

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ УРОВНЯ БАЗОВОЙ СИСТЕМЫ ВВОДА-ВЫВОДА

Dallas Lock

(версия изделия 2.0.14)



Руководство оператора
(пользователя)

ПФНА.501410.004 34

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1 НАЗНАЧЕНИЕ СДЗ УБ DALLAS LOCK	4
2 УСЛОВИЯ ВЫПОЛНЕНИЯ СИСТЕМЫ ЗАЩИТЫ	5
2.1 ПАРАМЕТРЫ (НАСТРОЙКИ) БЕЗОПАСНОСТИ СРЕДСТВА, ДОСТУПНЫЕ ПОЛЬЗОВАТЕЛЮ	5
2.2 ДАННЫЕ УЧЕТНОЙ ЗАПИСИ	5
2.3 ПЕРЕЧЕНЬ РОЛЕЙ ПОЛЬЗОВАТЕЛЯ	6
2.4 ПРАВА ДЛЯ РАБОТЫ ПОД УЧЕТНОЙ ЗАПИСЬЮ	6
2.5 ВХОД НА ЗАЩИЩЕННОЕ ТС	7
2.6 ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ	8
2.7 СМЕНА ПОЛЬЗОВАТЕЛЯ	8
2.8 СМЕНА ПАРОЛЯ	8
2.9 ТИПЫ СОБЫТИЙ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С ДОСТУПНЫМИ ПОЛЬЗОВАТЕЛЮ ФУНКЦИЯМИ СДЗ УБ	11
3 СООБЩЕНИЯ ОБ ОШИБКАХ	12
3.1 Ошибки, возникающие при входе	12
4 ИНТЕРФЕЙСЫ, ДОСТУПНЫЕ ПОЛЬЗОВАТЕЛЯМ	13
ТЕРМИНЫ И СОКРАЩЕНИЯ	20

ВВЕДЕНИЕ

Данное руководство предназначено для пользователей (операторов) ТС, на которых установлено изделие «Средство доверенной загрузки уровня базовой системы ввода-вывода «Dallas Lock» ПФНА.501410.004 (далее — изделие, СДЗ УБ, СДЗ УБ Dallas Lock).

В руководстве содержатся сведения, необходимые пользователю для работы на компьютерах, защищенных СДЗ УБ Dallas Lock.

1 НАЗНАЧЕНИЕ СДЗ УБ DALLAS LOCK

СДЗ УБ Dallas Lock 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 предназначено для использования на технических средствах (далее — ТС) Intel 3 поколения (Ivy Bridge) или AMD Ryzen (Zen2) с архитектурой x86-64, таких как персональные и портативные компьютеры, серверы.

В соответствии с требованиями безопасности предприятия лицами, ответственными за установку и эксплуатацию СДЗ УБ Dallas Lock, проводится соответствующая настройка параметров и политик безопасности, а также механизмов, которые реализованы в СДЗ УБ Dallas Lock. Подробное описание настройки механизмов администрирования содержится в документе «Руководство по эксплуатации» ПФНА.501410.004 РЭ.

Режим работы СДЗ УБ Dallas Lock настраивается администратором. В оболочке администратора доступны гибкие настройки политик авторизации пользователей, работа с локальными и доменными учетными записями пользователей, введение СДЗ УБ Dallas Lock в домен безопасности.

Администратор — пользователь ответственный за управление СДЗ УБ Dallas Lock. Эту функцию могут выполнять и 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 (оператор) — пользователь защищенного персонального компьютера (ТС), осуществляющий ввод и обработку информации любыми программными средствами.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ СИСТЕМЫ ЗАЩИТЫ

2.1 Параметры (настройки) безопасности средства, доступные пользователю

Доступ к управлению и права для работы пользователей с учетной записью аудитора и пользователя в СДЗ УБ назначаются только администратором СДЗ УБ через оболочку администрирования. Добавляя пользователя, аудитора или администратора в определенную категорию, администратор задает разрешенные действия для них в СДЗ УБ.

Учетной записи пользователя, которой присвоена категория «Пользователи» доступны следующие параметры безопасности:

- имеет право запускать ШОС;
- имеет право менять пароль учетной записи, если иные настройки учетной записи не активированы администратором.

Учетной записи пользователя, которой присвоена категория «Аудиторы» доступны следующие параметры безопасности:

- помимо всех прав пользователя имеет полномочия просматривать значения всех параметров СДЗ УБ Dallas Lock без возможности их изменения в режиме администрирования;
- имеет полномочия сохранять отчет о конфигурации;
- имеет полномочия выводить сообщение о системе;
- после успешной авторизации в момент проверки целостности имеет возможность видеть, сколько и где обнаружено нарушений целостности и процент заполнения журнала;
- при заполнении журнала на 95% не имеет возможности входа в систему.

2.2 Данные учетной записи

Чтобы получить доступ к компьютеру, на который установлено СДЗ УБ Dallas Lock, необходимо иметь зарегистрированную в СДЗ УБ Dallas Lock учетную запись. Регистрация учетных записей осуществляется администратором СДЗ УБ Dallas Lock.

Учетная запись пользователя, зарегистрированного в СДЗ УБ Dallas Lock, имеет следующие атрибуты, которые необходимы для входа на защищенный компьютер (авторизации):

Основные	
Имя пользователя (логин)	За пользователем закрепляется условное имя
Пароль	Пользователю сообщается пароль, который необходим для подтверждения того, что именно он является пользователем, зарегистрированным под этим именем (происходит аутентификация)
Дополнительные	
Аппаратный идентификатор (АИ)	Пользователю может быть выдан один АИ
ПИН-код аппаратного идентификатора	Если учетной записи пользователя назначен АИ, то для авторизации дополнительно может быть использован ПИН-код идентификатора



Внимание! Пользователю необходимо:

- уточнить у администратора все авторизационные данные для входа на защищенный компьютер;
- запомнить свое имя пользователя и пароль;
- никому не сообщать пароль и никому не передавать персональный АИ.

Авторизация пользователя осуществляется при каждом запуске ТС.

При вводе имени и пароля необходимо соблюдать следующие правила:

- Для имени:**
- максимальная длина имени — 31 символ;
 - имя может содержать латинские символы, символы кириллицы, цифры и специальные символы;
 - разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).
- Для пароля:**
- минимальная длина пароля — 8 символов по умолчанию, редактируется в пределах от 0 до 14;
 - пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;
 - разрешается использовать различные регистры клавиатуры, при этом нужно помнить, что заглавные и прописные буквы воспринимаются как различные (Password и password являются разными паролями).

2.3 Перечень ролей пользователя

Роль «Аудиторы» обладает всеми привилегиями на просмотр информации, в том числе:

- просмотр списка пользователей и свойств учетных записей пользователей;
- просмотр политик авторизации и политик паролей;
- просмотр списка контролируемых объектов;
- просмотр журнала;
- просмотр параметров загрузки и параметров сети;
- создание отчета о конфигурации СДЗ УБ;
- вывод сообщения о системе;
- просмотр информации об обнаруженных нарушениях целостности и проценте заполнения журнала.

Учетной записи с ролью «Аудиторы» разрешена работа по следующим сценариям сессии:

- «Загрузка ОС» — переход к загрузке ОС;
- «Смена пароля» — переход к смене пароля текущей учетной записи пользователя;
- «Администрирование» — переход в режим администрирования к интерфейсу оболочки администрирования СДЗ УБ Dallas Lock.

Роль «Пользователи» не имеет полномочий на администрирование СДЗ УБ.

Следует уточнить у администратора, какими правами обладает пользователь в системе.

Учетной записи с ролью «Пользователи» разрешена работа по следующим сценариям сессии:

- «Загрузка ОС» — переход к загрузке ОС;
- «Смена пароля» — переход к смене пароля текущей учетной записи пользователя (если данный сценарий сессии не запрещен администратором для данной учетной записи пользователя).

В разделе 2 данного документа представлено описание общих для аудитора и пользователя интерфейсов, их параметров и порядок работы с ними.

В разделе 4 данного документа приведены описание и перечень интерфейсов с привязкой к ролям пользователей, для которых они доступны.

2.4 Права для работы под учетной записью

Необходимо выяснить у администратора, какими именно правами и привилегиями обладает пользователь и к каким ресурсам может иметь доступ.

Во всех сложных ситуациях, связанных с работой на защищенном компьютере, которые пользователь не в состоянии разрешить самостоятельно, необходимо обращаться к администратору СДЗ УБ Dallas Lock.

2.5 Вход на защищенное ТС

Для входа на защищенный СДЗ УБ Dallas Lock компьютер каждому пользователю нужно выполнить следующую последовательность шагов.

1. Включить питание компьютера. При загрузке ТС с установленным СДЗ УБ Dallas Lock появляется экран приглашения на вход в систему (Рис. 1).

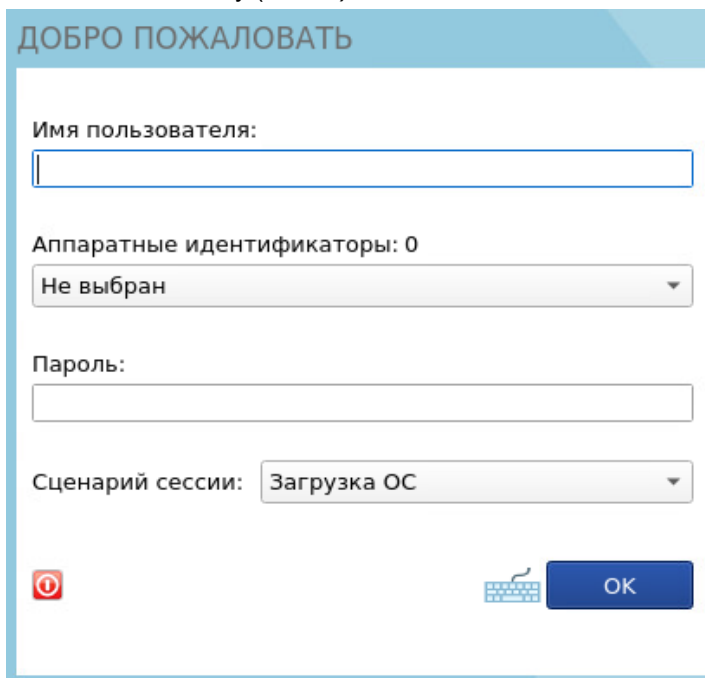


Рис. 1. Экран приглашения на вход в систему



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

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

2. Предъявить АИ (если назначен данной учетной записи).
3. Заполнить поле «Имя пользователя» — ввести имя учетной записи, под которой пользователь зарегистрирован в СДЗ УБ Dallas Lock.
4. Ввести пароль. При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «•» (точка). Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля. Дополнительная кнопка  изменит скрытые символы на явные.
5. Выбрать в выпадающем списке:
 - «Загрузка ОС» — переход к загрузке ОС;
 - «Смена пароля» — переход к смене пароля текущей учетной записи пользователя;
 - «Администрирование» — переход в режим администрирования к интерфейсу оболочки администрирования СДЗ УБ Dallas Lock.
6. Нажать клавишу «Enter» или кнопку «OK» на экранной форме.

Вход на защищенное ТС с использованием АИ

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

- вставить его в USB-порт или прикоснуться к считывателю (в зависимости от типа устройства);
- выбрать наименование идентификатора, которое появится в выпадающем меню «Аппаратные идентификаторы».

В зависимости от настроек АИ, произведенных администратором применительно к учетной записи пользователя, возможны следующие способы авторизации:

- необходимо предъявить АИ, ввести имя учетной записи пользователя и пароль;
- необходимо предъявить АИ (при этом в поле «Пользователь» будет подставлена хранящаяся в памяти АИ идентификационная информация, поле будет недоступно для редактирования) и ввести пароль учетной записи пользователя;
- необходимо предъявить АИ (при этом в поля «Пользователь» и «Пароль» будут подставлена хранящаяся в памяти АИ идентификационная и аутентификационная информация, поля будут недоступны для редактирования);
- необходимо предъявить АИ (при этом в поле «Пользователь» 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 введенный ПИН верен.



Примечание. При вводе имени и пароля переключение раскладки клавиатуры (русская/латинская) производится нажатием комбинации клавиш «Alt+Shift».

2.6 Завершение сеанса работы

СДЗ УБ поддерживает завершение сеанса работы с использованием графической оболочки ОС. За более подробной информацией следует обратиться к документации на используемую ОС.

2.7 Смена пользователя

Для смены пользователя необходимо осуществить завершение сеанса работы или перезагрузку ТС. После включения ТС до загрузки ШОС будет предложен экран приглашения на вход в систему СДЗ УБ (Рис. 1). Далее необходимо осуществить авторизацию учетной записью пользователя согласно описанию в п. 2.5 «Вход на защищенное ТС».

2.8 Смена пароля

Смена пароля возможна в трех случаях:

- по запросу пользователя;
- по истечении срока действия пароля учетной записи пользователя;
- для учетной записи пользователя был установлен атрибут «Потребовать смену пароля при следующем входе».

1. Смена пароля по запросу пользователя.

При выборе действия «Смена пароля» в окне авторизации осуществляется переход к процедуре смены пароля (Рис. 2).

Рис. 2. Диалоговое окно смены текущего пароля учетной записи пользователя

Действие «Смена пароля» 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. 3).

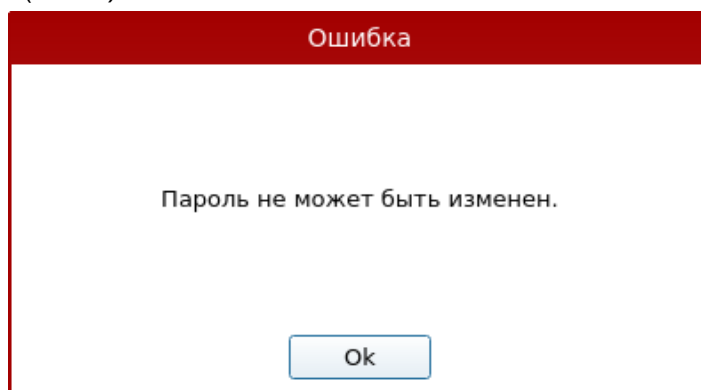


Рис. 3. Окно сообщения при запрете смены пароля пользователем

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

При несоответствии пароля требованиям политики сложности паролей выводится соответствующее сообщение (Рис. 4 и Рис. 5), смена пароля не производится, осуществляется возврат к окну смены пароля.

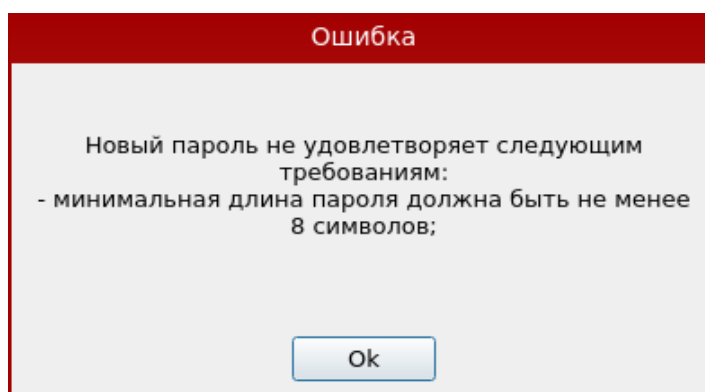


Рис. 4. Сообщение при несоответствии длины пароля учетной записи пользователя политике сложности паролей

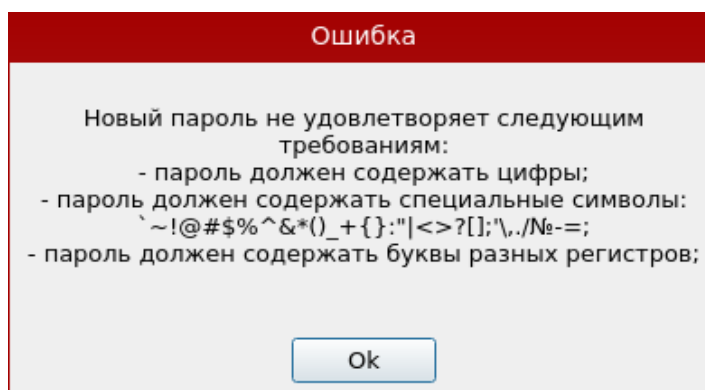


Рис. 5. Сообщение при несоответствии сложности пароля учетной записи пользователя политике сложности паролей



Примечание. В случае несоответствия политикам сложности паролей или иной ошибки, возникшей при смене пароля, выводится сообщение, описывающее суть в достаточной степени.

При вводе пароля на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка). Возможно воспользоваться дополнительной кнопкой , которая изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет неактивно.

Если значения пароля в поле ввода и в поле повтор не совпадают, выводится соответствующее сообщение и осуществляется возврат к окну смены пароля (Рис. 6).

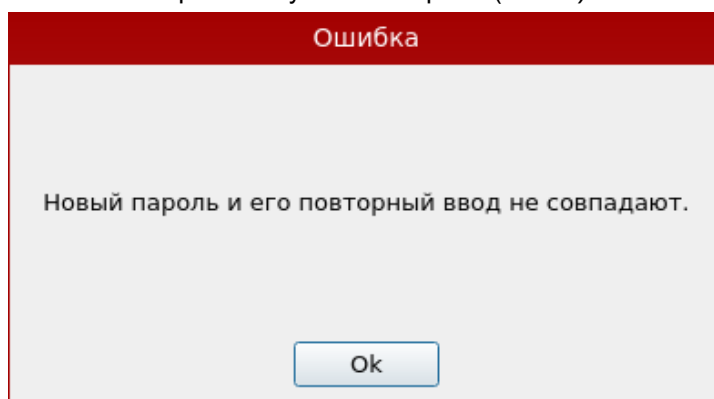


Рис. 6. Сообщение при несовпадении паролей

При успешной смене текущего пароля учетной записи пользователя выводится соответствующее сообщение (Рис. 7) и осуществляется возврат в окно авторизации.

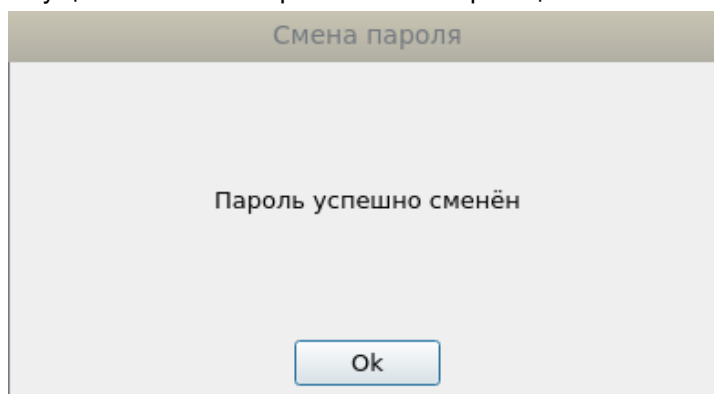


Рис. 7. Сообщение при успешной смене текущего пароля учетной записи пользователя



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

2. Смена пароля по истечении срока действия пароля учетной записи пользователя.

В случае истечения срока действия пароля проверяется разрешение для пользователя на смену своего пароля в соответствии с установленным атрибутом в настройках учетной записи пользователя «Запретить смену пароля пользователем».

Если атрибут не установлен, происходит переход к процедуре смены пароля. Дальнейшие действия осуществляются аналогично пункту «Смена пароля по запросу пользователя».

В случае отсутствия разрешения на смену пароля пользователем выводится сообщение «Истек срок действия пароля». Производится возврат к этапу авторизации. Загрузка штатной операционной системы (далее — ШОС) недоступна пользователям с истекшим сроком действия пароля.

3. Для учетной записи пользователя был установлен атрибут «Потребовать смену пароля при следующем входе».

Если установлен данный атрибут в настройках учетной записи, то при следующем входе пользователя выводится сообщение о необходимости сменить пароль (Рис. 8) и по нажатию кнопки «ОК» происходит переход к процедуре смены пароля.

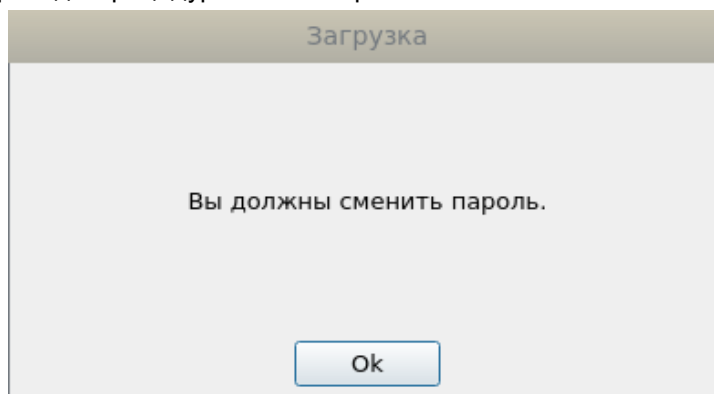


Рис. 8. Сообщение о необходимости сменить пароль

Дальнейшие действия осуществляются аналогично пункту «Смена пароля по запросу пользователя».

2.9 Типы событий безопасности, связанные с доступными пользователю функциями СДЗ УБ

При совершении пользователем действий, связанных с выполнением функций безопасности СДЗ УБ, информация об этих действиях заносится в журнал событий, который доступен только учетным записям пользователей с категориями «Аудиторы» и «Администраторы». СДЗ УБ регистрирует следующие типы событий безопасности, связанные с доступными пользователю и аудитору функциями СДЗ УБ:

- события, связанные с процессом аутентификации:
 - проверка пользователя;
 - инициализация системы;
 - старт ОС;
 - запуск оболочки администратора;
 - выход пользователя из системы;
 - перезагрузка;
 - выключение;
 - смена пароля;
- события, связанные с управлением и конфигурацией:
 - сохранение конфигурации в файл;
 - экспорт журнала;
- события по срабатыванию сторожевого таймера;
- события, связанные с контролем целостности:
 - пересчет целостности объекта;
 - завершение пересчета целостности объекта;
- в случае возникновения события, не попадающего ни под одну из категорий, в журнал заносится событие «Неизвестное событие».

3 СООБЩЕНИЯ ОБ ОШИБКАХ

3.1 Ошибки, возникающие при входе

Если пользователем не была пройдена процедура авторизации, то на экран могут быть выведены следующие сообщения об ошибках:

- «Пользователь указан неверно» — если введенное имя учетной записи пользователя отсутствует в СДЗ УБ Dallas Lock;
- «Указан неверный пароль» — если введенный пароль неверен. Пользователю будет предложено повторно ввести имя и пароль;
- «Не предъявлен или предъявлен неверный аппаратный идентификатор» — при предъявлении неверного АИ;
- «Не выбран аппаратный идентификатор» — при отсутствии АИ;
- «Указан неверный PIN-код» — если память выбранного АИ защищена ПИН-кодом, ПИН-код не введен или введен неверно;
- «Учетная запись отключена» — если администратор установил атрибут «Отключен» для данной учетной записи. Необходимо обратиться к администратору;
- «Учетная запись заблокирована» — если превышено количество попыток ввода пароля, происходит автоматическая блокировка учетной записи. Разблокировка учетной записи пользователя осуществляется автоматически по истечении указанного времени блокировки или после явной разблокировки администратором;
- «Нарушено расписание работы пользователя» — если осуществляется попытка авторизации пользователя в неустановленное для него время работы;
- «Обнаружено нарушение целостности» — выводится в случае обнаружения нарушений целостности контролируемых объектов после ввода имени и пароля учетной записи пользователя. Далее осуществляется проверка разрешения на работу пользователя с нарушенной целостностью (если для учетной записи пользователя установлен атрибут «Запретить работу при нарушенной целостности», выводится дополнительное сообщение «Работа запрещена!»);
- «Срок действия пароля истек. Вам необходимо его изменить» — если истек срок действия пароля и у данной учетной записи не установлен атрибут «Запретить смену пароля пользователем». Осуществляется переход к процедуре смены пароля;
- «Истек срок действия пароля» — если истек срок действия пароля и у данной учетной записи установлен атрибут «Запретить смену пароля пользователем». Необходимо обратиться к администратору.



Примечание. Возможна ситуация, при которой пользователь забыл свой пароль. В этом случае он должен обратиться к администратору СДЗ УБ Dallas Lock, который может назначить учетной записи пользователя новый пароль.

4 ИНТЕРФЕЙСЫ, ДОСТУПНЫЕ ПОЛЬЗОВАТЕЛЯМ

Интерфейсы, доступные учетной записи пользователя с категорией «Пользователи»:

- «Окно авторизации» (Рис. 9). Подробное описание параметров интерфейса представлено в п. 2.5 настоящего документа.

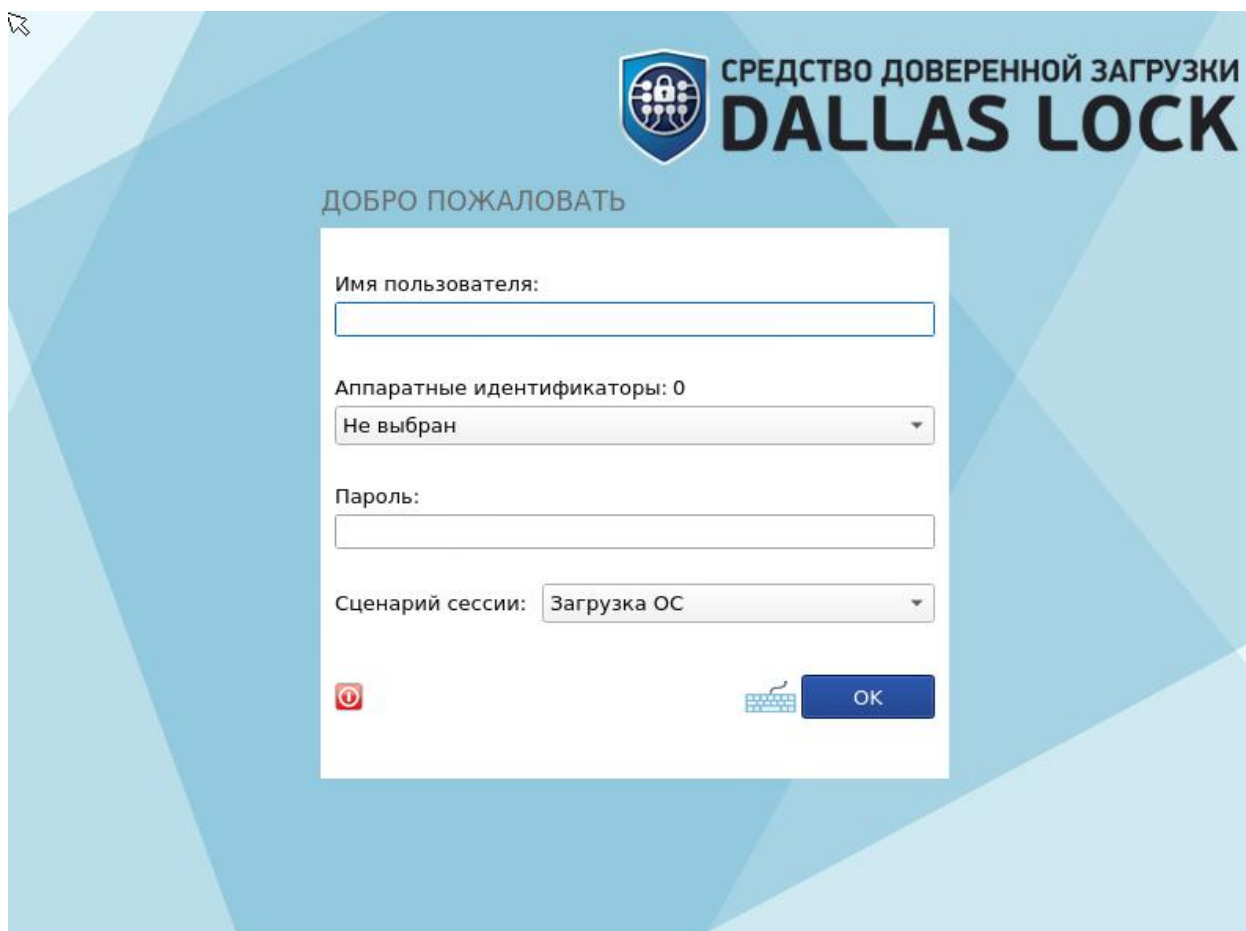


Рис. 9. Интерфейс «Окно авторизации»

- «Установка пароля пользователю». Подробное описание параметров интерфейса представлено в п. 2.8 настоящего документа.

Параметры интерфейса «Установка пароля пользователю» доступны пользователю только при выборе сценария сессии «Смена пароля» в интерфейсе «Окно авторизации» (Рис. 9).

При выборе сценария сессии «Смена пароля» пользователю предоставляется возможность изменить свой пароль (Рис. 10), если данная функция не отключена администратором в настройках учетной записи данного пользователя.

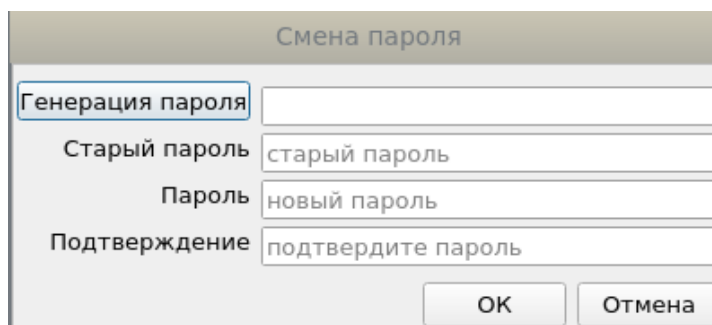


Рис. 10. Окно интерфейса «Установка пароля пользователю»

- «Диалоговые окна» (полное описание интерфейса представлено в п. 7.2.1 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра результатов тестирования после успешной авторизации (Рис. 12) и информации о том, что учетная запись заблокирована (Рис. 11).

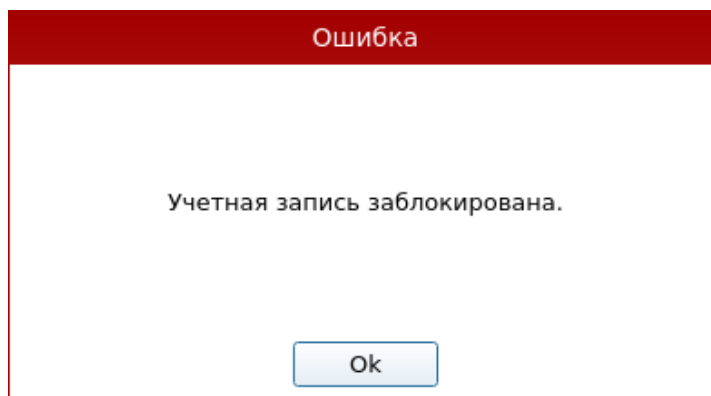


Рис. 11. Интерфейс «Диалоговые окна». Сигнализация о блокировке учетной записи пользователя

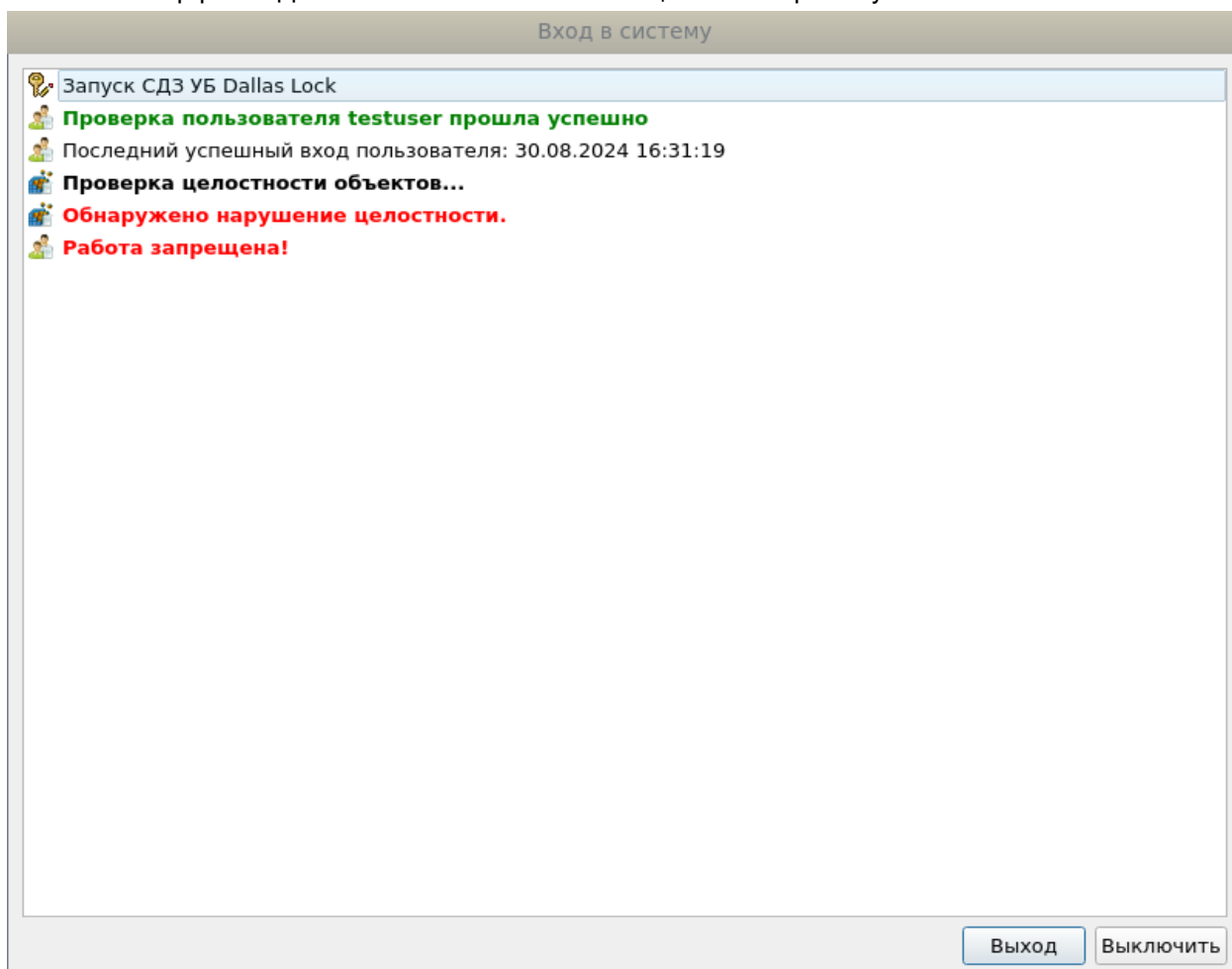


Рис. 12. Интерфейс «Диалоговые окна». Сигнализация в случае неуспешного прохождения процедуры контроля целостности

Для аудитора доступны все интерфейсы, доступные для пользователя, а также следующие интерфейсы:

- «Журнал» (полное описание интерфейса представлено в п. 5.2.1 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра всех журналов, а также осуществления функций фильтрации, экспорта и просмотра информации о каждой записи аудита (Рис. 13).

Сервис						
Пользователи						
Контролируемые объекты						
Политики безопасности						
Журнал						
Параметры						
Все Входы Администрирование Учётные записи Целостность Категория				Фильтр Очистить Экспорт Информация Действия		
№	Время	Пользователь	АИ	Событие	Результат	Описание
23	2024.10.29 10:36...	admin		Запуск оболочки администратора	ОК	
22	2024.10.29 10:36...	admin		Завершение контроля целостности спи...	ОК	Проверено 0 объектов
21	2024.10.29 10:36...	admin		Проверка пользователя	ОК	
20	2024.10.29 10:36...	testuser		Проверка пользователя	У пользоват...	
19	2024.10.29 10:35...	admin		Выход пользователя	ОК	
18	2024.10.29 10:35...	admin		Создание учётной записи	ОК	"testuser" (Пользователи)
17	2024.10.29 10:35...	admin		Запуск оболочки администратора	ОК	
16	2024.10.29 10:35...	admin		Завершение контроля целостности спи...	ОК	Проверено 0 объектов
15	2024.10.29 10:35...	admin		Проверка пользователя	ОК	
14	2024.10.29 10:35...			Инициализация системы, инициализац...	ОК	
13	2024.10.29 10:34...	admin		Задание загрузочного устройства	ОК	(GPT)/9F862C3C-7A20-4ACA-99C...
12	2024.10.28 15:13...	admin		Задание пароля учётной записи	ОК	auditor
11	2024.10.28 15:13...	admin		Создание учётной записи	ОК	"auditor" (Аудиторы)

Рис. 13. Интерфейс «Журналы»

- «Конфигурация и процедуры управления» (полное описание интерфейса представлено в п. 3.2.1 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части сохранения конфигурации (Рис. 14) и выгрузки отчетов об аппаратной части ТС и об информации о правах и конфигурации, а также осуществления выхода, загрузки ОС, перезагрузки ТС и выключения ТС (Рис. 15).

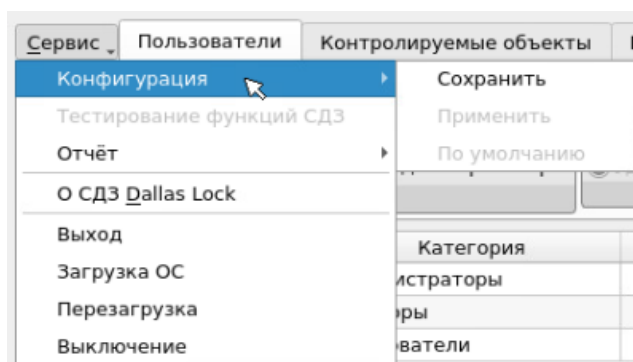


Рис. 14. Интерфейс «Конфигурация и процедуры управления». Функция сохранения конфигурации

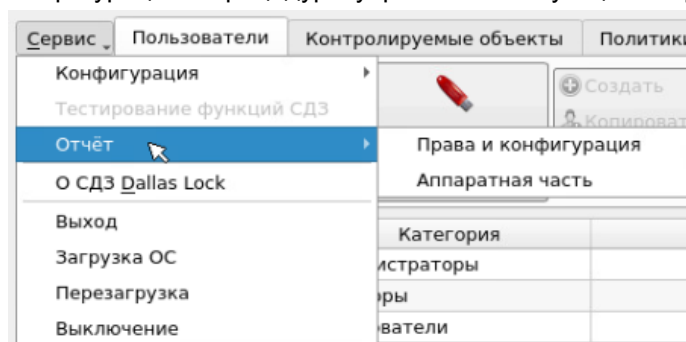


Рис. 15. Интерфейс «Конфигурация и процедуры управления». Функция выгрузки отчетов

- «Управление пользователями» (полное описание интерфейса представлено в п. 6.2.1 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра списка учетных записей пользователей (Рис. 16), просмотра свойств учетных записей пользователей (Рис. 17), просмотра и обновления списка заблокированных пользователей (Рис. 18) и просмотра списка аппаратных идентификаторов (Рис. 19).

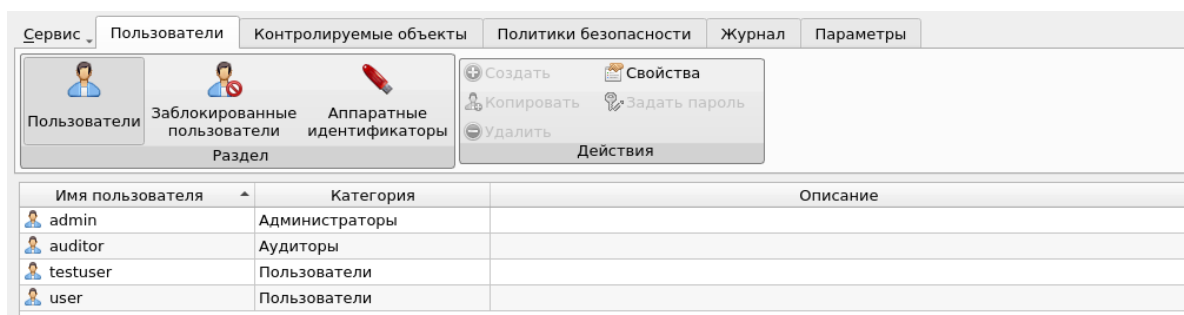


Рис. 16. Интерфейс «Управление пользователями». Функция просмотра списка учетных записей пользователя

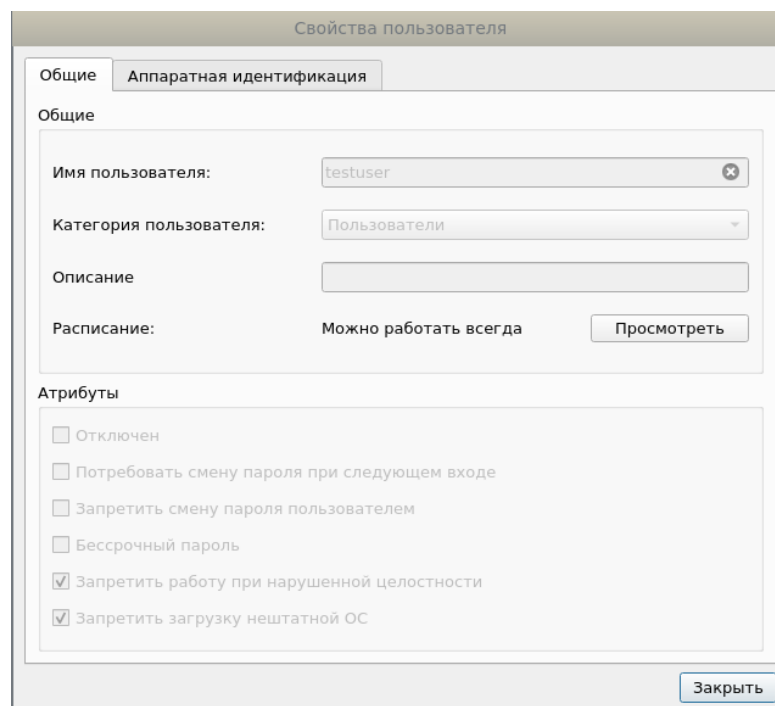


Рис. 17. Интерфейс «Управление пользователями». Функция просмотра свойств учетной записи пользователя

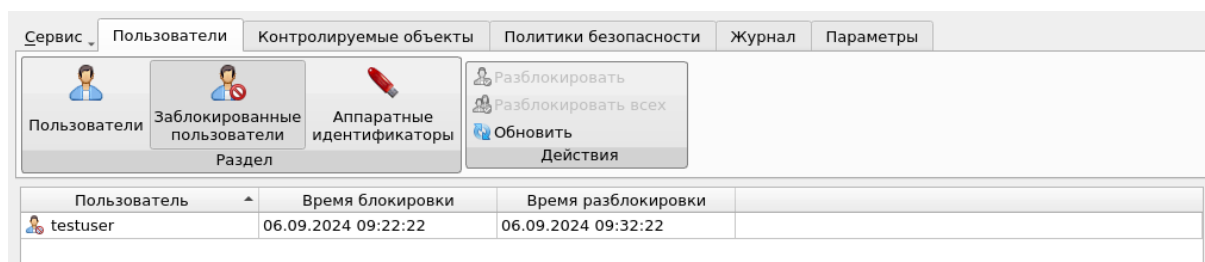


Рис. 18. Интерфейс «Управление пользователями». Функция просмотра списка заблокированных пользователей

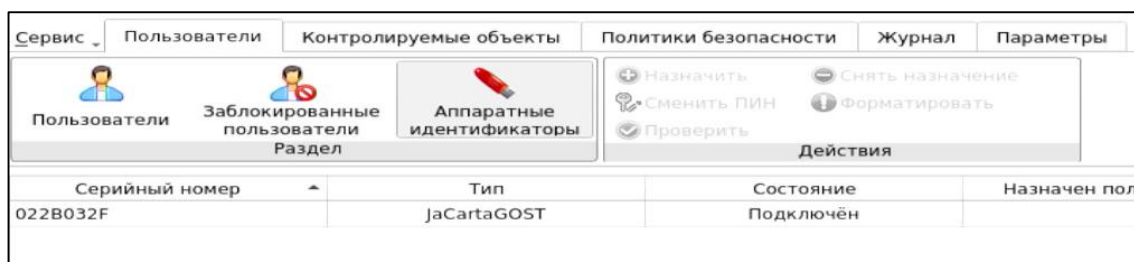


Рис. 19. Интерфейс «Управление пользователями». Функция просмотра списка аппаратных идентификаторов

- «Контролируемые объекты» (полное описание интерфейса представлено в п. 7.2.2 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра списка контролируемых объектов и выполнения функции пересчета КС (Рис. 20).

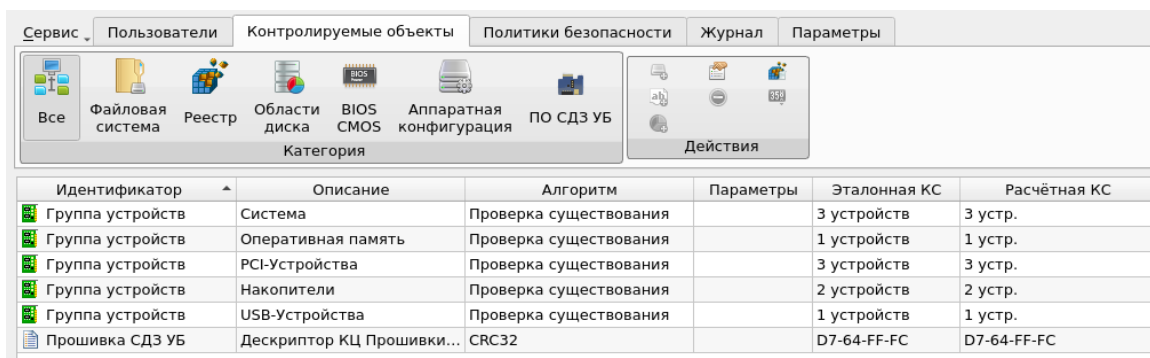


Рис. 20. Интерфейс «Контролируемые объекты». Список контролируемых объектов

- «Контроль BIOS SMBIOS CMOS» (полное описание интерфейса представлено в п. 7.2.3 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра информации о контролируемых значениях BIOS, SMBIOS и CMOS и обновления CMOS (Рис. 21).

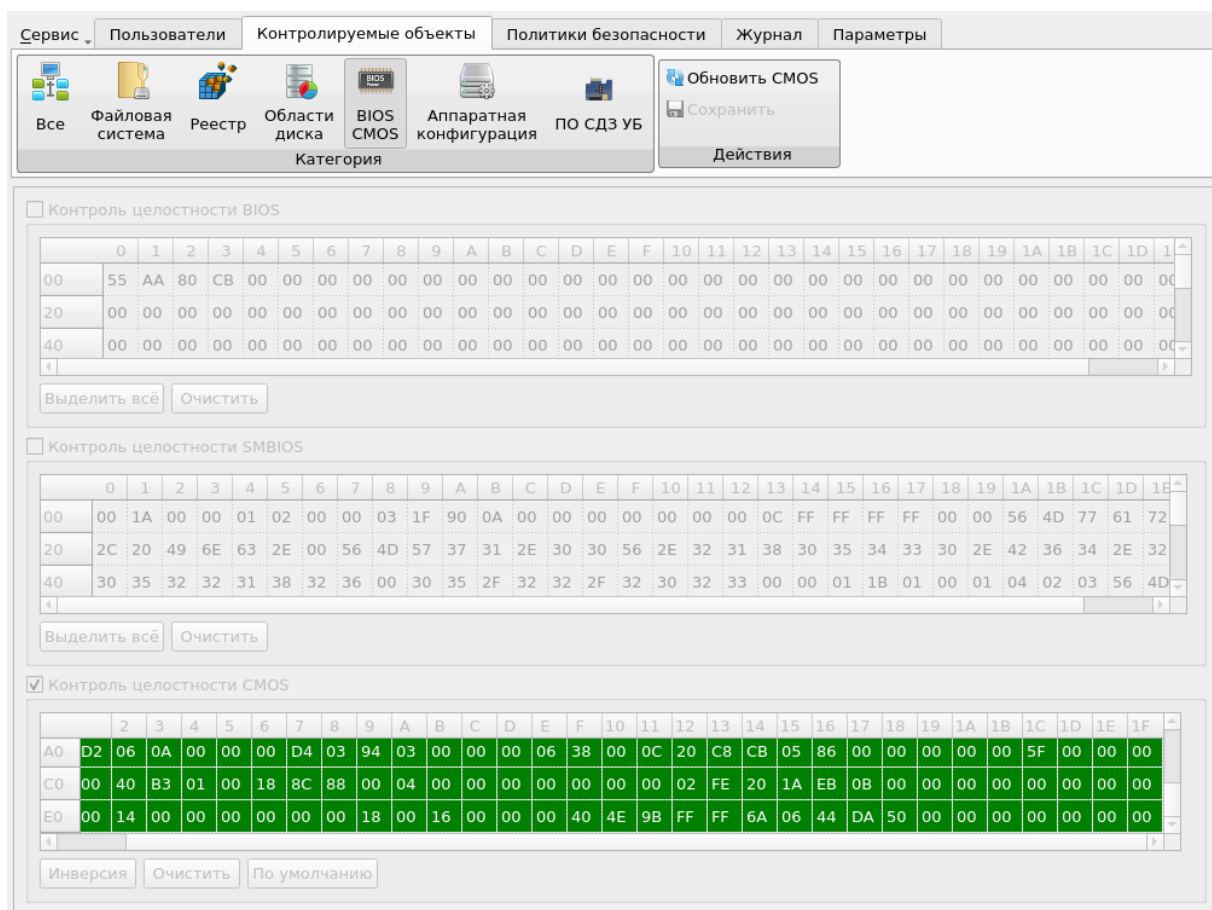


Рис. 21. Интерфейс «Контроль BIOS CMOS». Отображение информации о контролируемых значениях CMOS

- «Контроль аппаратной конфигурации» (полное описание интерфейса представлено в п. 7.2.4 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра информации о контролируемых объектах аппаратной конфигурации ТС и обновления результатов подсчета КС (Рис. 22).

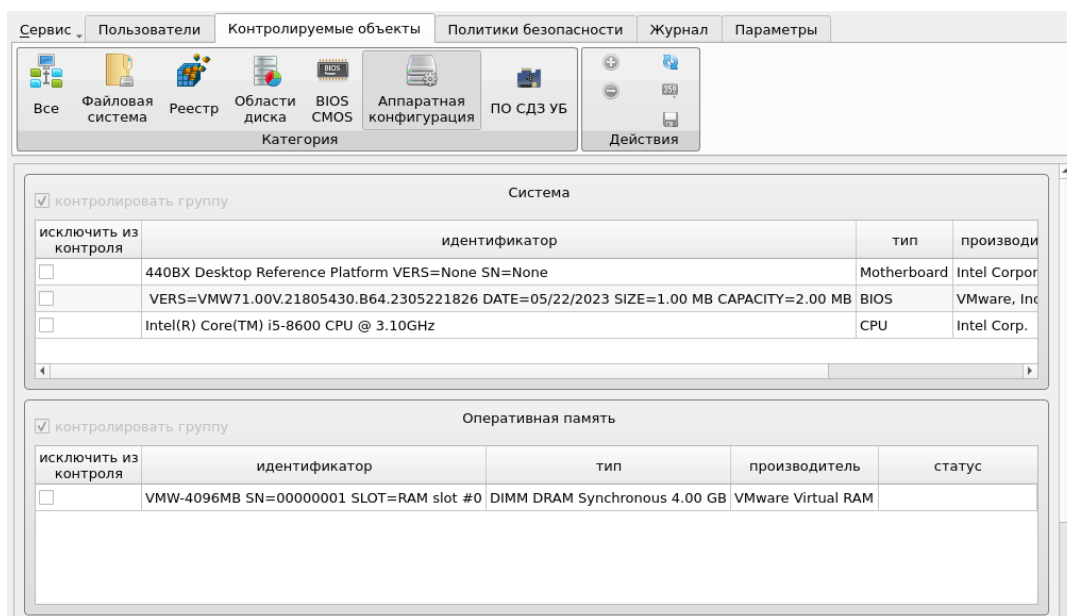


Рис. 22. Интерфейс «Контроль аппаратной конфигурации». Отображение информации о контролируемых объектах аппаратной конфигурации ТС

- «Контроль ПО СДЗ УБ» (полное описание интерфейса представлено в п. 7.2.5 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра информации о постановке под контроль ПО СДЗ УБ и обновления результатов подсчета КС (Рис. 23).

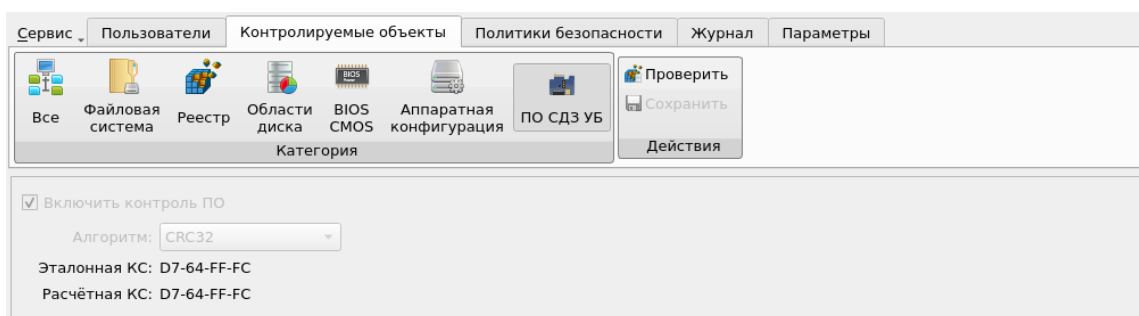


Рис. 23. Интерфейс «Контроль ПО СДЗ УБ». Отображение информации о постановке под контроль ПО СДЗ УБ

- «Политики безопасности» (полное описание интерфейса представлено в п. 9.2.1 документа «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС) в части просмотра значений политик паролей (Рис. 25) и политик авторизации (Рис. 24).

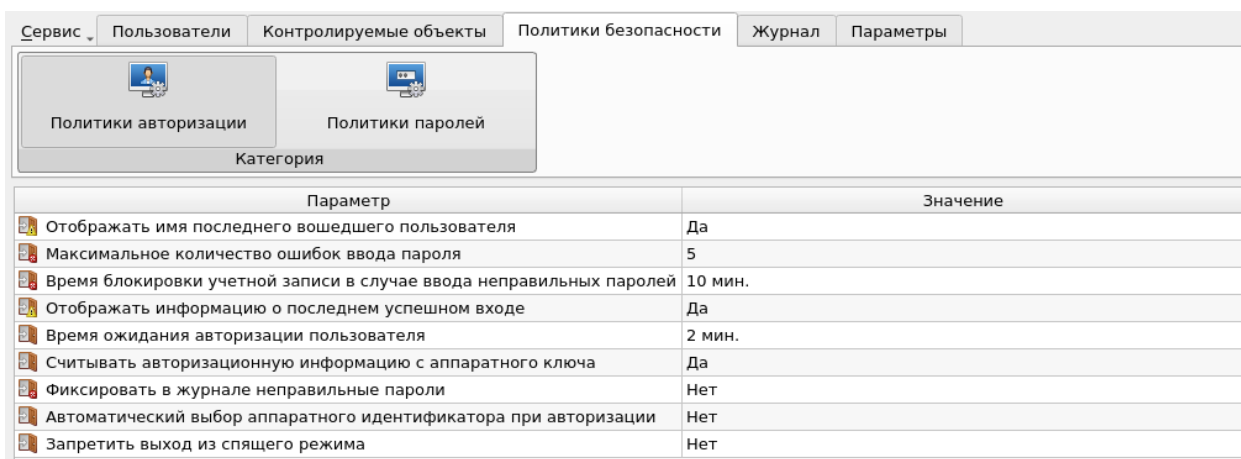


Рис. 24. Интерфейс «Политики безопасности». Отображение значений политик авторизации

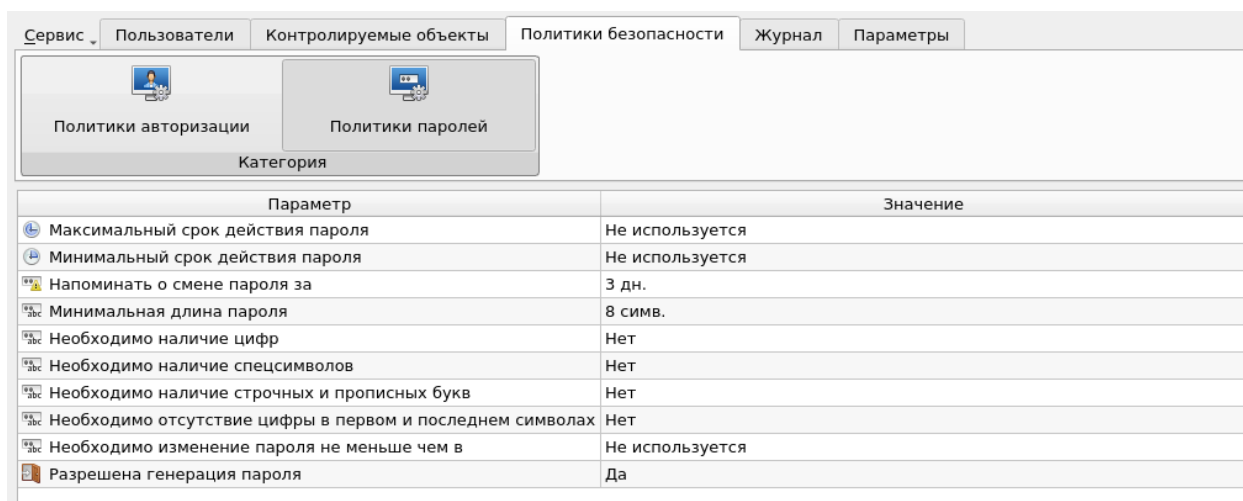


Рис. 25. Интерфейс «Политики безопасности». Отображение значений политик паролей

Описание доступных пользователю функций, возможных прав и обязанностей, а также принципов безопасной работы с описанными интерфейсами представлено в документах «Руководство по эксплуатации» ПФНА.501410.004 РЭ и «Полуформальная функциональная спецификация» ПФНА.501410.004 ПФС.

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
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
ТС	техническое средство
ШОС	штатная операционная система