УТВЕРЖДЕН
ПФНА.501410-02 34 01-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА Dallas Lock Linux

Руководство оператора (пользователя)

ПФНА.501410-02 34 01

Листов 11

2016 г.

Аннотация

Настоящее руководство оператора распространяются на изделие «Система защиты информации от несанкционированного доступа Dallas Lock Linux» (далее по тексту - изделие).

В состав изделия входит сертифицированное программное обеспечение (ПО) «Система защиты информации от несанкционированного доступа Dallas Lock Linux» (далее по тексту – «СЗИ НСД» или «Dallas Lock Linux»).

Изделие рассчитано на обслуживание и эксплуатацию персоналом со среднетехническим образованием.

В руководстве содержатся сведения, необходимые пользователю для работы на защищенном СЗИ НСД техническом средстве.

Руководство подразумевает наличие у пользователя навыков работы в операционной системе Linux.

Содержание

1. НАЗНАЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ

1.1. Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), автоматизированных системах управления производственными и технологическими процессами (АСУ ТП), государственных информационных системах (ГИС).

1.2. Изделие предназначено для использования на технических средствах (ТС), таких как: персональные компьютеры, портативные компьютеры (ноутбуки), сервера и ТС с поддержкой виртуальных сред.

1.3. СЗИ НСД предназначена для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа (НСД) на ТС, работающих под управлением следующих операционных систем (ОС) семейства Linux:

- Debian 7.8 (systemd) x86/x64 (версия ядра 3.2.65-1 x86_64);

- CentOS 7.0 x86/x64 (версия ядра 3.10.0-123.el7. x86_64);

- Red Hat Enterprise Linux Server 7.0 x86/x64 (версия ядра 3.10.0-123.el7.x86_64);

- Fedora 20 x86/x64 (версия ядра 3.11.10-301.fc20.x86_64);

- openSUSE 12.3 x86/x64 (версия ядра 3.7.10-1.1-desktop).

2. УСЛОВИЯ ВЫПОЛНЕНИЯ СИСТЕМЫ ЗАЩИТЫ

2.1. Данные учетной записи

2.1.1. Чтобы получить доступ к компьютеру, на который установлена СЗИ НСД, необходимо иметь зарегистрированную в системе защиты учетную запись.

2.1.2. Регистрация учетных записей осуществляется администратором безопасности.

2.1.3. Пользователю защищенного ТС необходимо уточнить у администратора безопасности свои авторизационные данные. Запомнить свое имя в системе защиты и пароль. Никому не сообщать пароль и никому не передавать персональный аппаратный идентификатор.

2.1.4. Учетная запись пользователя, зарегистрированного в СЗИ НСД, имеет следующие атрибуты, которые необходимы непосредственно для входа на защищенный компьютер (авторизации):

	Описание
Имя (логин)	За пользователем закрепляется условное имя (идентификатор), необходимое для идентификации его в системе защиты. - максимальная длина имени – 16 символов; - имя может содержать латинские символы, цифры и специальные символы. Разрешается использовать различные регистры клавиатуры, при этом нужно помнить, что заглавные и прописные буквы воспринимаются как различные (User и user являются разными именами)
Пароль	Пользователю сообщается пароль, который необходим для подтверждения того, что именно он является пользователем, зарегистрированным под этим именем (происходит аутентификация). - длина пароля – от 6 до 16 символов; - пароль может содержать латинские символы, 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)
Персональный идентификатор	Пользователю могут быть выдан один электронный идентификатор

2.2. Права для работы под учетной записью

2.2.1. Пользователю защищенного ТС необходимо выяснить у администратора безопасности, какими именно правами и привилегиями обладает пользователь, к каким ресурсам может иметь доступ и с какими программами и приложениями работать.

2.2.2. Во всех сложных ситуациях, связанных с работой на защищенном ТС, которые пользователь не в состоянии разрешить самостоятельно, необходимо обращаться к администратору. Так, в частности, если имеющихся прав доступа к ресурсам недостаточно для эффективного выполнения должностных обязанностей (запрещающие сообщения), необходимо обратиться к администратору безопасности или другому должностному лицу, отвечающему за распределение прав доступа к ресурсам компьютера и сети.

3. РАБОТА НА ЗАЩИЩЕННОМ ТС

В данном разделе представлена общая информация. За более подробной информацией следует обратиться к документации на используемую ОС.

В зависимости от используемой ОС можно воспользоваться одним из следующих источников:

- Debian 7.8 (systemd): https://www.debian.org/doc/;
- CentOS 7.0: https://wiki.centos.org/;
- Red Hat Enterprise Linux Server 7.0: http://www.redhat.com/en/resources;
- Fedora 20: https://fedoraproject.org/wiki/Fedora_Project_Wiki/ru;
- openSUSE 12.3: https://en.opensuse.org/Main_Page.

3.1. Вход в защищенную ОС

Вход в защищенную ОС осуществляется точно так же, как и в незащищенную.

3.1.1. Вход с использованием консоли

Для осуществления входа необходимо ввести логин пользователя (Рисунок 1).

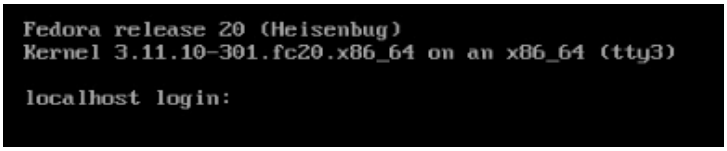

Рисунок 1 – Вход на защищенное ТС. Ввод логина пользователя

После корректного ввода логина должно отобразиться предложение ввести пароль пользователя.

Следует обратить внимание, что при вводе пароля символы пароля отображаться на экране не будут, так же не будут отображаться звездочки или иные символы (Рисунок 2).

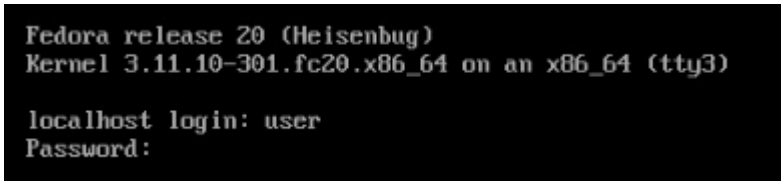

Рисунок 2 – Вход на защищенное ТС. Ввод пароля пользователя

После корректного ввода логина и пароля должна отобразиться строка приветствия (Рисунок 3).

Рисунок 3 – Строка приветствия

3.1.2. Вход с использованием графической оболочки ОС

3.1.2.1. KDE

Для осуществления входа необходимо ввести имя пользователя и пароль, нажать кнопку «Enter» на клавиатуре (Рисунок 4).

Рисунок 4 – KDE. Вход в ОС

3.1.2.2. GNOME

Для осуществления входа необходимо выбрать пользователя (Рисунок 5), ввести пароль и нажать кнопку «Войти» (Рисунок 6).

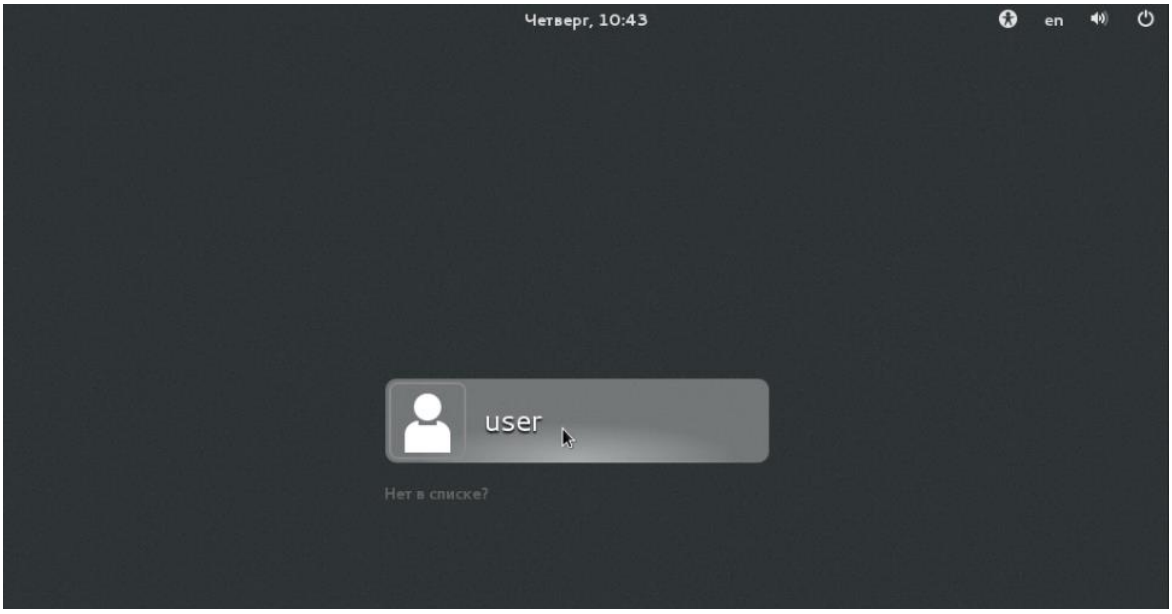

Рисунок 5 –GNOME. Выбор пользователя

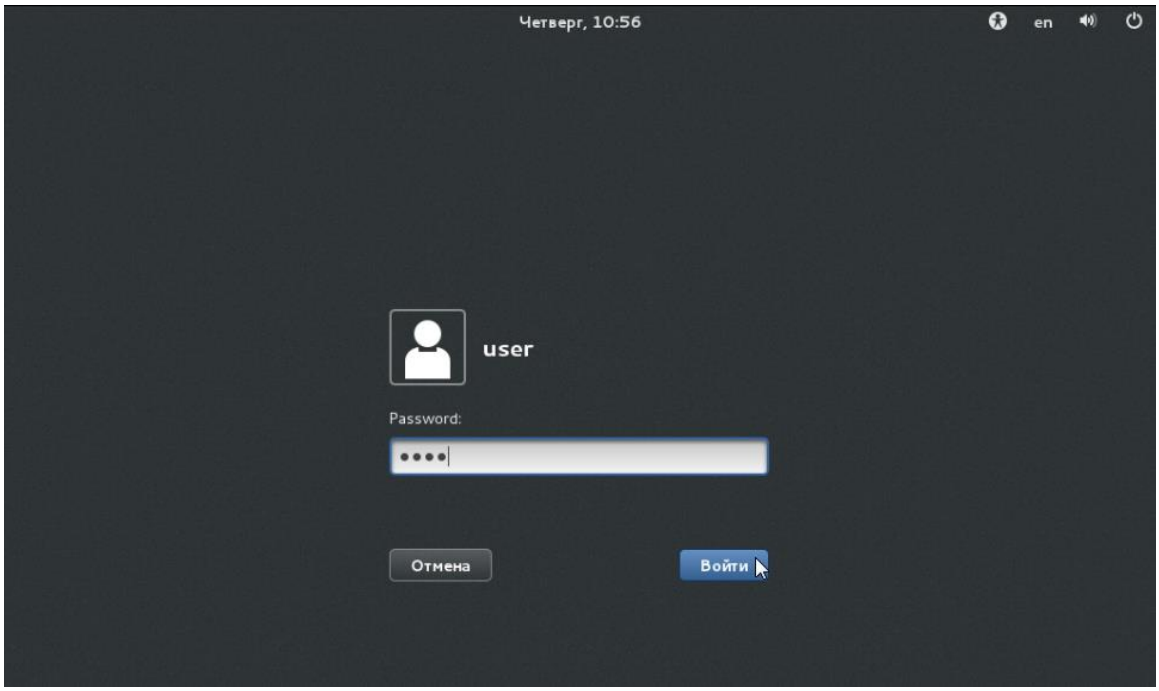

Рисунок 6 –GNOME. Ввод пароля.

3.2. Завершение сеанса работы

Завершение сеанса работы на защищенном ТС осуществляется точно так же, как и на незащищенном ТС.

Для завершения сеанса работы необходимо нажать клавиши Ctrl+D.

Вместо строки приветствия (см. Рисунок 2) будет отображаться предложение ввести логин пользователя (см. Рисунок 1).

Также поддерживается завершение сеанса работы с использованием графической оболочки ОС.

Для получения более подробной информации обратитесь с документации на используемую ОС.

3.3. Смена пользователя

Смена пользователя на защищенном ТС осуществляется точно так же, как и на незащищенном ТС.

Для смены пользователя необходимо осуществить завершение сеанса работы. Строка приветствия будет изменена на предложение ввести логин пользователя.

Также поддерживается смена пользователя с использованием графической оболочки ОС.

Для получения более подробной информации обратитесь с документации на используемую ОС.

3.4. Смена пароля

Смена пароля на защищенном ТС осуществляется точно так же, как и на незащищенном ТС.

Для смены пароля необходимо запустить эмулятор терминала или перейти в терминальный сеанс (одновременно нажать клавиши «Ctrl», «Alt» и одну из функциональных клавиш «F2»-«F6») и ввести команду *passwd* (Рисунок 7).

Администратор СЗИ НСД средствами СЗИ НСД может запретить смену пароля пользователем.

В этом случае при необходимости сменить пароль, следует обратиться к администратору.

Рисунок 7 – Смена пароля

Также поддерживается смена пароля с использованием графической оболочки ОС.

Для получения более подробной информации обратитесь с документации на используемую ОС.

3.5. Блокировка ТС

Блокировка защищенного ТС осуществляется точно так же, как и блокировка незащищенного ТС.

Для осуществления блокировки ТС необходимо ввести команду *vlock* (Рисунок 8).

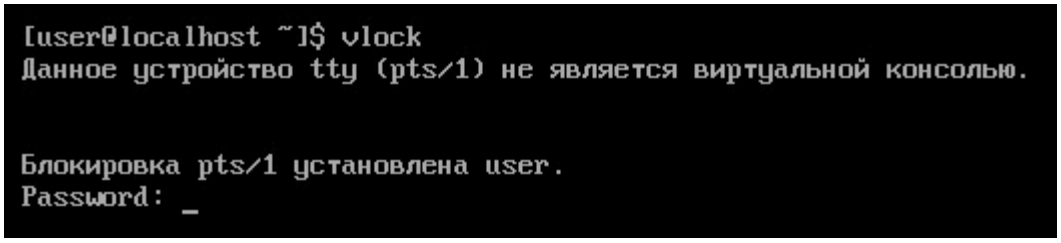

Рисунок 8 – Блокировка защищенного ТС

Также поддерживается блокировка ТС с использованием графической оболочки ОС.

Для получения более подробной информации обратитесь с документации на используемую ОС.

4. СООБЩЕНИЯ ОБ ОШИБКАХ

4.1. Ошибки, возникающие при входе

4.1.1. Попытка входа пользователя на защищенное ТС может быть неудачной, к чему приводит ряд событий. При этом на экран могут выводиться сообщения о характере события и сообщения предупреждающего характера (Рисунок 9).

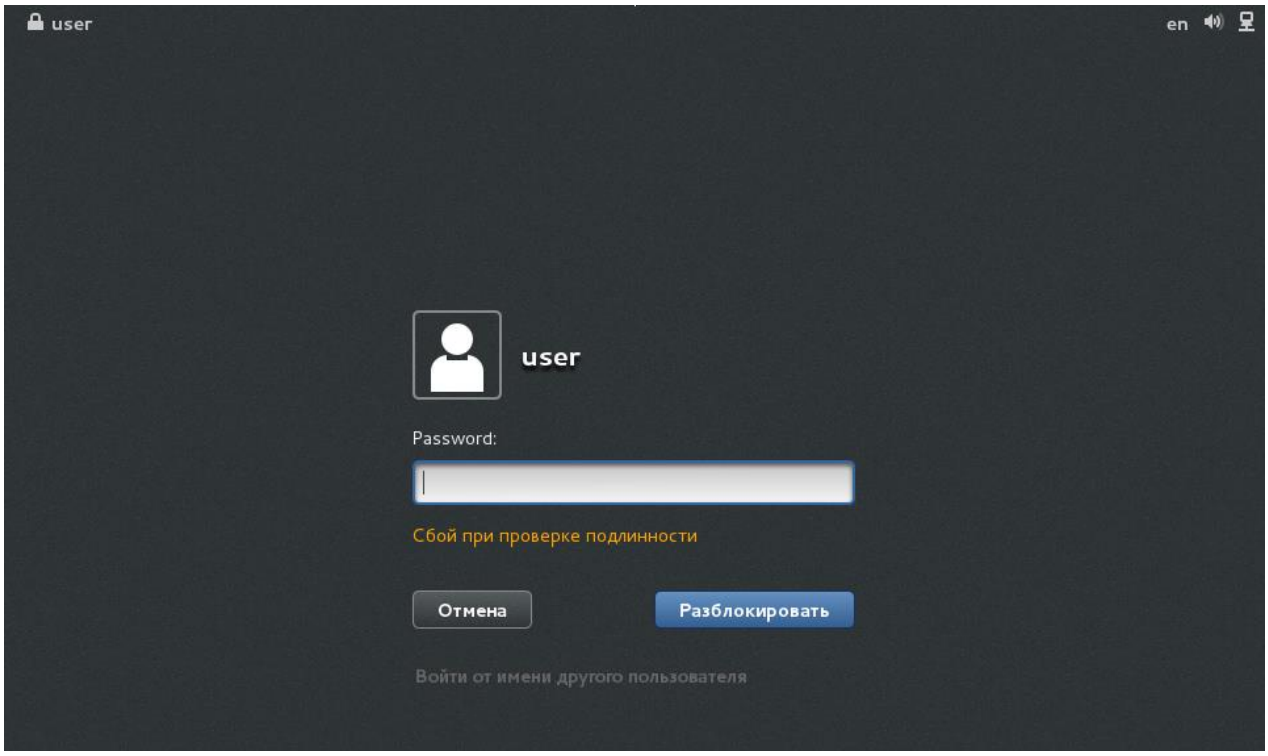

Рисунок 9 – GNOME. Сообщение об ошибке

Для получения более подробной информации обратитесь с документации на используемую ОС.