

УТВЕРЖДЕН
ПФНА.501410.003 РЭ

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ

Dallas Lock

(версия изделия 5.0.397)



Руководство оператора
(пользователя)

ПФНА.501410.003 РЭ

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ.....	3
ВВЕДЕНИЕ	4
1 НАЗНАЧЕНИЕ СДЗ DALLAS LOCK	5
2 УСЛОВИЯ РАБОТЫ.....	6
2.1 ДАННЫЕ УЧЕТНОЙ ЗАПИСИ	6
2.2 ПРАВА ДЛЯ РАБОТЫ ПОД УЧЕТНОЙ ЗАПИСЬЮ	6
3 ЗАПУСК СДЗ DALLAS LOCK	8
3.1 ВХОД НА ЗАЩИЩЕННОЕ ТС	8
3.2 ОШИБКИ, ВОЗНИКАЮЩИЕ ПРИ ВХОДЕ	9
3.3 СМЕНА ПАРОЛЯ.....	9

ТЕРМИНЫ И СОКРАЩЕНИЯ

Некоторые термины, содержащиеся в тексте руководства, уникальны для **СДЗ Dallas Lock**, другие используются для удобства, третьи выбраны из соображений краткости.

Сокращение	Полная формулировка
АИ	аппаратный идентификатор
НШОС	нештатная операционная система
ПИН (ПИН-код)	пароль, предоставляющий доступ к защищенным АИ
СДЗ	средство доверенной загрузки
ТС	техническое средство
ШОС	штатная операционная система

ВВЕДЕНИЕ

Данное руководство предназначено для пользователей (операторов) ТС, на которых установлено изделие **Средство доверенной загрузки Dallas Lock** (далее — изделие, **СДЗ Dallas Lock**).

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

1 НАЗНАЧЕНИЕ СДЗ DALLAS LOCK

СДЗ Dallas Lock представляет собой программно-техническое средство, которое предназначено для блокирования попыток несанкционированной загрузки нештатной операционной системы (далее — НШОС), а также для предоставления доступа к информационным ресурсам загружаемой штатной операционной системы (ШОС) в случае успешной проверки подлинности.

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

В соответствии с требованиями безопасности предприятия лицами, ответственными за установку и эксплуатацию **СДЗ Dallas Lock**, проводится соответствующая настройка параметров и политик безопасности, а также механизмов, которые реализованы в **СДЗ Dallas Lock**. Подробное описание настройки механизмов администрирования содержится в документе Руководство системного программиста ПФНА.501410.003 32.

В оболочке администратора доступны гибкие настройки политик авторизации пользователей, работа с локальными и доменными учетными записями пользователей, локальное и удаленное управление платой **СДЗ**.

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

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

Пользователь (оператор) — пользователь защищенного персонального компьютера (ТС), осуществляющий ввод и обработку информации любыми программными средствами.

2 УСЛОВИЯ РАБОТЫ

К основным принципам безопасности работы **СДЗ Dallas Lock** относятся:

1. Выполнение ограничений по эксплуатации **СДЗ Dallas Lock**, перечисленных в п. 3.2 документа ПФНА.501410.003 ФО Формуляр.
2. Осуществление работы **СДЗ Dallas Lock** строго в соответствии с эксплуатационной документацией.

2.1 Данные учетной записи

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

Учетная запись пользователя, зарегистрированного в **СДЗ 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

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).

2.2 Права для работы под учетной записью

Доступ к управлению и права для работы пользователя и аудитора в **СДЗ Dallas Lock** назначаются администратором **СДЗ Dallas Lock** из строго предопределенного списка (Рис. 1).

Общие | Аппаратная идентификация | Вход в СЗИ НСД

Общие

Имя пользователя: admin

Категория пользователя: Администраторы

Описание

Расписание: Можно работать всегда Настроить

Атрибуты

- ☐ Отключен
- ☐ Потребовать смену пароля при следующем входе
- ☐ Запретить смену пароля пользователем
- ☐ Бессрочный пароль
- ☐ Запретить работу при нарушенной целостности
- ☐ Запретить работу при событиях от ДВК
- ☐ Запретить загрузку нештатной ОС
- ☐ Запретить работу при неисправности часов
- ☐ Запретить работу при неисправности ДСЧ

OK Отмена

Рис. 1. Настройка параметров учетных записей

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

Параметры безопасности средства, доступные пользователю — вход в систему и смена пароля в соответствии с правилами, если разрешено администратором.

Исходя из параметров безопасности, доступных пользователям, выделяют такое событие безопасности, как вход в систему (события аутентификации).

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

3 ЗАПУСК СДЗ DALLAS LOCK

3.1 Вход на защищенное ТС

При загрузке ТС с установленной платой **СДЗ Dallas Lock** появляется экран приглашения на вход в систему (рис. 2).

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

1. Включить питание компьютера. На экране появится приветствие (рис. 2)

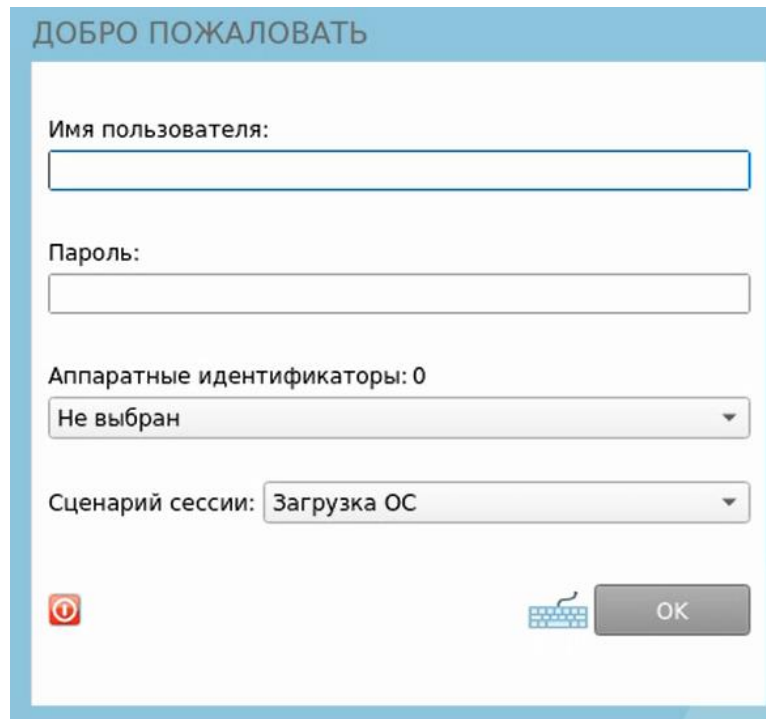


Рис. 2. Экран приглашения на вход в систему



Если защищенный **СДЗ Dallas Lock** компьютер введен в домен безопасности, в левом нижнем углу экрана приглашения на вход, рядом со значком  выведено соответствующее сообщение:

- «Соединение с 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 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 операционной системы;
 - «Смена пароля» — переход к смене пароля текущей учетной записи пользователя;
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 подставлены 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.



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

3.2 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 **СД3 Dallas Lock**;
- «Указан неверный пароль» — если введенный пароль неверен. Пользователю будет предложено повторно ввести имя и пароль;
- «Предъявлен неверный аппаратный идентификатор пользователя» — при отсутствии или предъявлении неверного АИ;
- «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.
- «Нарушена целостность контролируемых файлов» — выводиться 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;
- «Истек срок действия пароля. Смена пароля данному пользователю запрещена» — если истек срок действия пароля и у данной учетной записи установлен атрибут **Запретить смену пароля пользователем**. Необходимо обратиться к администратору.



Возможна ситуация, при которой пользователь забыл свой пароль. В этом случае он должен обратиться к администратору **СД3 Dallas Lock**, который может назначить учетной записи пользователя новый пароль.

3.3 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. 3)

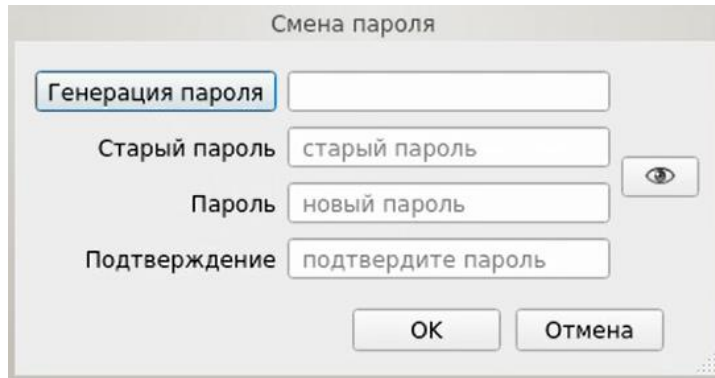


Рис. 3. Диалоговое окно смены текущего пароля учетной записи пользователя

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. 4).

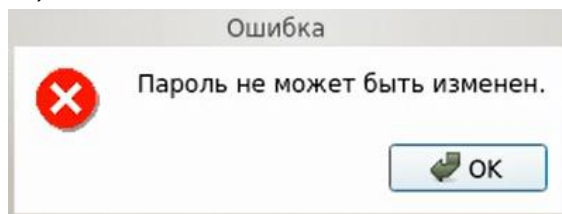


Рис. 4. Окно сообщения при запрете смены пароля пользователем

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. 5 и рис. 6), смена пароля не производится, осуществляется возврат к окну смены пароля.

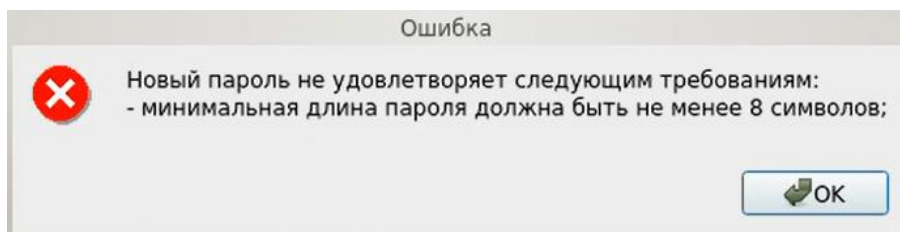


Рис. 5. Сообщение при несоответствии длины пароля учетной записи пользователя политике сложности паролей

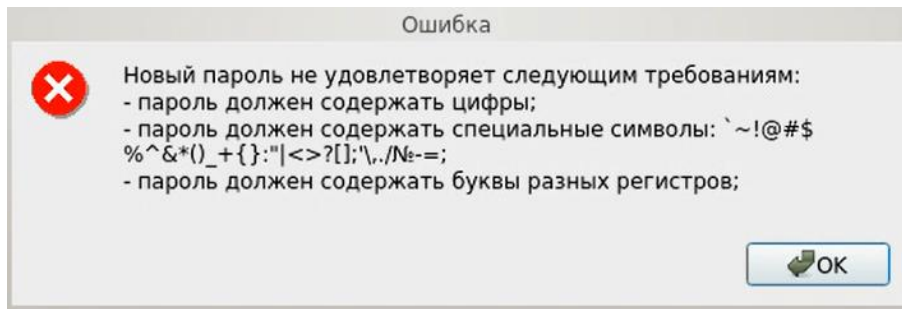


Рис. 6. Сообщение при несоответствии сложности пароля учетной записи пользователя политике сложности паролей



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). В **СДЗ Dallas Lock** 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 повтора не совпадают, выводится соответствующее сообщение и осуществляется возврат к окну смены пароля (рис. 7).

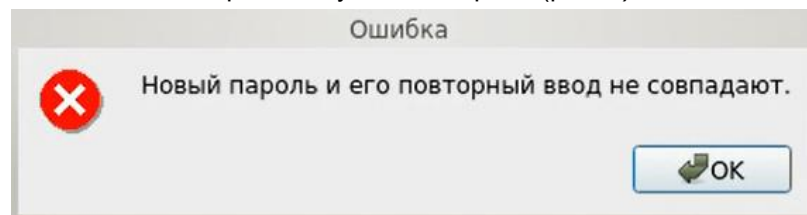


Рис. 7. Сообщение при несовпадении паролей

При успешной смене текущего пароля учетной записи пользователя выводится соответствующее сообщение (рис. 8) и осуществляется возврат в окно авторизации.

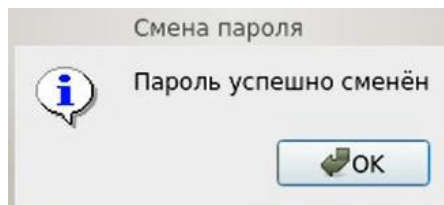


Рис. 8. Сообщение при успешной смене текущего пароля учетной записи пользователя



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. Пароль не может быть изменен». Производится возврат к этапу авторизации. Загрузка 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. 9) и по нажатию кнопки **ОК** происходит переход к процедуре смены пароля.

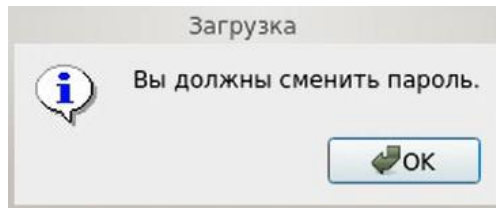


Рис. 9. Сообщение о необходимости сменить пароль

Дальнейшие действия осуществляются аналогично пункту **Смена пароля по запросу пользователя.**