

СРЕДСТВО ДОВЕРЕННОЙ ЗАГРУЗКИ «Dallas Lock»

Руководство оператора (пользователя)



ПФНА.501410.003 34

Листов 13

2018

Содержание

ВВЕДЕНИЕ	3
1 НАЗНАЧЕНИЕ СДЗ DALLAS LOCK	4
2 УСЛОВИЯ РАБОТЫ	5
2.1 Данные учетной записи	5
2.2 Права для работы под учетной записью	6
3 ВЫПОЛНЕНИЕ СДЗ DALLAS LOCK	7
3.1 Вход на защищенный компьютер.....	7
3.2 Ошибки, возникающие при входе	8
3.3 Смена пароля	9
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	12

Введение

Данное руководство предназначено для пользователей (операторов) рабочих станций, на которых установлено изделие «Средство доверенной загрузки «Dallas Lock» (далее по тексту – 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 предназначен для блокирования попыток несанкционированной загрузки штатной операционной системы (ШОС) средств вычислительной техники (СВТ), а также для предоставления доступа к информационным ресурсам загружаемой штатной операционной системы (ШОС) в случае успешной проверки подлинности.

СДЗ Dallas Lock предназначен для использования на персональных компьютерах и серверах архитектуры x86-32, x86-64.

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.

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.

Оператор (пользователь) – пользователь защищенного персонального компьютера, осуществляющий ввод и обработку информации любыми программными средствами.

2 УСЛОВИЯ РАБОТЫ


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 (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	
Персональный идентификатор	Пользователю могут быть выдан один аппаратный идентификатор
PIN-код аппаратного идентификатора	Если учетной записи пользователя назначен аппаратный идентификатор, то для авторизации дополнительно может быть использован PIN-код идентификатора

Внимание! Пользователю необходимо:

-  • уточнить у администратора все авторизационные данные для входа на защищенный компьютер.
- запомнить свое имя и пароль.
- никому не сообщать пароль и никому не передавать персональный аппаратный идентификатор.

Авторизация пользователя осуществляется при каждом запуске ПЭВМ.

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

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 Dallas Lock.

3 ЗАПУСК СДЗ DALLAS LOCK

3.1 Вход на защищенный компьютер

При загрузке компьютера с установленной платой СДЗ Dallas Lock появляется экран приглашения на вход в систему (Рис. 1).

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

1. Включить питание компьютера. На экране появится приветствие (Рис. 1).

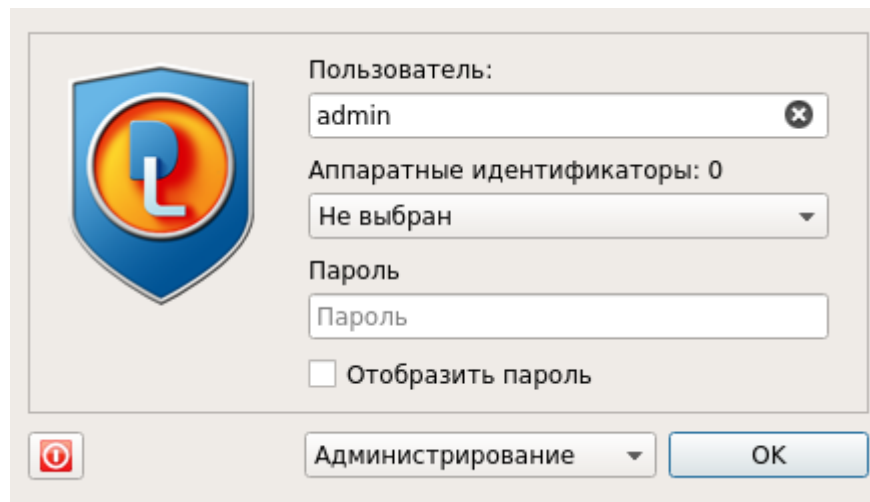


Рис. 1. Экран приглашения на вход в систему



Примечание. Если защищенный СДЗ Dallas Lock компьютер введен в Домен безопасности, в левом нижнем углу экрана приглашения на вход будет отображен соответствующий значок: - при наличии связи с Сервером безопасности, - при отсутствии связи с Сервером безопасности.

2. Предъявить аппаратный идентификатор (если назначен данной учетной записи).
3. Заполнить поле «Пользователь», имя учетной записи, под которой пользователь зарегистрирован в СДЗ Dallas Lock.
4. Ввести пароль. При вводе пароля поле для ввода является текстовым. На экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «•» (точка).
5. Выбрать в выпадающем списке:
 - «Загрузка» – переход к загрузке;
 - «Смена пароля» – переход к смене текущего пароля учетной записи пользователя.
6. Нажать кнопку «Enter».

Вход на защищенную ПЭВМ с использованием аппаратного идентификатора:

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 аппаратного идентификатора, 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.



Примечание. 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 СДЗ 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 аппаратного идентификатора;
- «Учетная запись отключена» - если администратор установил атрибут «Отключен» для данной учетной записи. Необходимо обратиться к администратору;
- «Достигнуто максимально допустимое количество ошибок ввода пароля. 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» - 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;
- «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.



Примечание. Возможна ситуация, при которой пользователь забыл свой пароль. В этом случае он должен обратиться к администратору СДЗ 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. 2)

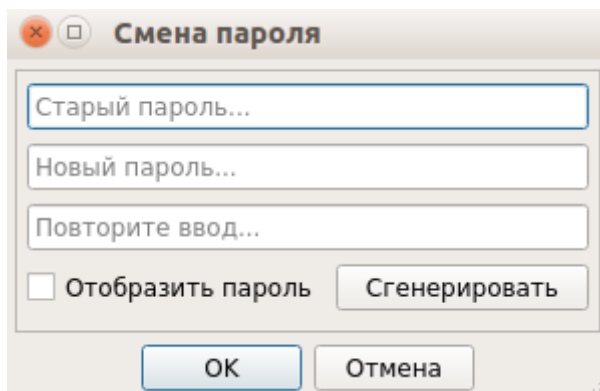


Рис. 2. Диалоговое окно смены текущего пароля учетной записи пользователя

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).

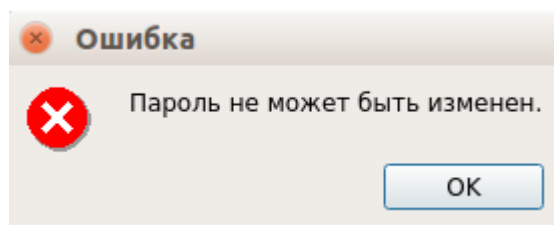


Рис. 3. Окно сообщения при запрете смены пароля пользователем

Для смены пароля необходимо корректно ввести:

- текущий пароль;
- новый пароль (должен отвечать установленным политикам сложности паролей);
- подтвердить новый пароль.

Также имеется 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, смена пароля не производится, осуществляется возврат к процедуре смены пароля (Рис. 4 и 5).

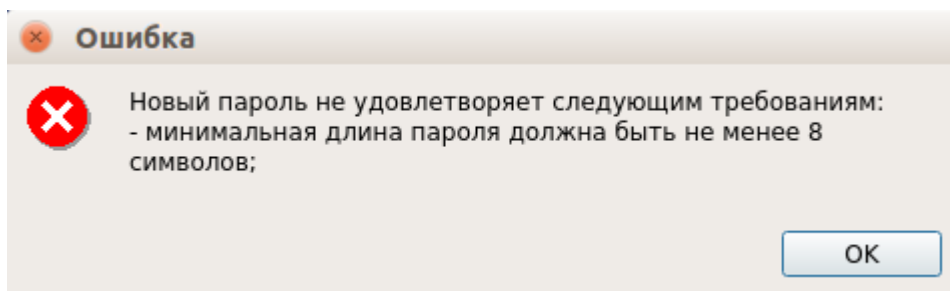


Рис. 4. Сообщение при несоответствии длины пароля учетной записи пользователя политике сложности паролей

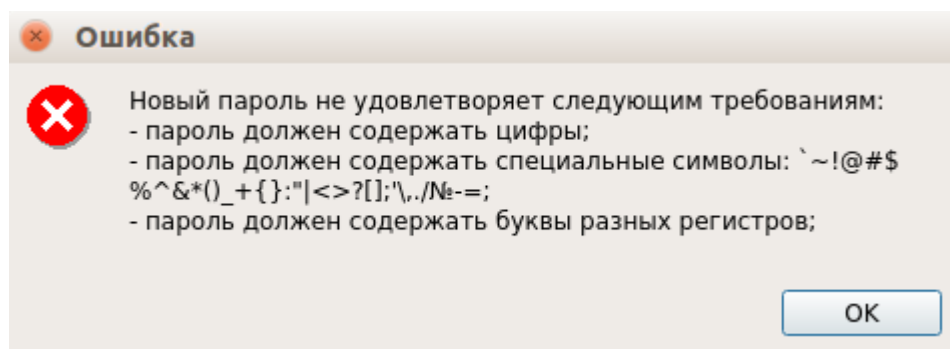


Рис. 5. Сообщение при несоответствии сложности пароля учетной записи пользователя политике сложности паролей



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). Для контроля правильности ввода значений пароля можно воспользоваться полем «Отобразить пароль».

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

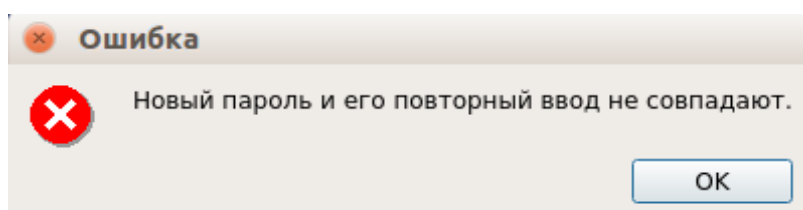


Рис. 6. Сообщение при несовпадении паролей

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

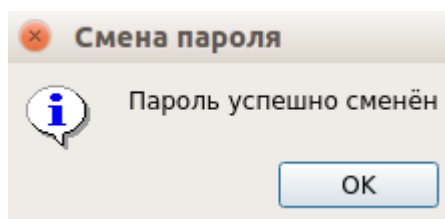


Рис. 7. Сообщение при успешной смене текущего пароля учетной записи пользователя



Примечание. При использовании авторизационных данных из аппаратного идентификатора новый пароль записывается в аппаратный идентификатор.

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 «Истёк 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 и по нажатию кнопки «ОК» происходит переход к процедуре смены пароля.

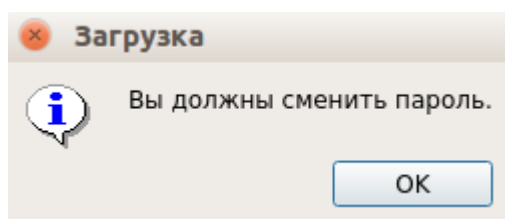


Рис. 8. Сообщение о необходимости сменить пароль

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

Термины и определения

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

Термин	Формулировка
BIOS	Базовая система ввода-вывода, реализованная в виде микропрограмм, записанных в ПЗУ (постоянное запоминающее устройство) компьютера. Это – первая программа, которую компьютер использует сразу же после включения. Задача – опознать устройства (процессор, память, видео, диски и т. д.), проверить их исправность, инициировать запуск ОС
АИ	Аппаратный идентификатор
ПЭВМ	Персональная электронно-вычислительная машина (компьютер)
ШОС	Штатная операционная система
НШОС	Нештатная операционная система

