УТВЕРЖДЕН
ПФНА.501410.002 34-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock Linux

Руководство оператора (пользователя)

ПФНА.501410.002 34

Листов 11

АННОТАЦИЯ

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

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 семейства Linux.

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ СИСТЕМЫ ЗАЩИТЫ

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), при защите значимых объектов критической информационной инфраструктуры (КИИ).

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

Система защиты информации от несанкционированного доступа «Dallas Lock Linux» (СЗИ НСД) может быть использовано на ТС, работающих под управлением операционных систем (ОС) семейства Linux[1]:

- Альт Рабочая Станция 8.2 x64 (версия ядра СЗИ НСД 4.9);
- Альт Рабочая Станция 9.0 x64 (версия ядра СЗИ НСД 4.19);
- Astra Linux Common Edition (Орёл) 2.12 x64 (версия ядра СЗИ НСД 4.19);
- Debian 8 (версия ядра СЗИ НСД 3.16);
- Debian 9 (версия ядра СЗИ НСД 4.19);
- CentOS 7 x64 (версия ядра СЗИ НСД 3.16);
- Red Hat Enterprise Linux 7 x64 (версия ядра СЗИ НСД 3.16);
- Fedora 30 x64 (версия ядра СЗИ НСД 4.19);
- Ubuntu 16.04 x64 (версия ядра СЗИ НСД 4.19);
- Ubuntu 18.04 x64 (версия ядра СЗИ НСД 4.19);
- РЕД ОС 7.1, 7.2 Муром (версия ядра СЗИ НСД 4.19);
- ROSA Enterprise Linux Desktop/Server x64 (версия ядра СЗИ НСД 3.16);
- ЛотОС 2.1 x64 (версия ядра СЗИ НСД 3.16).

СЗИ НСД поддерживает 64-битные версии ОС архитектуры AMD64 (архитектура IA64 (Itanium) не поддерживается).

СЗИ НСД поддерживает следующие типы файловой системы: ext2, ext3, ext4, JFS, Reiser FS.

СЗИ НСД может функционировать как на автономных ТС, так и на ТС в составе локальной вычислительной сети.

Поддерживаемые внешние устройства:

- USB-накопители, внешние жесткие диски, накопители на оптических дисках;
- принтеры;
- беспроводные устройства.

[1] При установке СЗИ НСД происходит замена ядра ОС на ядро, включающее программные модули СЗИ НСД.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ СИСТЕМЫ ЗАЩИТЫ

2.1 Данные учетной записи

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

Регистрация учетных записей пользователей осуществляется администратором безопасности.

Пользователю защищенного ТС необходимо уточнить у администратора безопасности свои авторизационные данные, запомнить имя своей учетной записи и пароль. Пользователю запрещается сообщать кому-либо пароль и передавать персональный аппаратный идентификатор.

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

Атрибут	Основные
Имя (логин)	За пользователем закрепляется условное имя (идентификатор), необходимое для идентификации его в системе защиты. - максимальная длина имени — 64 символа; - имя должно состоять только из строчных букв, цифр, символов «_» и «-»; имя должно начинаться со строчной буквы или символа подчёркивания, может заканчиваться символом «$»
Пароль	Пользователю сообщается пароль, который необходим для подтверждения того, что именно он является пользователем, зарегистрированным под этим именем (для прохождения аутентификации). - 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	Аппаратная идентификация в СЗИ НСД не является обязательной и может применяться дополнительно к основному способу аутентификации пользователя с помощью пароля. Пользователю может быть назначен только один аппаратный идентификатор

2.2 Права для работы под учетной записью

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

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

2.2.1 Работа на защищенном ТС

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

Описание доступных пользователю функций, возможных прав и обязанностей, а также принципов безопасной работы с предоставленными в СЗИ НСД интерфейсами и типов событий безопасности представлено в документах «Руководство по эксплуатации» ПФНА.501410.002 РЭ и «Полная функциональная спецификация» ПФНА.501410.002 ПФС.

Описание мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования представлено в документе ПФНА.501410.002 ЗБ «Задание по безопасности».

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

- Debian (systemd): https://www.debian.org/doc/;
- CentOS: https://wiki.centos.org/;
- Red Hat Enterprise Linux Server: https://www.redhat.com/en/resources;
- Fedora: https://fedoraproject.org/wiki/Fedora_Project_Wiki/ru;
- Ubuntu: https://wiki.ubuntu.com;
- ЛотОС: https://lotos-group.ru/lotos.html;
- Astra Linux: https://astralinux.ru/information/library;
- Альт Рабочая Станция: https://docs.altlinux.org/ru-RU/index.html;
- РЕД ОС: https://redos.red-soft.ru/documentation/;
- ROSA Enterprise Linux: https://www.rosalinux.ru/docs/.

2.3 Вход в защищенную ОС

2.3.1 Вход с использованием консоли

При входе в ОС без использования графической оболочки ОС отображается запрос на вход по аппаратному идентификатору (рисунок 1).

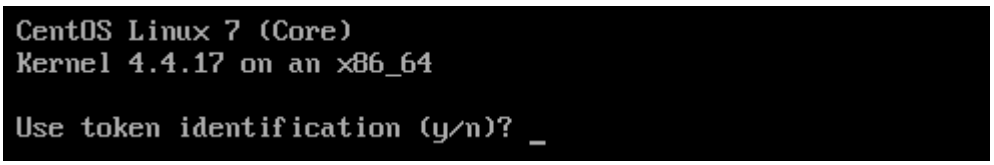

Рисунок 1. Вход на защищенное ТС

Если пользователю не назначен аппаратный идентификатор, необходимо ввести «n» и нажать кнопку «Enter», появится предложение ввести имя пользователя. После корректного ввода логина будет предложено ввести пароль (рисунок 2).

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

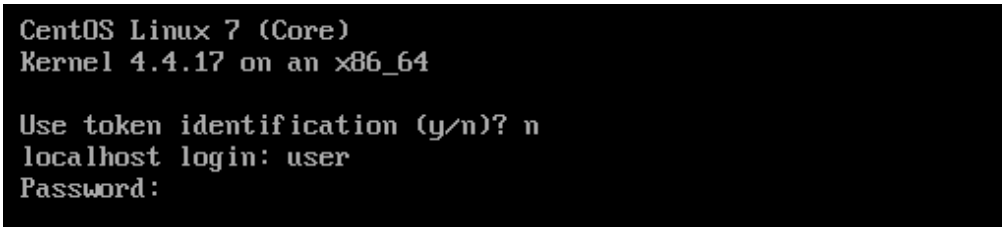

Рисунок 2. Вход на защищенное ТС пользователя, которому не назначен аппаратный идентификатор

После корректного ввода логина и пароля отобразится строка приглашения к вводу команд (рисунок 3).

Рисунок 3. Строка приглашения к вводу команд

Если пользователю назначен аппаратный идентификатор, необходимо его предъявить, затем ввести «y» и нажать кнопку «Enter».

В зависимости от хранимой на аппаратном идентификаторе информации возможна различная последовательность дальнейших шагов.

Если в открытой памяти идентификатора хранится пароль учетной записи, логин и пароль считается с ключа автоматически. Отобразится строка приглашения к вводу команд (рисунок 3).
Если в закрытой памяти идентификатора хранится пароль учетной записи, то пользователю необходимо ввести PIN-код идентификатора (рисунок 4).

Следует обратить внимание, что при вводе PIN-кода символы PIN-кода отображаться на экране не будут, так же не будут отображаться звездочки или иные символы.

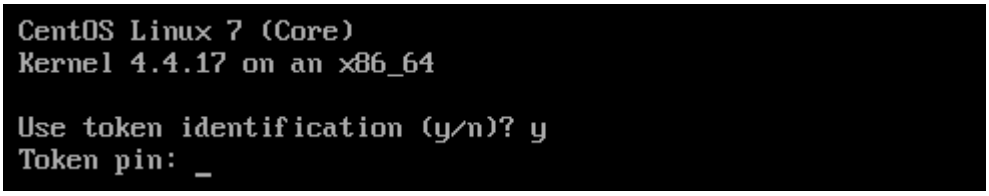

Рисунок 4. Вход на защищенное ТС с аппаратным идентификатором. Ввод PIN-кода идентификатора

После корректного ввода PIN-кода идентификатора отобразится строка приглашения к вводу команд (рисунок 3).

Если в идентификаторе хранится информация только о логине учетной записи, то пользователю необходимо ввести пароль учетной записи (рисунок 5).

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

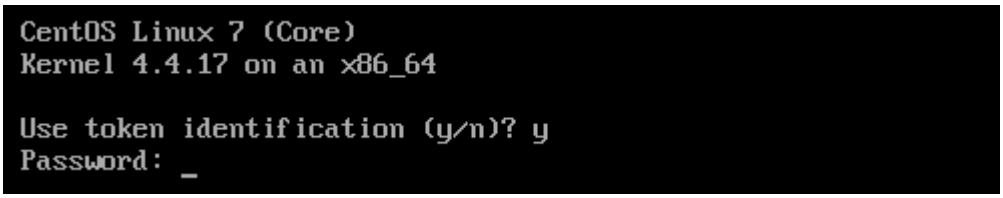

Рисунок 5. Вход на защищенное ТС с аппаратным идентификатором. Ввод пароля пользователя

После корректного ввода пароля отобразится строка приглашения к вводу команд (рисунок 3).

Если в идентификаторе не хранится информация об учетной записи, то пользователю необходимо по запросу ОС ввести логин и пароль учетной записи (рисунок 6).

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

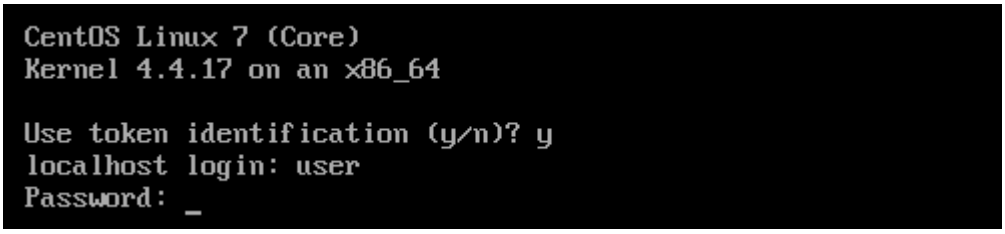

Рисунок 6. Вход на защищенное ТС с аппаратным идентификатором. Ввод логина и пароля пользователя

После корректного ввода логина и пароля отобразится строка приглашения к вводу команд (рисунок 3).

2.4 Вход с использованием графической оболочки ОС GNOME

Для осуществления входа необходимо выбрать пользователя (рисунок 7).

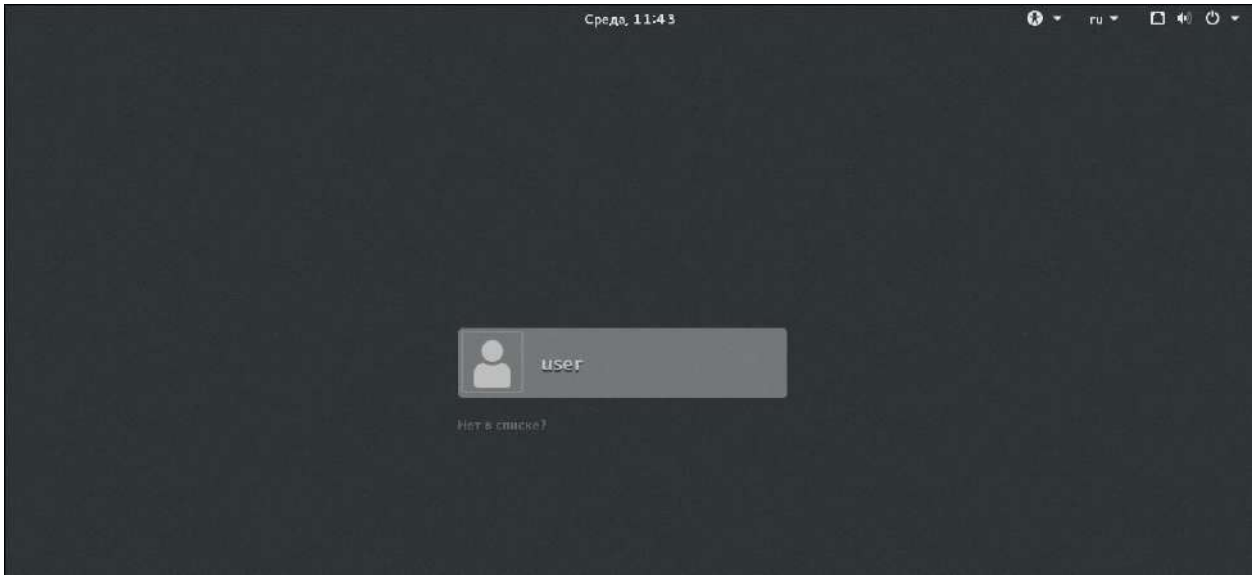

Рисунок 7. GNOME. Выбор пользователя

Если пользователю не назначен аппаратный идентификатор, необходимо ввести пароль и нажать кнопку «Войти» (рисунок 8).

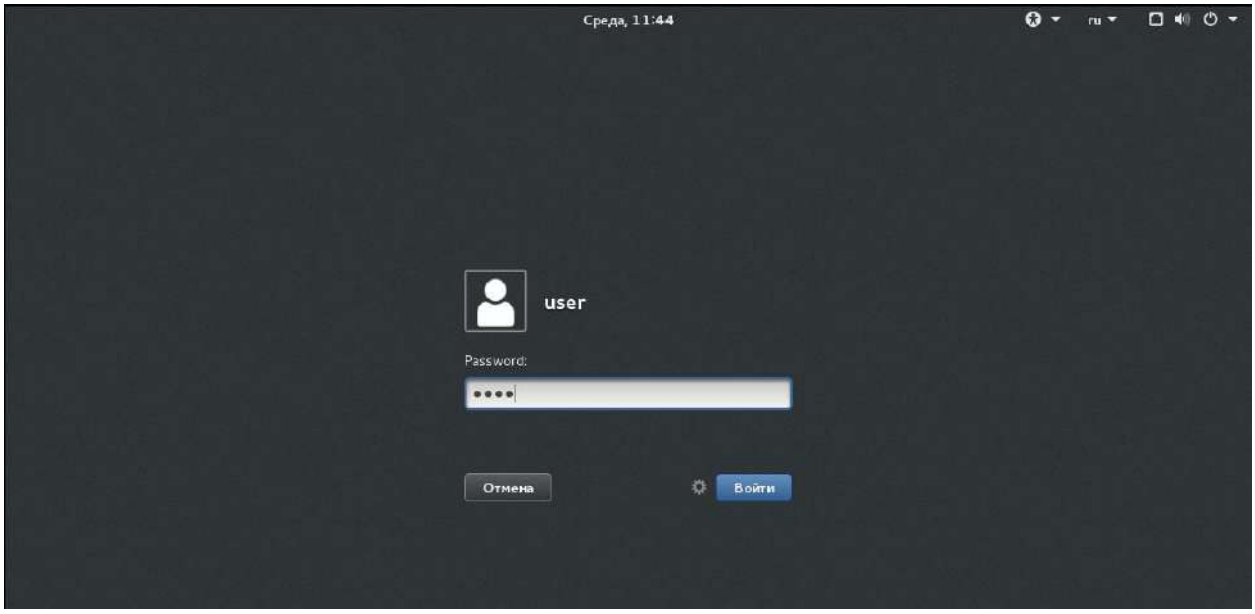

Рисунок 8. GNOME. Ввод пароля

Если пользователю назначен аппаратный идентификатор, то отобразится запрос на вход по аппаратному идентификатору, пользователю необходимо его предъявить, затем ввести «y» и нажать кнопку «Далее» (рисунок 9).

Рисунок 9. GNOME. Запрос на вход по аппаратному идентификатору

В зависимости от хранимой на аппаратном идентификаторе информации возможна различная последовательность дальнейших шагов.

Если в открытой памяти идентификатора хранится пароль учетной записи, логин и пароль считается с ключа автоматически.

Если в закрытой памяти идентификатора хранится пароль учетной записи, то пользователю необходимо ввести PIN-код идентификатора (рисунок 10).

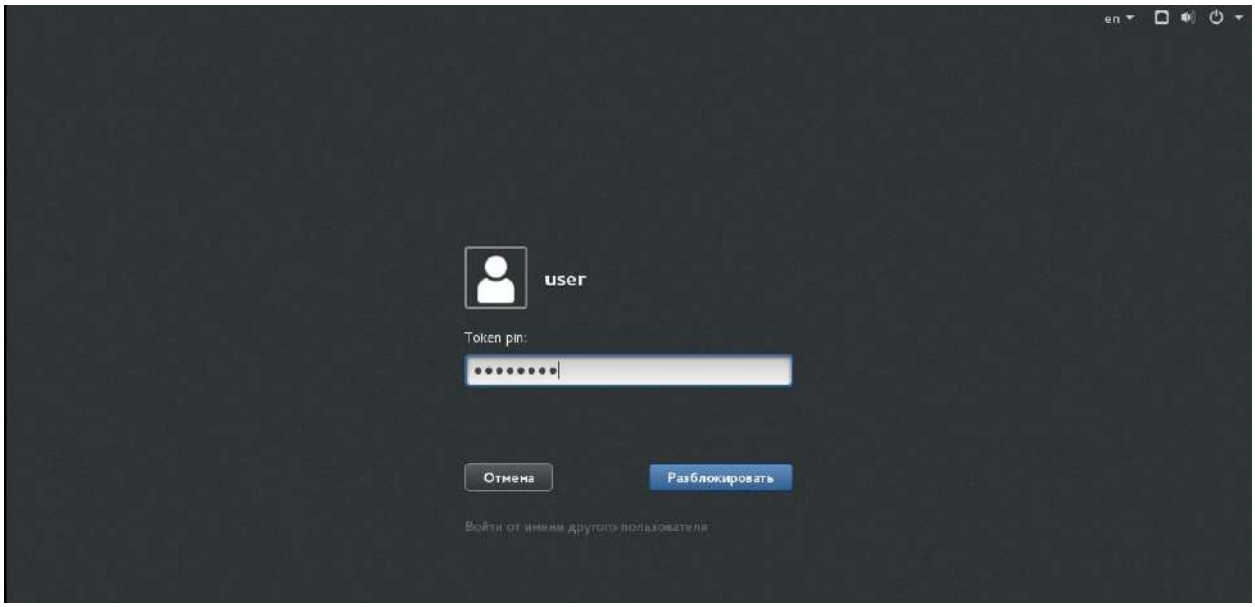

Рисунок 10. GNOME. Ввод PIN-кода идентификатора

Если в идентификаторе хранится информация только о логине учетной записи, то пользователю необходимо ввести пароль учетной записи (рисунок 8).

Если в идентификаторе не хранится информация об учетной записи, то пользователю необходимо ввести логин и пароль учетной записи.

2.5 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 приглашения к вводу команд (рисунок 3) будет отображаться запрос на вход по аппаратному идентификатору (рисунок 1).

Также поддерживается завершение сеанса работы с использованием графической оболочки ОС.

За более подробной информацией следует обратиться к документации на используемую ОС.

2.6 Смена пользователя

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

Для смены пользователя необходимо осуществить завершение сеанса работы. Вместо строки приглашения к вводу команд (рисунок 3) будет отображаться запрос на вход по аппаратному идентификатору (рисунок 1).

Также поддерживается смена пользователя с использованием графической оболочки ОС.

За более подробной информацией следует обратиться к документации на используемую ОС.

2.7 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 11).

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

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

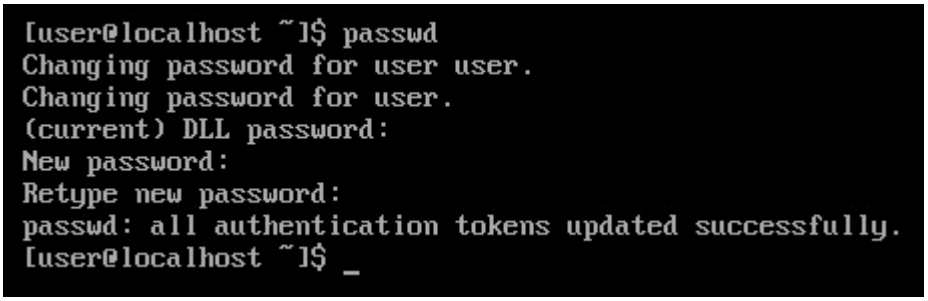

Рисунок 11. Смена пароля

Также поддерживается смена пароля с использованием графической оболочки ОС.

За более подробной информацией следует обратиться к документации на используемую ОС.

2.8 Блокировка ТС

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

Для осуществления блокировки ТС необходимо ввести команду *vlock* (рисунок 12).

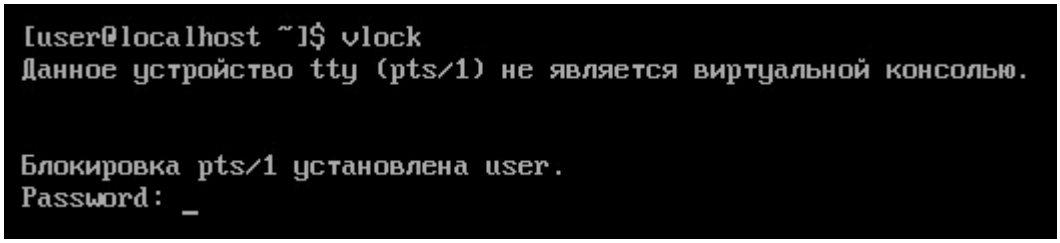

Рисунок 12. Блокировка защищенного ТС

Также поддерживается блокировка ТС с использованием графической оболочки ОС.

За более подробной информацией следует обратиться к документации на используемую ОС.

3 СООБЩЕНИЯ ОБ ОШИБКАХ

3.1 Ошибки, возникающие при входе

Попытка входа пользователя на защищенное ТС может быть неудачной по ряду причин. При этом на экран выводятся сообщения о характере события и сообщения предупреждающего характера (рисунок 13).

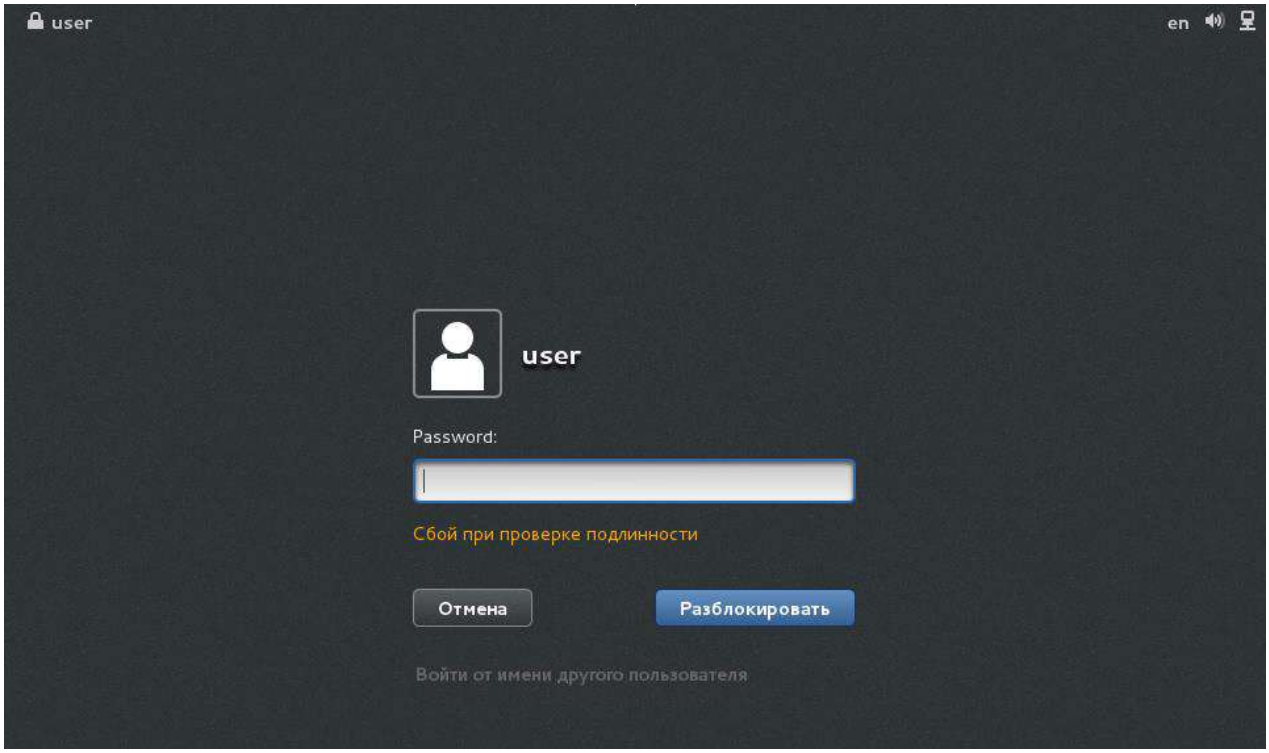

Рисунок 13. GNOME. Сообщение об ошибке

За более подробной информацией следует обратиться к документации на используемую ОС.

Внимание! При всех затруднительных ситуациях, возникающих вследствие ошибок работы на ТС, следует обращаться к администратору.