УТВЕРЖДЕН
ПФНА.501410.002 34-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Dallas Lock Linux

Руководство оператора (пользователя)

ПФНА.501410.002 34

Листов 12

АННОТАЦИЯ

Настоящее руководство оператора (пользователя) распространяется 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, информационных системах персональных данных, автоматизированных системах управления производственными и технологическими процессами, государственных информационных системах, при защите значимых объектов критической информационной инфраструктуры.

Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа на технических средствах, работающих под управлением следующих операционных систем семейства Linux (x64).

Поддерживаются такие ОС[1]:

- Альт 8 СП релиз 10 (Рабочая станция, Сервер);
- Альт Рабочая Станция 9.0, 9.1, 9.2, 10.0, 10.1, 10.2;
- Альт Сервер 10;
- Astra Linux Common Edition 2.12;
- Astra Linux Special Edition 1.7;
- Debian 10, 11;
- Red Hat Enterprise Linux 7;
- Ubuntu-desktop 18.04, 20.04;
- РЕД ОС 7.1[2], 7.2[2], 7.3 Муром;
- РЕД ОС 8;
- РОСА «КОБАЛЬТ» 7.9 (Рабочая станция, Сервер);
- ROSA Enterprise Linux Desktop/Server 7.3[2];
- CentOS 7[2].

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

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

Директория «/usr» не должна быть на отдельном от корневого каталога «/» разделе ФС (это касается всех дистрибутивов).

Минимальная конфигурация ТС определяется требованиями к соответствующей ОС.

Для размещения файлов **СЗИ НСД** требуется 9 Гб пространства на корневом каталоге жесткого диска:

- в каталоге «/boot» (или «boot/efi») должно быть не менее 300 Мб свободного пространства;
- в каталоге «/dllx» должно быть не менее 530 Мб свободного пространства;
- в каталоге «/dllibckp» должно быть не менее 374 Мб свободного пространства;
- в каталоге «/lib/modules» должно быть не менее 4,2 Гб свободного пространства;
- в каталоге «/tmp» должно быть не менее 3 Гб свободного пространства.

СЗИ НСД успешно устанавливается на АРМы как с UEFI/GPT, так и с BIOS/MBR на автоматически размеченный жесткий диск (разметка жесткого диска по умолчанию при установке ОС). При условии, что для всех каталогов есть необходимое свободное место.

Минимальный объем оперативной памяти, занимаемый компонентами **СЗИ НСД**, составляет 500 Мб. При высокой интенсивности файловых операций потребление может доходить до 3 Гб.

[1] Модуль «Персональный межсетевой экран» может использоваться на операционных системах семейства Linux с ядром версии 5.6 и выше. Для использования модуля «Персональный межсетевой экран» на операционных системах семейства Linux с ядром версии ниже 5.6 необходимо использовать версию изделия 3.31.58.

[2] Для защиты ТС, работающих под управлением ОС CentOS 7, РЕД ОС 7.1 и 7.2, ROSA Enterprise Linux Desktop/Server 7.3, необходимо использовать версию изделия 3.34.44 совместно с локальными репозиториями, предоставляемыми предприятием-изготовителем.

Для обеспечения интеграции с доменом[3], изделие поддерживает работу со следующими компонентами:

- SSSD 2.6.3 и старше;
- Winbind 4.13.17 и старше;
- Kerberos 5 и старше;
- OpenLDAP 2.6.1 и старше;
- Samba 4 и старше;
- FreeIPA 3 и старше.

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.

К основным принципам безопасности работы **СЗИ НСД** относятся:

1) Выполнение ограничений по эксплуатации **СЗИ НСД**, перечисленных в п.3.3 документа ПФНА.501410.002 ФО Формуляр.
2) Осуществление работы **СЗИ НСД** строго в соответствии с эксплуатационной документацией.

[3] Microsoft Active Directory — служба каталогов корпорации Microsoft для операционных систем семейства Windows Server;

FreeIPA — открытый проект для создания централизованной системы по управлению идентификацией пользователей, задания политик доступа и аудита для сетей на базе Linux и Unix;

Samba — программное обеспечение для реализации файлового сервера. Устанавливается на Windows, Linux/FreeBSD.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ СИСТЕМЫ ЗАЩИТЫ

2.1 Параметры (настройки) безопасности средства, доступные пользователю

Доступ к управлению и права для работы аудитора и пользователя в **СЗИ НСД** назначаются администратором **СЗИ НСД** через вкладку «*Учетные записи*» — в панели действия «**Свойства**» — «**Общие**». Добавляя пользователя или аудитора в определенную группу, администратор задает разрешенные действия для них в **СЗИ НСД** (Рисунок 1).

Безопасность значений доступных параметров интерфейсов для всех ролей пользователя обусловлены множеством детерминированных значений для каждого параметра, покрывающем все возможные значения, а также валидностью данного множества в контексте безопасности.

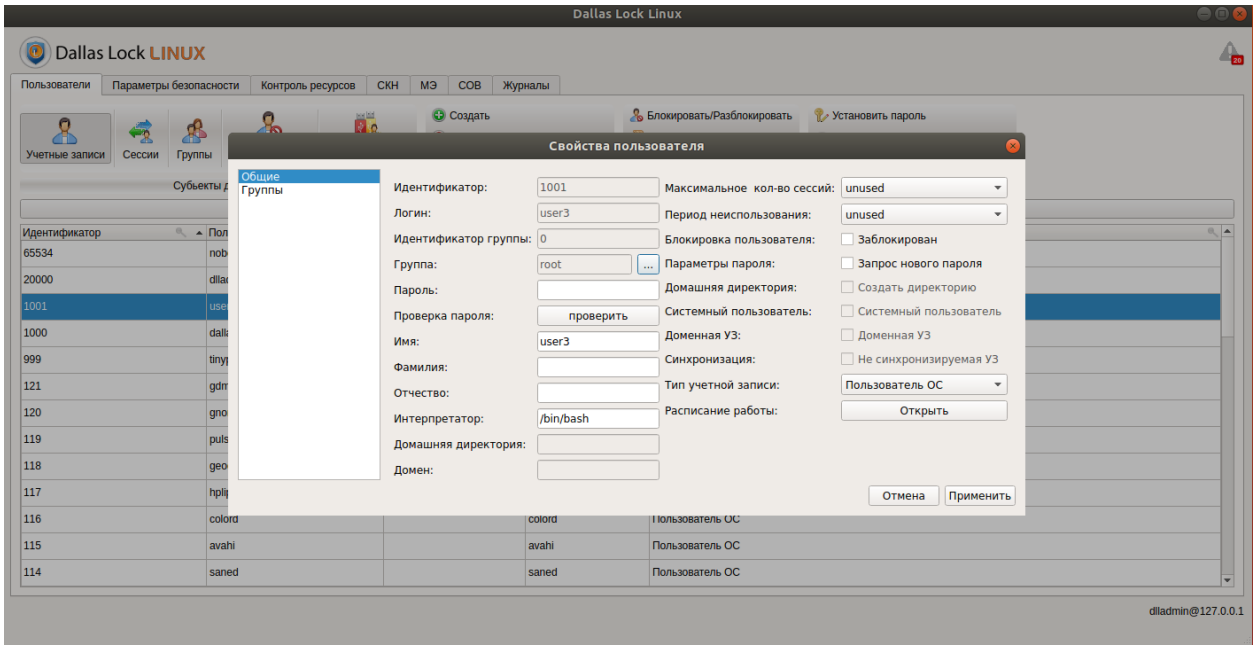

Рисунок 1. Свойства пользователя

Параметры безопасности доступные пользователю:

- вход в систему и смена пароля в соответствии с правилами, если разрешено администратором.

Исходя из параметров безопасности, доступных пользователям, выделяют такие события безопасности, как:

- вход в систему (события аутентификации).

Следует уточнить у администратора какие параметры безопасности доступны для аудитора.

Подробное описание параметров безопасности для пользователей содержится в документе «Руководство по эксплуатации» ПФНА.501410.002 РЭ.

2.2 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),

Атрибут	Основные
	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 подчеркивания, 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 0 до 14 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

2.3 Перечень ролей пользователей

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

- возможность просмотра назначений ролей;
- просмотр списка учетных записей и групп, а также просмотр свойств учетных записей и групп;
- просмотр политик безопасности;
- просмотр прав пользователей и их назначений;
- просмотр списка зарегистрированных устройств, назначенных на них прав доступа;
- возможность сбора и просмотра журналов, настройки параметров фильтра журналов;
- просмотр номера лицензии и ключа технической поддержки;
- просмотр настроек **МЭ**, правил **МЭ**, правил исключений, профилей и соединений;
- запуск автоматического тестирования основных функциональных возможностей;
- просмотр настроек централизованного управления.

Роль «*Пользователь*» не имеет полномочий на администрирование **СЗИ НСД**.

Следует уточнить у администратора какими правами обладает аудитор в системе.

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.

Перечень интерфейсов, доступных для ролей аудитора, определяется администратором, их описание приведено в ПФНА.501410.002 ПФС и в эксплуатационной документации **СЗИ НСД**.

2.4 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.

2.4.1 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;
- Ubuntu: https://wiki.ubuntu.com;
- Astra Linux: https://astralinux.ru/information/library;
- Альт Рабочая Станция, Альт Сервер: https://docs.altlinux.org/ru-RU/index.html;
- РЕД ОС: https://redos.red-soft.ru/documentation/;
- ROSA Enterprise Linux: https://www.rosalinux.ru/docs/.

2.5 Вход в защищенную ОС

2.5.1 Вход с использованием консоли

При входе в ОС без использования графической оболочки ОС, если пользователю назначен аппаратный идентификатор, необходимо его предъявить. Затем, в зависимости от хранимой на идентификаторе информации, по запросу ОС нужно будет ввести:

- логин и пароль в открытой памяти идентификатора — открытая авторизация: если аппаратный идентификатор ассоциирован с пользователем, то произойдет автоматический вход в систему;
- логин и пароль в закрытой памяти идентификатора — закрытая авторизация: если аппаратный идентификатор ассоциирован с пользователем, то для авторизации дополнительно потребуется ввести ПИН;
- только имя пользователя: если аппаратный идентификатор ассоциирован с пользователем, то для авторизации потребуется ввести пароль;
- пустой аппаратный идентификатор: если аппаратный идентификатор ассоциирован с пользователем, то для авторизации потребуется ввести логин, пароль.

Если ни одному считывателю (USB-порту или считывателю Touch Memory) не предъявлен аппаратный идентификатор, то произойдет приглашение для ввода логина.

Если с данным пользователем не ассоциирован аппаратный идентификатор, то появится соответствующее сообщение, и аутентификация будет прекращена.

Если аппаратный идентификатор ассоциирован с пользователем, но он не обнаружен ни одним считывателем, то появится сообщение, требующее предъявить аппаратный идентификатор. Если он предъявлен, то произойдет авторизация в соответствии с одним из типов, отмеченных выше. Если по истечении некоторого периода ожидания аппаратный идентификатор не предъявлен, то авторизация прекращается.

Следует обратить внимание, что в случае входа в ОС без использования графической оболочки, при вводе пароля символы пароля отображаться на экране не будут, также не будут отображаться звездочки или иные символы.

После успешной авторизации отобразится строка приглашения к вводу команд (Рисунок 2).

Рисунок 2. Строка приглашения к вводу команд

Более подробная информация представлена в документе ПФНА.501410.002 РЭ «Руководство по эксплуатации».

2.6 Вход с использованием графической оболочки ОС GNOME

Для осуществления входа необходимо выбрать или ввести логин пользователя (Рисунок 3).

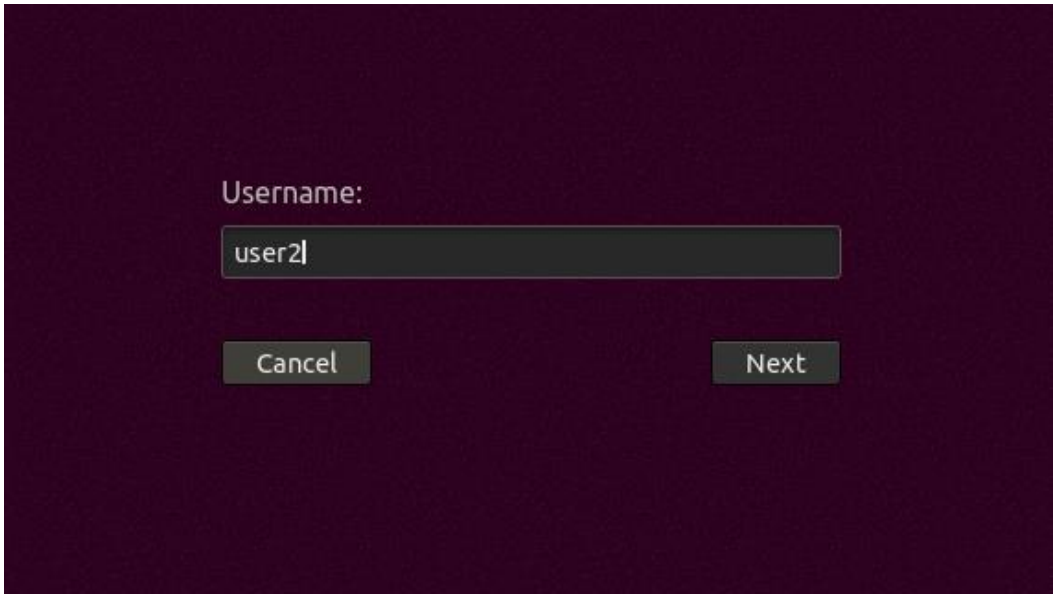

Рисунок 3. GNOME. Выбор пользователя

Если пользователю не назначен аппаратный идентификатор, необходимо ввести пароль и нажать кнопку «**Войти**» (Рисунок 4).

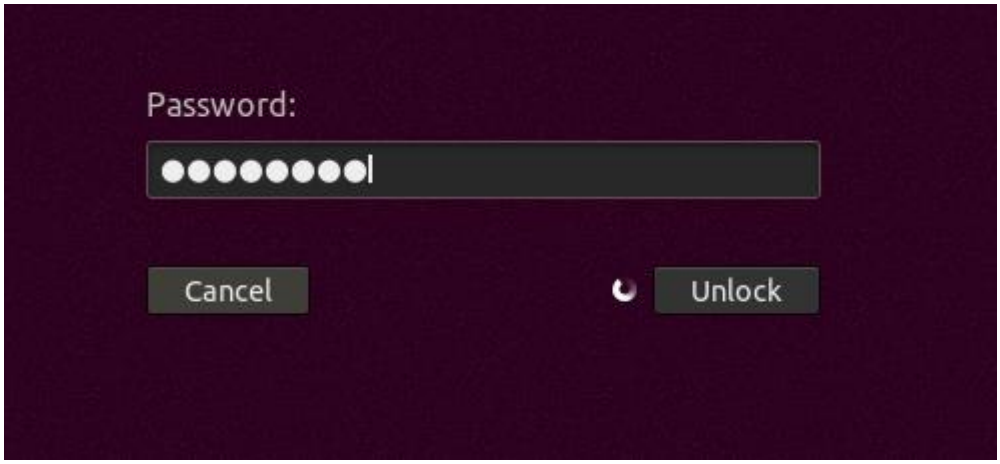

Рисунок 4. GNOME. Ввод пароля

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

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.
Если в идентификаторе хранится информация только о логине учетной записи, то пользователю необходимо ввести пароль учетной записи (Рисунок 4).
Если в идентификаторе не хранится информация об учетной записи, то пользователю необходимо ввести логин и пароль учетной записи.

2.7 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 2) будет отображаться запрос на вход

по аппаратному идентификатору.

Также поддерживается завершение сеанса работы с использованием графической оболочки ОС.

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

2.8 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 2) будет отображаться запрос на вход по аппаратному идентификатору.

Также поддерживается смена пользователя с использованием графической оболочки ОС.

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

2.9 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 5).

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

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

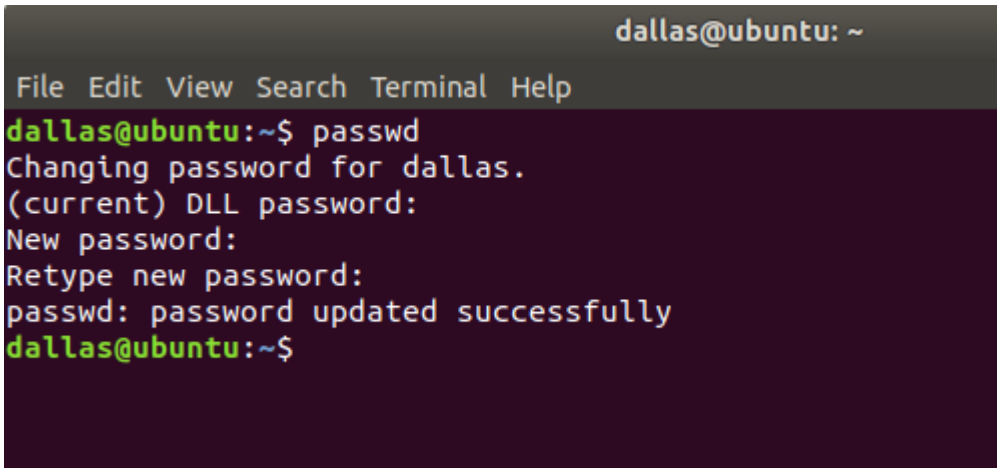

Рисунок 5. Смена пароля

Также поддерживается смена пароля с использованием графической оболочки ОС.

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

2.10 Блокировка ТС

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

Для осуществления блокировки ТС необходимо ввести команду *vlock* (Рисунок 6).

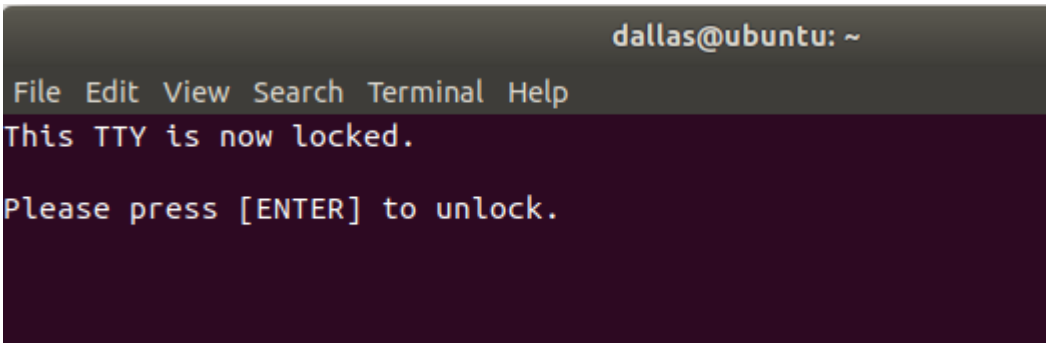

Рисунок 6. Блокировка защищенного ТС

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 7).

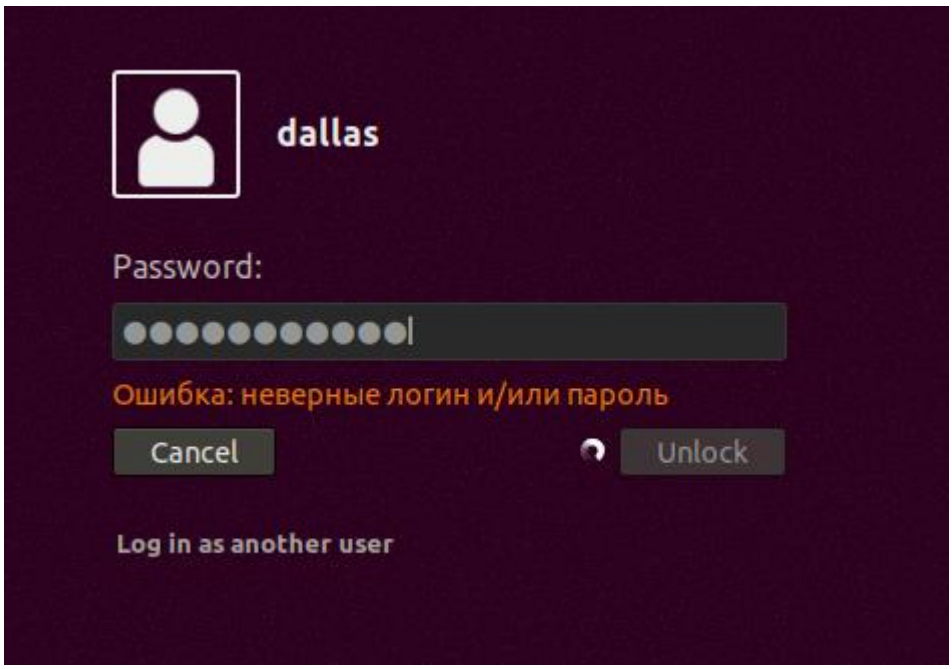

Рисунок 7. GNOME. Сообщение об ошибке

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

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

4 ИНТЕРФЕЙСЫ, ДОСТУПНЫЕ ПОЛЬЗОВАТЕЛЯМ

Для аудитора и пользователя доступны свои параметры интерфейса.

Для аудитора разрешены действия, которые предоставил администратор безопасности. Например, если администратор запретил аудитору создавать и редактировать пользователей, то эти кнопки в оболочке или команды в консоли будут недоступны (Рисунок 8).

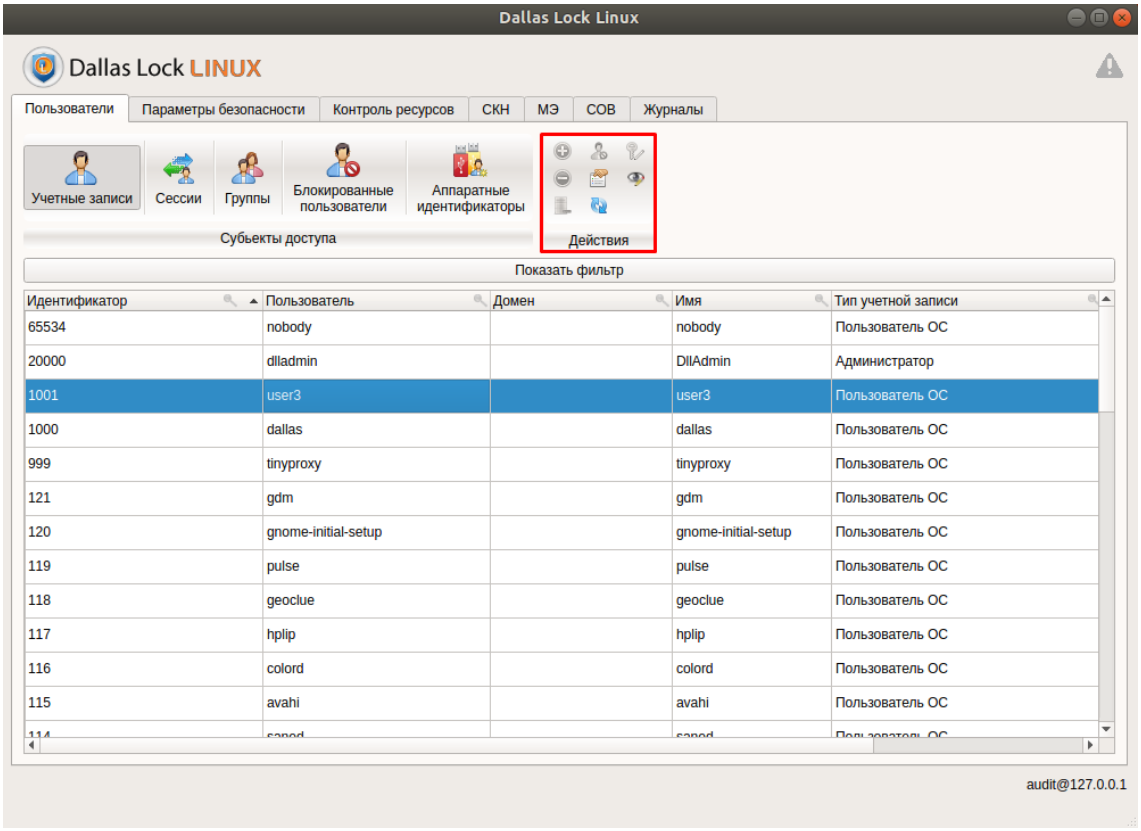

Рисунок 8. Окно «Пользователи» для аудитора

Для обычного пользователя при входе в **СЗИ НСД** будет выводиться ошибка о том, что у пользователя недостаточно прав для входа в систему (Рисунок 9).

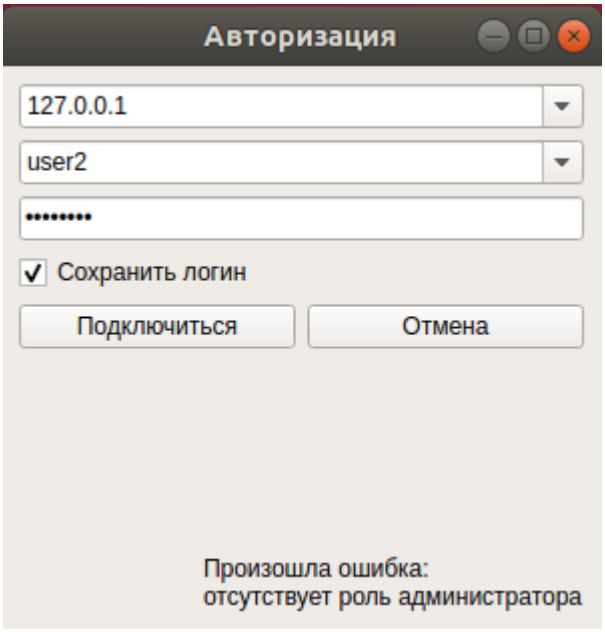

Рисунок 9. Ошибка при входе в СЗИ НСД пользователя