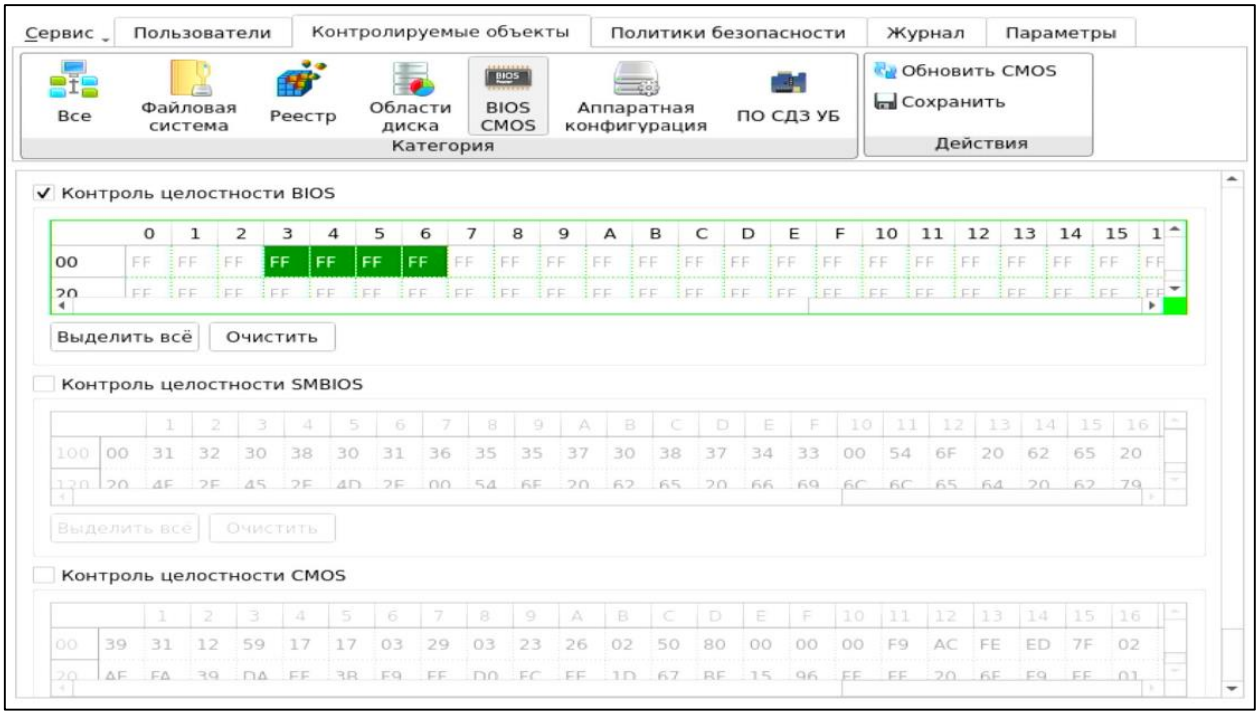


Рис. 52. Блок «BIOS», назначение контроля целостности на выбранные ячейки

Контроль целостности объектов аппаратной конфигурации ТС

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

Для категории «Аппаратная конфигурация» доступны следующие функциональные кнопки:

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

Для настройки контроля аппаратной конфигурации в основной области доступны соответствующие группам чекбоксы (рис. 53) «контролировать группу» и напротив конкретного идентификатора в группе «исключить из контроля»/«включить контроль».

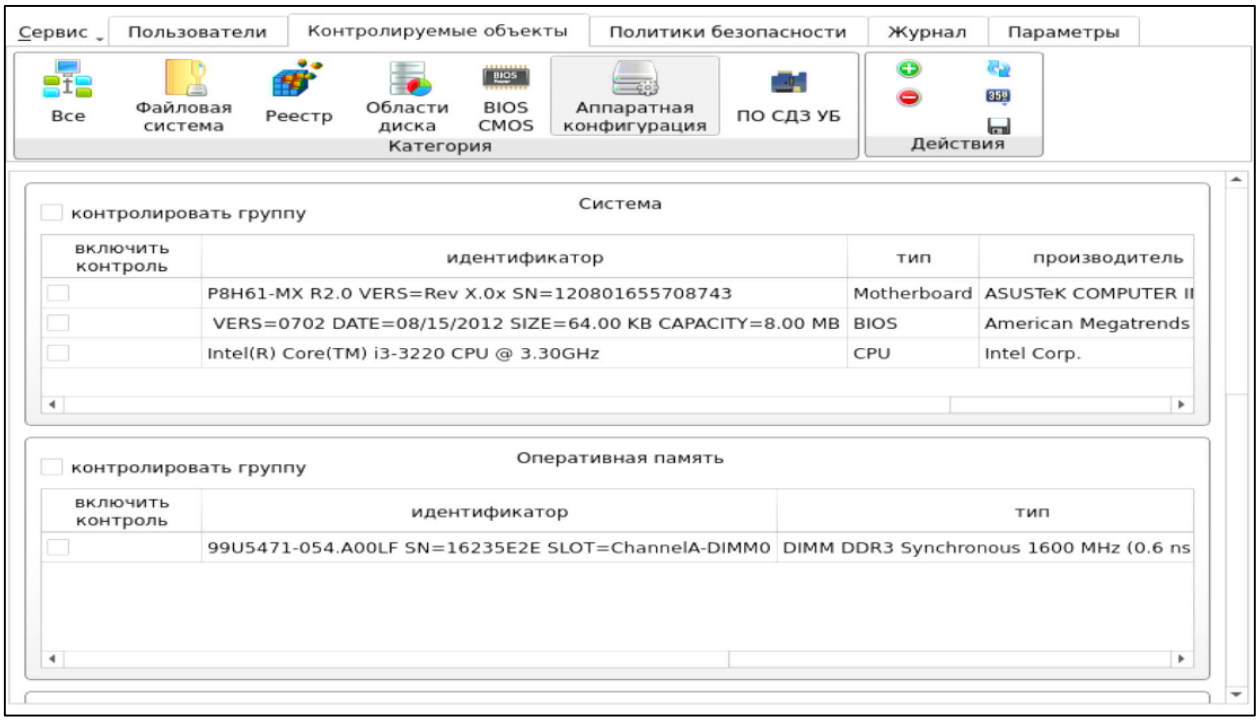


Рис. 53. Главное окно. Контролируемые объекты аппаратной конфигурации ТС

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

Таблица 2 — Пример списка групп аппаратной конфигурации

Группа	Описание
Система	Информация о материнской плате, BIOS и центральном процессоре
Оперативная память	Установленные модули оперативной памяти
PCI-Устройства	Подключенные PCI-устройства
Накопители	Установленные накопители

USB-Устройства	Различные устройства, подключенные через USB-порт, например, АИ, USB-преобразователи и USB-HID устройства

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

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

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

Контроль программного обеспечения СДЗ УБ

Для категории «ПО СДЗ УБ» доступны следующие действия:

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

Для установки контроля целостности ПО СДЗ УБ необходимо установить флаг в поле «Включить контроль ПО» (рис. 54).

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

Для сохранения установленных данных необходимо нажать кнопку «Сохранить».

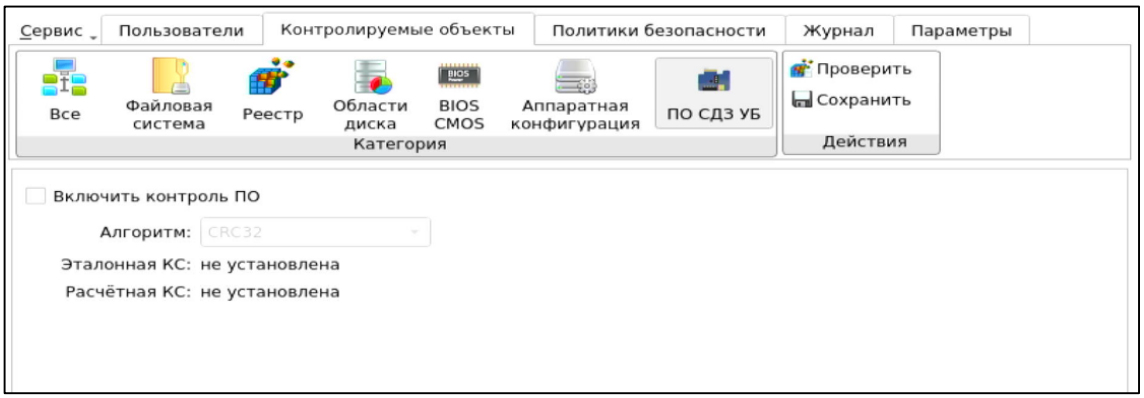


Рис. 54. Главное окно. Контроль ПО СДЗ УБ

3.3.3 Настройка авторизации в СДЗ УБ Dallas Lock

В разделе «Политики безопасности» в виде таблицы отображаются параметры и значения политик безопасности. Выделяются следующие категории политик безопасности:

- «Политики авторизации»;
- «Политики паролей».

Просмотр параметров и значений конкретной категории политик осуществляется через соответствующие кнопки в панели «Политики» (рис. 55, рис. 56). Описание и возможные значения политик приведены в Таблицах 3 и 4.

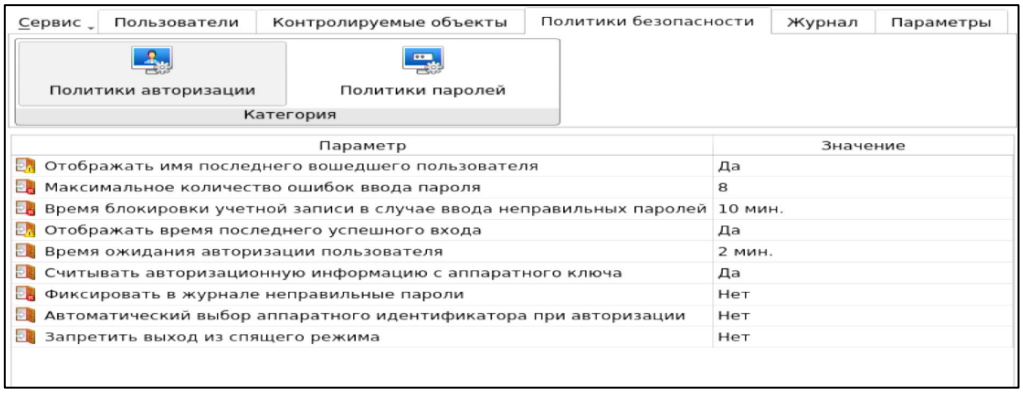


Рис. 55. Главное окно. Политики авторизации

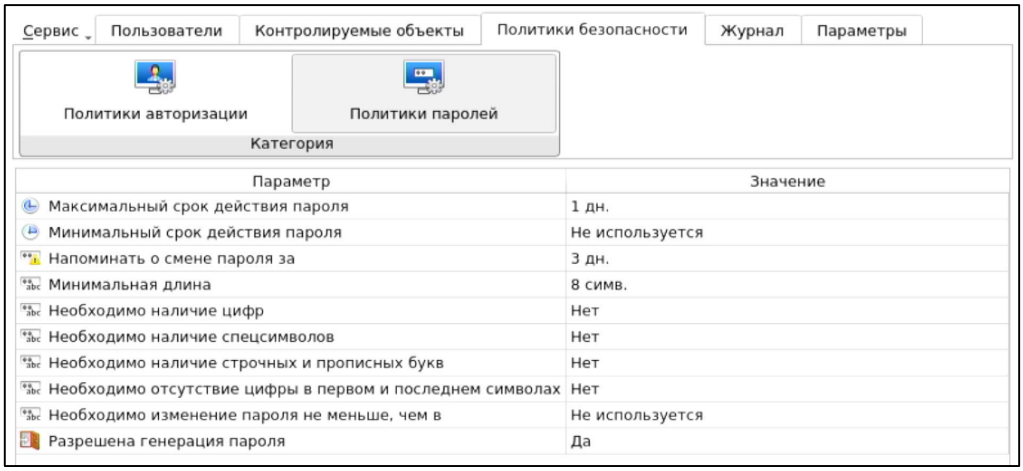


Рис. 56. Главное окно. Политики паролей

Редактирование значений параметров политик осуществляется через соответствующие диалоговые окна, вызываемые двойным нажатием левой кнопки мыши на поле таблицы с редактируемой записью. Пример диалогового окна редактирования параметров политики безопасности приведен на рис. 57. Сохранение измененных значений параметров политики безопасности осуществляется после нажатия кнопки «ОК» в диалоговом окне редактирования параметров политики безопасности.

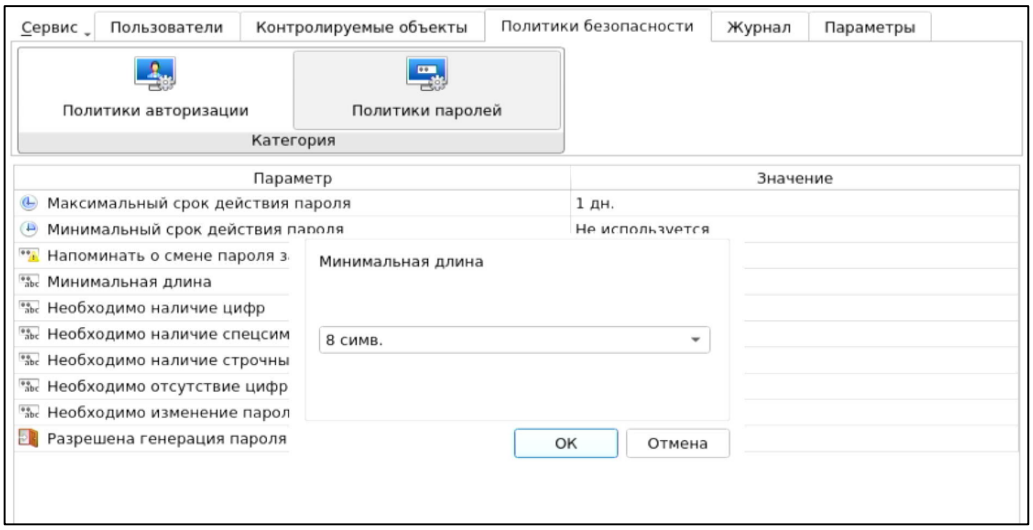


Рис. 57. Диалоговое окно редактирования параметров политики безопасности

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

Параметр политики	Описание
«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. Значение по умолчанию — «Нет».
«Автоматический выбор аппаратного идентификатора при авторизации»	Возможное значение параметра: «Да/Нет». В значении «Да» во время авторизации информация автоматически считывается с АИ. В значении «Нет» этого не происходит. Значение по умолчанию — «Нет».
«Запретить выход из спящего режима»	Возможное значение параметра: «Да/Нет». При включении параметра в значение «Да» вместо нормального выхода из спящего режима будет произведена перезагрузка компьютера. Значение по умолчанию — «Нет».

Таблица 4 — Список параметров категории «Политики паролей»

Параметр политики	Описание
«Максимальный срок действия пароля»	Параметр устанавливает максимальный срок действия пароля пользователей. По истечении срока действия пользователю автоматически будет предложено сменить пароль. Не распространяется на учетные записи пользователей с установленным атрибутом «Бессрочный пароль». Возможное значение параметра: от 1 дня до 25 недель и «Не используется» — максимальный срок действия пароля не установлен. Значение по умолчанию — «6 нед.».
«Минимальный срок действия пароля»	Параметр определяет минимальный срок действия пароля. Если этот срок еще не истек, смена пароля пользователем запрещена. Возможное значение параметра: от 1 дня до 4 недель и «Не используется» — минимальный срок действия не установлен. Значение по умолчанию — «Не используется».
«Напоминать о смене пароля за»	Параметр задает период до установленного максимального срока действия пароля, в который пользователю будет выводиться сообщение о необходимости смены пароля. Возможное значение параметра: от 1 дня до 2 недель и «Не используется» — сообщение выводиться не будет. Значение по умолчанию — «3 дн.».
«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. Значение по умолчанию — «8 симв.».
«Необходимо наличие цифр»	Если данный параметр включен, то при создании пароля в нем должны присутствовать цифры. Возможное значение параметра: «Да/Нет».

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

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

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

3.3.4 Регистрация и учет

В разделе «Журнал» в виде таблицы отображаются все события, зарегистрированные в ходе работы СДЗ УБ Dallas Lock (рис. 58).

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

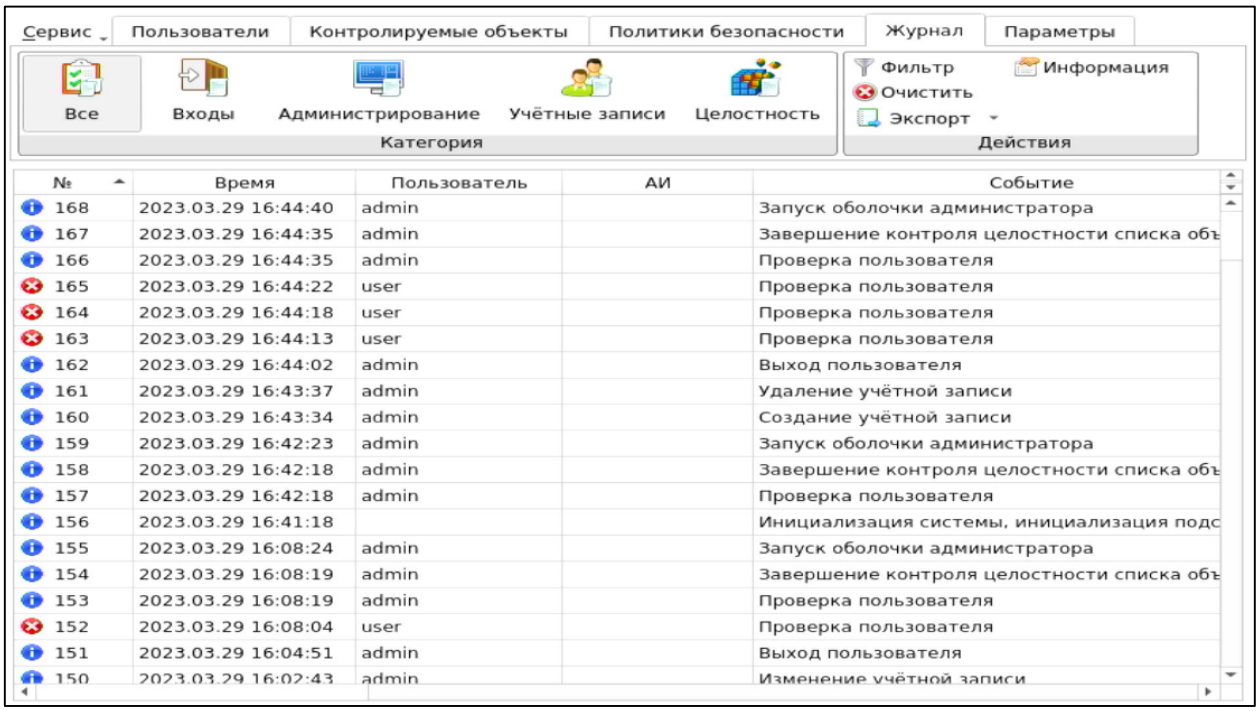
В ходе выполнения процедуры контроля целостности объектов отображается количество занятой памяти журналом (в процентах).

Выделяются следующие категории событий:

- «Входы»;
- «Администрирование»;

- «Учетные записи»;
- «Целостность».

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



№	Время	Пользователь	АИ	Событие
168	2023.03.29 16:44:40	admin		Запуск оболочки администратора
167	2023.03.29 16:44:35	admin		Завершение контроля целостности списка объ
166	2023.03.29 16:44:35	admin		Проверка пользователя
165	2023.03.29 16:44:22	user		Проверка пользователя
164	2023.03.29 16:44:18	user		Проверка пользователя
163	2023.03.29 16:44:13	user		Проверка пользователя
162	2023.03.29 16:44:02	admin		Выход пользователя
161	2023.03.29 16:43:37	admin		Удаление учётной записи
160	2023.03.29 16:43:34	admin		Создание учётной записи
159	2023.03.29 16:42:23	admin		Запуск оболочки администратора
158	2023.03.29 16:42:18	admin		Завершение контроля целостности списка объ
157	2023.03.29 16:42:18	admin		Проверка пользователя
156	2023.03.29 16:41:18			Инициализация системы, инициализация подс
155	2023.03.29 16:08:24	admin		Запуск оболочки администратора
154	2023.03.29 16:08:19	admin		Завершение контроля целостности списка объ
153	2023.03.29 16:08:19	admin		Проверка пользователя
152	2023.03.29 16:08:04	user		Проверка пользователя
151	2023.03.29 16:04:51	admin		Выход пользователя
150	2023.03.29 16:02:43	admin		Изменение учётной записи

Рис. 58. Главное окно. Журнал

Возможны следующие действия с журналом:

- «Фильтр»;
- «Очистить»;
- «Экспорт»;
- «Информация».

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

При нажатии кнопки «Фильтр» выводится всплывающее меню (рис. 59), в котором при нажатии правой кнопки мыши осуществляется выбор:

- текстового фильтра;
- интервального фильтра;
- фильтра по значению;
- регулярного выражения;
- автофильтра (рис. 60).

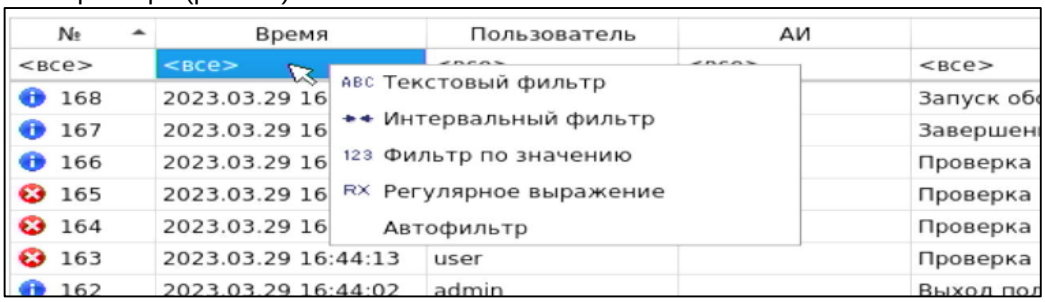


Рис. 59. Главное окно. Назначение фильтра

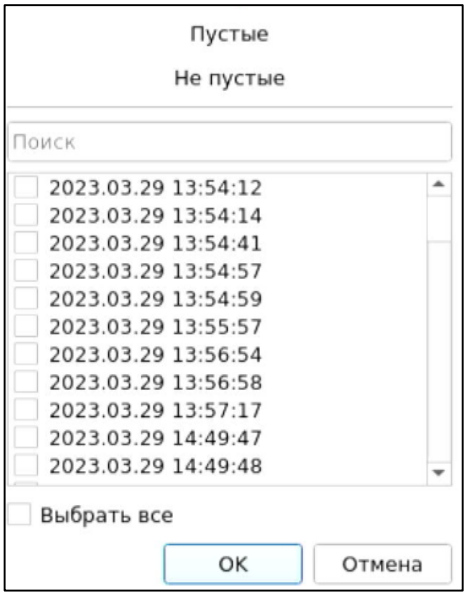


Рис. 60. Меню назначения автофильтра журнала

Результат применения фильтра журнала по заданию пользователя «admin» приведен на рис. 61.

№	Время	Пользователь	АИ	Событие
<все>	<нет>	1 строка	<все>	<все>
168	2023.03.29 16:44:40	admin		Запуск оболочки администратора
167	2023.03.29 16:44:35	admin		Завершение контроля целостности списка объ
166	2023.03.29 16:44:35	admin		Проверка пользователя
162	2023.03.29 16:44:02	admin		Выход пользователя
161	2023.03.29 16:43:37	admin		Удаление учётной записи
160	2023.03.29 16:43:34	admin		Создание учётной записи
159	2023.03.29 16:42:23	admin		Запуск оболочки администратора
158	2023.03.29 16:42:18	admin		Завершение контроля целостности списка объ
157	2023.03.29 16:42:18	admin		Проверка пользователя

Рис. 61. Результат применения фильтра журнала по заданию пользователя

Результат применения автофильтра журнала по наименованию события (выход пользователя, добавление объекта контроля целостности аппаратной конфигурации, завершение контроля целостности списка объектов) приведен на рис. 62.

Время	Пользователь	АИ	Событие	
<нет>	<все>	<все>	3 строк	<в
2023.03.29 16:44:35	admin		Завершение контроля целостности списка объектов	ОК
2023.03.29 16:44:02	admin		Выход пользователя	ОК
2023.03.29 16:42:18	admin		Завершение контроля целостности списка объектов	ОК
2023.03.29 16:08:19	admin		Завершение контроля целостности списка объектов	ОК
2023.03.29 16:04:51	admin		Выход пользователя	ОК
2023.03.29 16:02:02	admin		Завершение контроля целостности списка объектов	ОК
2023.03.29 16:01:49	auditor		Выход пользователя	ОК
2023.03.29 15:56:52	auditor		Завершение контроля целостности списка объектов	ОК
2023.03.29 15:56:38	admin		Выход пользователя	ОК
2023.03.29 15:44:57	admin		Завершение контроля целостности списка объектов	ОК

Рис. 62. Результат применения автофильтра журнала по наименованию события

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

При нажатии кнопки «Очистить» выводится соответствующее предупреждение (рис. 63).

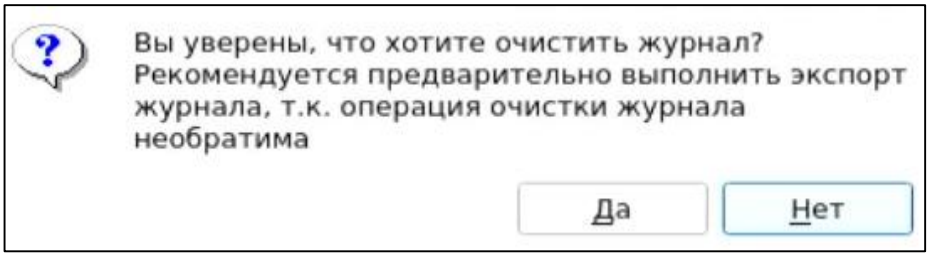


Рис. 63. Сообщение «Очистка журнала»

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

Поскольку операция удаления записей журнала необратима, то перед очисткой журнала рекомендуется произвести экспорт записей журнала в файл. При нажатии кнопки «Экспорт» из выпадающего списка выбирается формат создаваемого файла (рис. 64). Данная функция также доступна пользователям категории «Аудиторы».

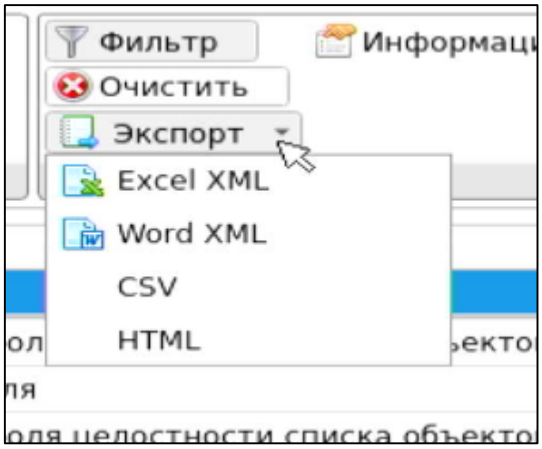


Рис. 64. Главное окно. Меню экспорта журнала в файл

При нажатии кнопки «Информация» выводится соответствующее информационное окно для выбранного события (рис. 65).

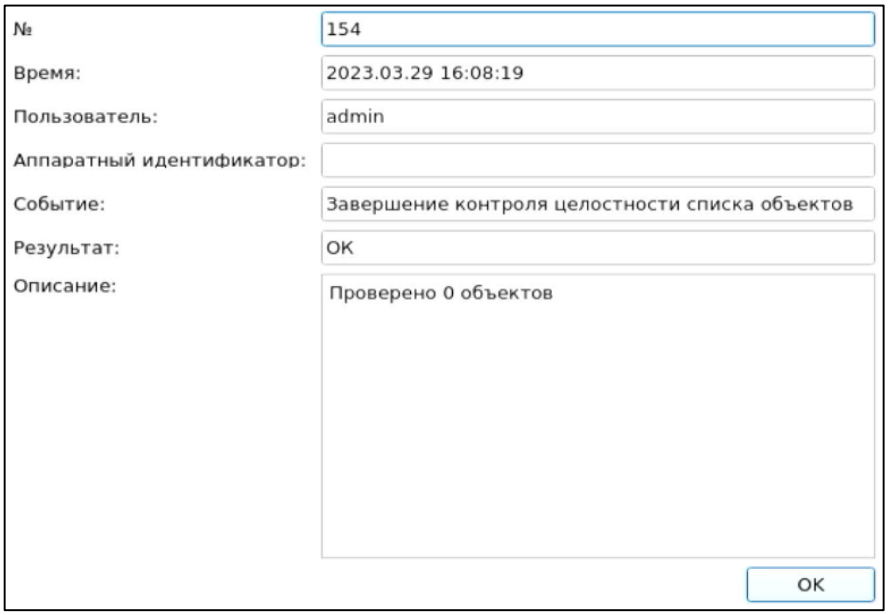


Рис. 65. Информационное окно

3.3.5 Управление параметрами загрузки и параметрами сети

В разделе «Параметры» отображаются следующие категории:

- «Параметры загрузки»;
- «Параметры сети».

Просмотр параметров и значений конкретной категории осуществляется через соответствующие кнопки в панели «Категория» (Рис. 66, рис. 67).

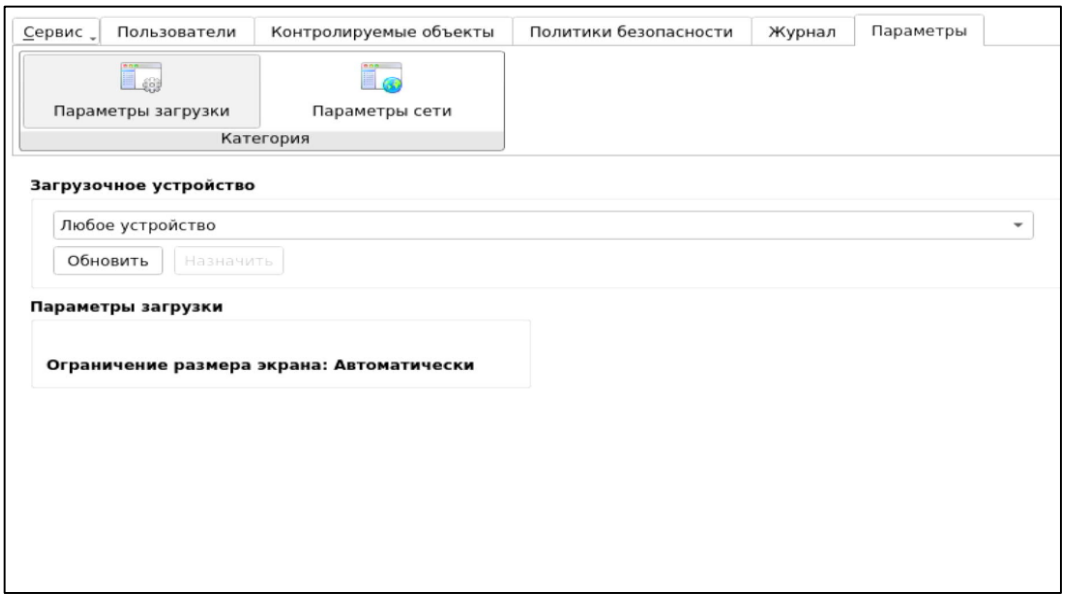


Рис. 66. Главное окно. Параметры загрузки

Категория «Параметры загрузки»:

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

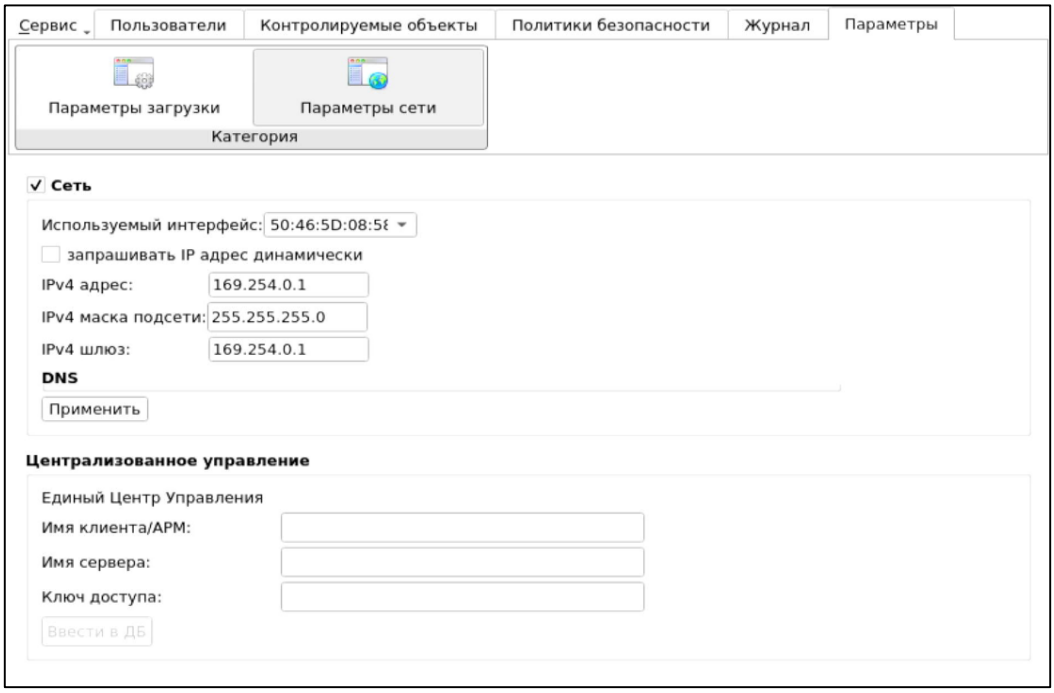


Рис. 67. Главное окно. Параметры сети

Категория «Параметры сети»:

- «Сеть» — чекбокс для включения сети. Содержит сетевые параметры, необходимые для удаленного администрирования с Консоли Единого центра управления. Для настройки

требуется заполнить следующие поля:

- «Используемый интерфейс» — из выпадающего списка необходимо выбрать MAC-адрес нужного сетевого адаптера;
- чекбокс «запрашивать динамически» — при установленном чекбоксе во время запуска оболочки функций безопасности сетевые параметры автоматически назначаются DHCP-сервером:
  - «IPv4 адрес», «IPv4 маска подсети», «IPv4 шлюз» — сетевые параметры компьютера, которые можно заполнить вручную или автоматически, установив флаг в поле «запрашивать динамически.

Примечание. Чтобы сетевые настройки (включая настройки, полученные от сервера DHCP) вступили в силу, необходимо нажать кнопку «Применить».

- «Централизованное управление» — для централизованного и оперативного управления клиентами они должны быть введены в Домен безопасности. Для ввода СДЗ УБ клиента в Домен безопасности необходимо выбрать заполнить следующие поля про Единый Центр Управления (далее — ЕЦУ):
  - «Имя клиента/АРМ» — необходимо ввести имя клиента, которое будет отображаться в Консоли ЕЦУ.
  - «Имя сервера» — необходимо ввести имя компьютера в сети или IP-адрес, на котором установлен ЕЦУ.
  - «Ключ доступа» — необходимо ввести ключ удаленного доступа к ЕЦУ. По умолчанию ключ доступа — пустой.

После нажатия кнопки «Ввести в ДБ» клиент СДЗ УБ будет введен в ДБ, появится сообщение об успешном вводе клиента (рис. 68). Для завершения операции и перезагрузки клиента СДЗ УБ необходимо нажать кнопку «ОК».

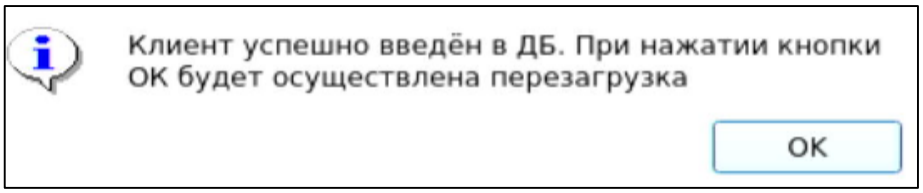


Рис. 68. Информационное сообщение о вводе клиента в ДБ

Примечание. Для удаленной перезагрузки/выключения клиентов СДЗ УБ, находящихся в режиме работы ШОС, необходима, чтобы клиент с СДЗ УБ был введен в Домен безопасности (см. «Удаленная перезагрузка и удаленное выключение клиентов СДЗ»).

В дереве объектов консоли ЕЦУ появится новый клиент СДЗ УБ, после чего в категории «Параметры сети» будет доступна только кнопка «Вывести из ДБ» (рис. 69).

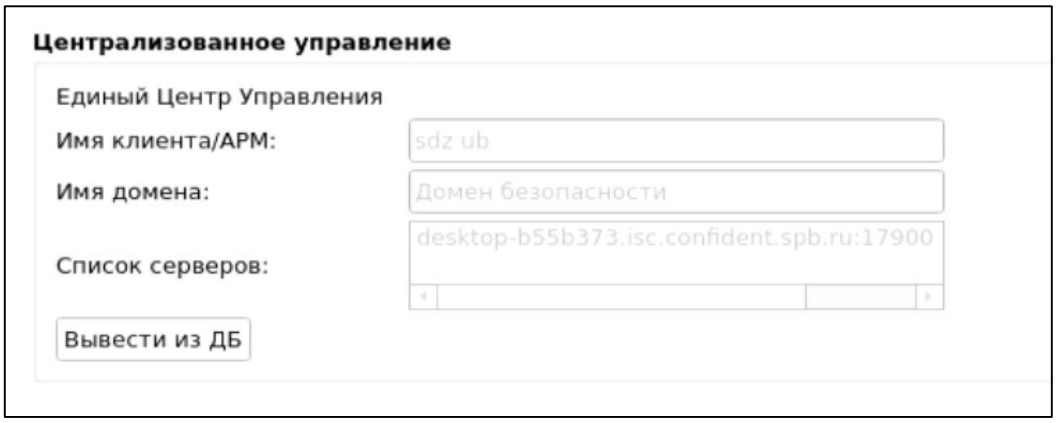


Рис. 69. Параметры сети. Кнопка вывода из ДБ

С подробным описанием ЕЦУ Dallas Lock можно ознакомиться в Инструкции по использованию ЕЦУ Dallas Lock ПФНА.501410.004 И3.

3.3.6 Дополнительные функции СДЗ УБ Dallas Lock

Меню «Сервис» позволяет получить доступ к дополнительным функциям СДЗ УБ Dallas Lock (рис. 72):

- «Конфигурация». Возможны следующие действия для пункта «Конфигурация»:
  - «Сохранить» — данные об учетных записях пользователей, контролируемых объектах и политиках безопасности сохраняются в специальном файле конфигурации в формате *.xml на различные носители информации;
  - «Применить» — применение сохраненных параметров конфигурации;
  - «По умолчанию» — восстановление конфигурации СДЗ УБ Dallas Lock по умолчанию.
- «Тестирование функций СДЗ» — самотестирование функций СДЗ УБ. Данный пункт меню «Сервис» доступен только администраторам. При запуске самотестирования результат самотестирования отображается в окне «Тестирование основных функций СДЗ» (Рис. 70).

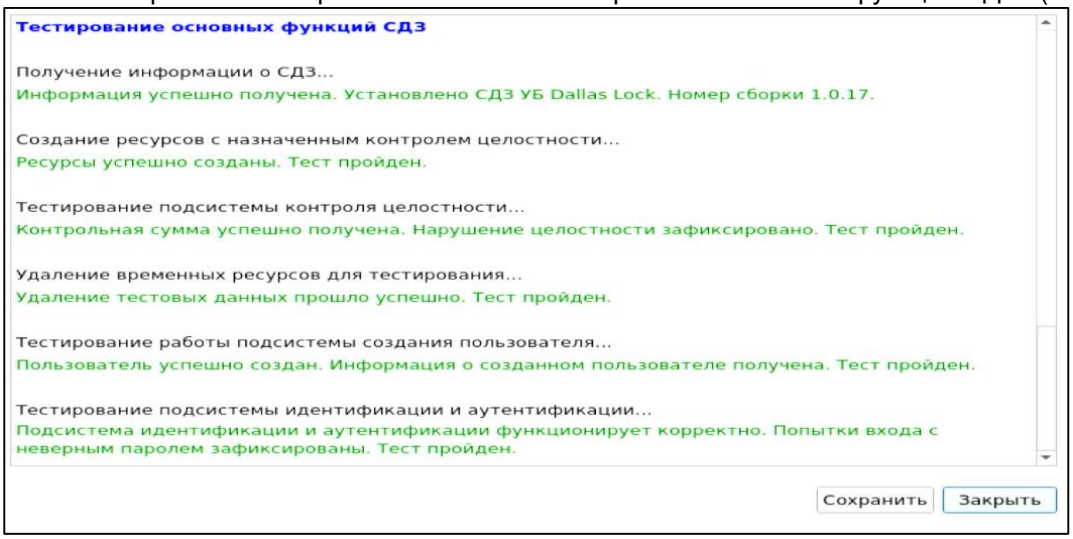


Рис. 70. Окно результатов тестирования основных функций СДЗ

При нажатии кнопки «Сохранить» в окне тестирования основных функций СДЗ происходит формирование отчета о тестировании в формате .txt. Пример отчета представлен на Рис. 71. Результат тестирования фиксируется в журнале в категориях «Администрирование», «Все».

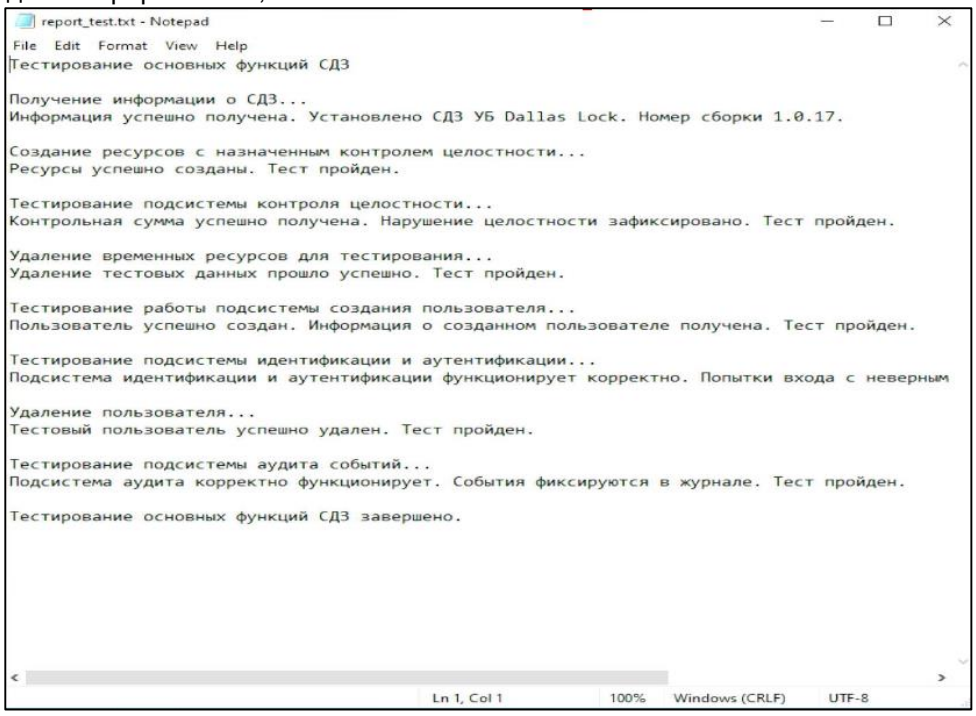


Рис. 71. Окно результатов тестирования основных функций СДЗ

- «Отчет» — сохранение отчета в формате *.txt на различные носители информации. Функция сохранения отчета о конфигурации СДЗ УБ Dallas Lock может использоваться для дальнейшей проверки соответствия этих настроек эталонным значениям. Доступно формирование отчетов «Права и конфигурация» и «Аппаратная часть».
  В отчете «Права и конфигурации» указываются следующие данные:
  - имя пользователя, который создал отчет;
  - способ создания отчета;
  - дата и время формирования отчета;
  - номер сборки ПО СДЗ УБ Dallas Lock;
  - параметры конфигурации СДЗ УБ Dallas Lock в соответствии с настройками отчета.

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

Рис. 72. Главное окно. Меню «Сервис»

Примечание. Код активации технической поддержки предоставляется по электронной почте в рамках договора.

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

3.4 Выключение/перезагрузка ТС

В меню «Сервис» также сгруппированы функциональные кнопки, отвечающие за соответствующие процедуры управления ТС (рис. 72):

- «Выход» — осуществляется выход текущей учетной записи пользователя из оболочки администратора и переход к окну авторизации пользователя в СДЗ УБ Dallas Lock;
- «Загрузка ОС» — осуществляется переход к загрузке ШОС;
- «Перезагрузка» — осуществляется перезагрузка ТС;
- «Выключение» — осуществляется выключение ТС.

3.5 Удаленная перезагрузка и удаленное выключение клиентов СДЗ УБ

В Консоли ЕЦУ реализована возможность удаленной перезагрузки/выключения ТС с установленным СДЗ УБ Dallas Lock для отдельных клиентов СДЗ УБ, для групп клиентов СДЗ УБ и для домена клиентов СДЗ УБ, находящихся в режиме работы ШОС.

Перезагрузка и выключение удаленной рабочей станции с установленным СДЗ УБ Dallas Lock доступны посредством Консоли ЕЦУ.

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

3.6 Порядок обновления изделия

Обновление ПО СДЗ УБ осуществляется через меню инсталлятора СДЗ УБ Dallas Lock следующим образом:

- Предприятие-изготовитель доводит до потребителей информацию о выпуске обновлений изделия и устраненных в новых версиях недостатках по электронной почте письмом с вложенным документом, подписанным ЭП, о новом обновлении продукта и публикует информацию на сайте www.dallaslock.ru.
- Потребитель при получении указанной информации выполняет загрузку обновления с сайта предприятия-изготовителя в виде дистрибутива, информация о контрольной сумме которого содержится на сайте предприятия-изготовителя, а также файл электронной подписи.
- Перед установкой обновления потребитель выполняет проверку подлинности электронной подписи (согласно инструкции, представленной на сайте предприятия-изготовителя), расчет[1] и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте предприятия-изготовителя.
- В случае успешной проверки электронной подписи и совпадения контрольных сумм, потребитель выполняет установку обновлений. Если проверка электронной подписи и контрольных сумм не пройдена, потребитель не выполняет установку обновлений и обращается к предприятию-изготовителю изделия.
- Для установки обновления необходимо записать файл обновления на USB-flash накопитель, установить подготовленный USB-flash накопитель с изделием в USB-порт ТС и запустить ТС.

3.7 Перечень возможных неисправностей в процессе использования

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

3.8 Порядок выполнения контроля работоспособности изделия

Контроль работоспособности изделия осуществляется в ходе проведения приемо-сдаточных испытаний в объеме, предусмотренном в Технических условиях ПФНА.501410.004 ТУ.

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

3.9 Порядок выключения изделия

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

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

4 ТРАНСПОРТИРОВАНИЕ И ХРАНЕНИЕ

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

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

В транспортных средствах должна соблюдаться изоляция изделия от кислот, щелочей и других химически активных веществ. При хранении изделия не допускаются резкие перепады температуры окружающего воздуха, попадания на USB-flash накопитель с изделием органических растворителей; не допускаются удары USB-flash накопителя.

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