Специальное программное обеспечение SR
для программно-технического комплекса «Модуль системы защиты управления телекоммуникационным оборудованием»
(Модели: SR2-WIC, SR2-SPA, SR2-SIC, SR2-S3KX, SR2-STK, SR2-CON)
(версия 1.3)

ОПИСАНИЕ
СПЕЦИАЛЬНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Москва 2016

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Специальное программное обеспечение SR (СПО «SR»)- предназначено для организации контролируемого управления телекоммуникационным оборудованием (далее – ТКО).

В качестве ТКО рассматриваются маршрутизаторы и коммутаторы, имеющие свободные слоты расширения. Одним из примеров реализации является установка СПО «SR» на специально разработанные модули в слоты расширения стандарта Cisco Wan Interface Card (WIC, VWIC, HWIC, EHWIC).

Функции защиты управления, реализованные в СПО «SR», позволяют обеспечить:

- разграничение прав доступа;
- контроль доступа к ТКО;
- доверенную загрузку операционной системы ТКО.

Под разграничением прав доступа понимается:

- аутентификация;
- определение ролей (субъектов доступа) и назначение их прав по отношению к объектам доступа.

Контроль доступа к ТКО включает в себя:

- контроль и запись сессий управления ТКО в реальном времени;
- контроль физических подключений к интерфейсу управления ТКО (включая консольный);
- контроль выполнения политик управления ТКО и принятие решений в соответствии с заданными правилами в случае нарушений политик.

Доверенная загрузка операционной системы ТКО обеспечивается реализацией в СПО «SR» механизмов средства доверенной загрузки уровня платы расширения.

Настоящее описание программного обеспечения предназначено для ознакомления пользователей с правилами и особенностями работы с СПО «SR».

2. ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ СПО «SR»

2.1. Разграничение прав доступа

2.1.1. Ролевая модель доступа

В СПО «SR» реализована ролевая модель доступа. Пользователь – человек, программное обеспечение и т.д. (субъект доступа), который получает доступ к СПО «SR» или ТКО (объекты доступа), может быть сопоставлен с одной или несколькими ролями, имеющими различные полномочия.

В модели доступа СПО «SR» реализованы следующие роли:

- Администратор СПО «SR» – уполномоченный пользователь, ответственный за конфигурирование СПО «SR», управления учетными записями пользователей и правами доступа.
- Администратор аудита – уполномоченный пользователь, имеющий доступ к файлам и записям журнала аудита с возможностью их просмотра, поиска, сортировки, упорядочения данных аудита, а также изменения, удаления, копирования.
- Функциональный контролер – уполномоченный пользователь, имеющий доступ к консоли контроля над функционированием СПО «SR».
- Оператор ТКО – пользователь, имеющий доступ к функциям настройки ТКО.

Роли Администратора СПО, Администратора аудита, Функционального контролера – роли Администратора, обладающего набором полномочий (привилегий) по управлению параметрами и данными СПО «SR», влияющими на выполнение функции безопасности.

Обобщенные сведения о ролях и полномочиях представлены в таблице:

Роль	Полномочия по отношению к ТКО	Полномочия по отношению к СПО «SR»
Администратор СПО	Активирует доверенную загрузку ТКО.	Управляет работой СПО «SR». Управляет функциями безопасности: - правилами подключения к ТКО и СПО

Роль	Полномочия по отношению к ТКО	Полномочия по отношению к СПО «SR»
	Деактивирует доверенную загрузку ТКО.	«SR»; - механизмами аутентификации; - политиками управления ТКО; - режимами тестирования. Управляет учетными записями (создание, модификация (изменение), блокирование, разблокирование)
Администратор аудита	-	Осуществляет операции по управлению функциями и данными аудита: - назначение и изменение параметров журнала аудита; - выполнение операций с файлами журнала аудита (перемещение, копирование, удаление); - выполнение операций с записями журнала аудита (просмотр, поиск, сортировка, упорядочение). Модифицирует атрибуты своей учётной записи (в части изменения пароля).
Функциональный контролер	-	Осуществляет контроль за работой СПО «SR» (включая функции безопасности). Модифицирует атрибуты своей учётной записи (в части изменения пароля).
Оператор ТКО	Выполняет разрешенные операции по управлению и конфигурированию ТКО.	Модифицирует атрибуты своей учётной записи (в части изменения пароля).

Полномочия по управлению учетными записями пользователей, за исключением операций по модификации, делегированы Администратору СПО.

Модификация учетной записи в части изменения пароля пользователя для прохождения однофакторной аутентификации разрешена всем пользователям. Данная функция управления позволяет исключить

возможность управления ТКО пользователям, не являющимися Операторами ТКО.

В СПО «SR» блокирование учетной записи пользователя производится:

- автоматически (в случае превышения максимального количества неуспешных попыток аутентификации – на 15 минут, через установленный период времени неиспользования, при превышении установленного периода действия пароля пользователя – 90 дней);
- в результате действия Администратора СПО по блокированию учетной записи.

Каждому событию блокирования учетной записи пользователя присваивается идентификатор события блокирования, что позволяет в дальнейшем проводить анализ инцидентов безопасности, а также не допускать повторного использования идентификатора пользователя раньше установленного периода.

При управлении учетными записями исключены операции по удалению учетных записей, что связано с реализацией возможности проведения анализа событий, в том числе связанных с нарушением безопасности, ведения статистики действий пользователей, даже в случае смены пользователей.

2.1.2. Аутентификация

Субъектами аутентификации являются пользователи, которым в СПО «SR» создана учетная запись.

Для поддержки аутентификации пользователей СПО «SR» предоставляет возможность сочетания механизмов аутентификации. Администратором СПО могут быть активированы механизмы однофакторной либо двухфакторной аутентификации, а также их сочетание в зависимости от принятой в ИС политики безопасности.

Аутентификационными данными при однофакторной аутентификации являются учетная запись (логин) и пароль.

Двухфакторная аутентификация осуществляется с помощью программного обеспечения Free RADIUS и LinOTP, установленных на

отдельном сервере (серверах). Для использования функционала двухфакторной аутентификации необходимо предварительно активировать его через интерфейс Администратора СПО. При выполнении процедуры двухфакторной аутентификации пользователь выполняет подключение к СПО «SR» под своей учетной записью. Аутентификационными данными являются логин и связка, состоящая из постоянной части – пин-кода и одноразового пароля, генерируемого ПО, установленным на АРМ пользователя.

2.1.3. Ограничение доступа

Механизмы управления подключениями к СПО «SR» и ТКО позволяют Администратору СПО ограничить доступ пользователей к консольному порту управления (тем самым, ограничив возможные действия пользователей на объектах доступа), а также устанавливать и изменять перечень рабочих мест, с которых разрешено подключение к объектам доступа для управления.

В СПО «SR» реализованы механизмы ограничения на число параллельных (одновременных) сеансов (сессий), основываясь на идентификаторах пользователей и (или) принадлежности к определенной роли. Разрешено не более одной сессии.

2.2.Контроль доступа

2.2.1. Контроль действий Операторов ТКО

СПО «SR» предоставляет Операторам ТКО единый шлюз для доступа к ТКО с возможностью фильтрации команд управления и конфигурации ТКО.

Команды управления и конфигурации ТКО рассматриваются СПО «SR» в качестве операций управляемого субъекта (Оператора ТКО) на управляемом объекте (ТКО). Для этих операций назначаются правила (политики управления) на основе политик безопасности, принятых в ИС. Правила основаны на атрибутах безопасности, которые явно разрешают или запрещают выполнение команды Оператора ТКО на управляемом ТКО – политики черных/белых списков.

Если Оператор ТКО ассоциирован с чёрным списком, ему разрешены все команды управления и конфигурирования, за исключением тех, которые указаны в списке.

Если Оператор ТКО ассоциирован с белым списком, ему запрещены все команды управления и конфигурирования, за исключением тех, которые указаны в списке.

2.2.2. Контроль целостности ПО и параметров

При поставке конечному пользователю СПО «SR» содержит файл образа операционной системы ТКО, прошедшей процесс верификации (сертифицирована регулятором или прошла иную проверку, которая может рассматриваться как доверенная). При этом для указанного файла разработчиком (производителем) СПО «SR» рассчитано и зафиксировано значение контрольной суммы (эталонное значение). В процессе функционирования СПО «SR», программой самотестирования производится расчет значения контрольной суммы файла образа ОС ТКО, хранящегося в СПО «SR», и сравнение этого значения с эталонным значением. Проверка наличия ошибок контрольных сумм может также осуществляться по запросу уполномоченного пользователя.

В случае, если контрольные суммы не совпадают, производится оповещение уполномоченных лиц об ошибке целостности файла образа ОС ТКО.

При изменении версий ОС ТКО производится перезапись в СПО «SR» файла образа ОС ТКО (замена на актуальный). При этом актуальный файл образа поставляется с указанием зафиксированного значения контрольной суммы, которое записывается в СПО «SR» и принимается в качестве эталонного.

Также в процессе функционирования СПО «SR» производятся проверки целостности программного обеспечения СПО «SR» и целостности данных СПО «SR». Проверки могут осуществляться с заданной периодичностью при выполнении программ самопроверки, а также по запросу уполномоченного пользователя. При проверке ПО СПО «SR» проверяется целостность заданного множества исполняемых файлов. В ходе проверки целостности данных СПО «SR» проверяется целостность

файла-паспорта СПО «SR», в котором записаны актуальные версии компонентов СПО «SR». Атрибутами контролируемых файлов являются значения контрольных сумм.

При обнаружении факта несовпадения значений контрольных сумм проверяемых файлов с эталонными значениями производится оповещение уполномоченных лиц об ошибке целостности с указанием файла, целостность которой нарушена. Механизмами СПО «SR» будет принята попытка восстановить указанные файлы из специальной папки СПО «SR». В случае, если это будет невозможно, происходит блокировка доступа к СПО «SR» и ТКО пользователей, за исключением Администратора СПО.

В СПО «SR» не предусмотрена возможность действий уполномоченных пользователей по восстановлению исполняемых файлов ПО СПО «SR», файла образа ОС ТКО, целостность которых нарушена.

2.2.3. Контроль физического подключения кабелей управления

Контроль физического подключения кабелей управления производится посредством выполнения программ самотестирования (см. п.2.5).

2.3.Доверенная загрузка

Доверенная загрузка является основным механизмом безопасности реализуемым СПО «SR». Механизм доверенной загрузки реализуется с использованием штатного механизма удаленной загрузки ТКО. Данный механизм предполагает загрузку ТКО с внешнего TFTP-сервера. В качестве такого TFTP-сервера выступает СПО «SR». Образ операционной системы ТКО находится на microSD-карте, установленной в СПО «SR». В качестве образа ОС ТКО рекомендуется использовать либо сертифицированную по требованиям регуляторов либо верифицированную версию ОС ТКО, которая в таком случае является доверенной. Размещение доверенной ОС ТКО на microSD-карту должно осуществляться по доверенному каналу. Одним из вариантов является запись образа ОС на аттестованном рабочем месте, другим – доставка по доверенному каналу с использованием утилит удаленной записи файлов. После установки microSD-карты в ОО осуществляется подсчет

контрольной суммы и сравнение полученного значения с эталонным, которое вводится при настройке TFTP-сервера. Механизм внесения и изменения эталонного значения контрольной суммы доверенной ОС ТКО описан в эксплуатационных документах ОО. В ОО предусмотрено использование одной доверенной ОС.

Доверенная загрузка может быть активирована и деактивирована Администратором СПО. В процессе активации осуществляется необходимая настройка ТКО, проверяется наличие эталонного значения контрольной суммы файла образа ОС ТКО, наличие собственно доверенной ОС ТКО на microSD-карте, установка необходимых значений параметров СПО «SR». Активация невозможна, если одно из перечисленных действий не закончилось успешно. В процессе деактивации осуществляется сброс настроек ТКО, позволяющих осуществлять удаленную загрузку ТКО.

Необходимым условием доверенной загрузки является ее активация и наступление одного из условий: включение ТКО, перезагрузка уже включенного ТКО по команде оператора ТКО. Процесс доверенной загрузки осуществляется в следующей последовательности:

1) после перезагрузки или включения питания ТКО переходит с специальный режим, когда ТКО ожидает авторизации оператора ТКО;
2) оператор ТКО авторизуется на СПО «SR»;
3) оператор ТКО вводит команду на загрузку ТКО;
4) ТКО забирает доверенный образ ОС ТКО с TFTP-сервера в оперативную память ТКО;
5) ТКО грузится с доверенного образа ОС ТКО, помещенного в оперативную память ТКО.

СПО «SR» осуществляет блокирование загрузки ОС:

- при выявлении попыток загрузки нештатной операционной системы;
- при превышении числа неудачных попыток аутентификации пользователя;
- при нарушении целостности СПО «SR»;
- при нарушении целостности загружаемой программной среды;

– блокирование загрузки ОС при критичных типах сбоев и ошибок.

2.4. Аудит

СПО «SR» располагает надлежащими механизмами регистрации о любых событиях, в том числе, относящихся к возможным нарушениям безопасности.

В СПО «SR» осуществляется генерация записей аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на неопределенном уровне аудита:

- успешная регистрация пользователя;
- неуспешная регистрация пользователя;
- смена параметров учетной записи пользователя (модификация);
- блокировка учетной записи пользователя;
- разблокировка учетной записи пользователя;
- успешная аутентификация пользователя;
- неуспешная аутентификация пользователя;
- окончание сессии пользователя;
- разрыв сессии пользователя по тайм-ауту;
- нарушение физической целостности СПО «SR»;
- нарушение программной целостности СПО «SR»;
- нарушение целостности файла образа ОС ТКО;
- команды Администратора СПО по изменению конфигурации СПО «SR»;
- команды Оператора ТКО по управлению ТКО (включая разрешенные и запрещенные команды);
- разрешение доверенной загрузки ОС ТКО;
- запрет загрузки ОС ТКО;
- выполнение доверенной загрузки ОС ТКО;
- физическое отключение портов управления;
- восстановление физического подключения портов управления;

– запуск программ самотестирования;
– результаты самотестирования.

Записи аудита содержат следующую информацию о событиях (определенные поля могут отсутствовать в зависимости от типа события):

– дата и время события;
– IP-адрес и(или) имя СПО «SR»;
– тип события;
– идентификатор субъекта;
– информационное сообщение (статус физического порта, проверки контрольной суммы);
– команда по управлению ТКО;
– команда по управлению СПО «SR»;
– результат выполнения команды (успешный или неуспешный).

Все события могут быть упорядочены (отсортированы) по типам событий:

– контроль физических портов;
– контроль целостности;
– аутентификация пользователей;
– доверенная загрузка;
– команды управления СПО «SR»;
– команды управления ТКО.

Для аудита событий, являющихся результатом действий идентифицированных пользователей, каждое событие, потенциально подвергаемое аудиту, ассоциируется с идентификатором пользователя, который был инициатором этого события.

Журнал аудита сохраняются в текстовом файле, находящемся в файловой системе СПО «SR» (максимальный размер файла – 100 Мб), а также могут быть перенаправлены на внешний syslog-сервер по протоколу syslog. Доступ в режиме записи к файлу журнала разрешен только учетной записи системного пользователя, которая используется программным обеспечением СПО «SR».

Действия (операции) по управлению данными аудита в СПО «SR» делегированы Администратору аудита.

Администратор аудита может производить следующие действия:

- назначать и изменять параметры журнала аудита (значение максимального размера файла журнала аудита может быть задано в диапазоне в диапазоне от 1 до100 Мб);
- выполнять операции с файлами журнала аудита (перемещение, копирование, удаление);
- выполнять операции с записями журнала аудита (просмотр, поиск, сортировка, упорядочение);
- определять действия, которые необходимо выполнить с данными аудита при сбое или превышении количества записей в журнале аудита;
- осуществлять резервное копирование данных аудита.

Механизмы регистрации предоставляют возможность Администратору аудита выборочного ознакомления с информацией о произошедших событиях, а также возможность выполнить поиск, сортировку, упорядочение данных аудита:

а) по идентификатору субъекта;

б) по заданным периодам (дата и время события);

в) по типу события;

г) по результату события (успешный, неуспешный).

2.5. Самотестирование

Для демонстрации правильного выполнения возложенных на СПО «SR» функций предусмотрен пакет программ самотестирования, которые могут быть запущены:

а) периодически в процессе нормального функционирования;

б) по запросу уполномоченного пользователя.

В процессе самотестирования осуществляется:

- проверка целостности СПО «SR» и целостности данных СПО «SR»;
- проверка целостности файла образа ОС ТКО;
- проверка функционирования microSD-карты в составе ОО;
- проверка физического подключения кабелей управления;

- проверка работоспособности СПО «SR» для роли Администратора СПО;
- проверка работоспособности СПО «SR» для роли Администратора аудита;
- проверка работоспособности СПО «SR» для роли Функционального контролера;
- проверка работоспособности СПО «SR» для роли Оператора ТКО.

Данные самотестирования записываются в журнал аудита в виде текстового файла с указанием параметра проверки и результата проверки по каждому из тестов, предусмотренных программой самопроверки – пройден / не пройден. Также результаты проверки отображаются в интерфейсе консоли уполномоченных пользователей. В случае неуспешной проверки теста, предусмотренного программой самотестирования предусмотрено информирование уполномоченных пользователей посредством отправки сообщения по электронной почте.

Администратором СПО в зависимости от необходимости может быть задана и изменена периодичность запуска программ самотестирования в диапазоне от 1 до 60 минут. Кроме того, запуск программ самотестирования может быть инициирован Администратором СПО с использованием команд запуска. Администратором СПО может быть определен как полный перечень тестов выполняемых в ходе самотестирования, так и выборочно – необходимые тесты, проводимые в ходе самопроверки (например, только контроль целостности ПО СПО «SR», исключая остальные проверки).

2.6. Сигнализация

СПО «SR» располагает надлежащими механизмами предупреждения (сигнализации) уполномоченных лиц о любых событиях, в том числе, относящихся к возможным нарушениям безопасности.

Следующие события рассматриваются в качестве факта нарушения безопасности:

- разрыв консольного или сетевого подключения СПО «SR» и ТКО;
- ошибки контрольных сумм файлов СПО «SR» и файла образа ОС ТКО.

Следующие события рассматриваются в качестве попытки нарушения безопасности:

- блокировка учетной записи пользователя в результате превышения допустимого числа попыток аутентификации;
- ввод Оператором ТКО команды управления (конфигурации), запрещенной в настроенной политике безопасности.

В СПО «SR» предусмотрено оповещение уполномоченных пользователей о событиях, относящимся к нарушениям (попыткам нарушения) безопасности посредством отображения в интерфейсе консоли уполномоченных пользователей и отправки им соответствующих сообщений по электронной почте.

2.7. Управление функционированием СПО «SR»

Управление функционированием СПО «SR» включает в себя следующие этапы:

- создание защищенной сети управления;
- управление параметрами и конфигурация (администрирование) СПО «SR»;
- перезагрузку СПО «SR».

Создание сети управления предусматривает: установку СПО «SR» в ТКО, подключение кабелей сети управления, инициализацию и начальную настройку СПО «SR». Данные действия производятся Администратором СПО.

Администрирование СПО «SR» осуществляется Администратором СПО и Администратором аудита (в части управления параметрами аудита) и может выполняться следующими способами:

- удаленно из защищаемого периметра с помощью интерфейса командной строки по протоколу SSH;
- локально с помощью интерфейса командной строки и терминального подключения.

Перезагрузка СПО «SR» в процессе функционирования предусмотрена в следующих случаях:

- при восстановлении функционирования СПО «SR» после сбоя (ошибок), отказа, аппаратной платформы и ПО СПО «SR»;

- в процессе восстановлении контролируемых исполняемых файлов, целостность которых была нарушена;
- в процессе установки актуальной (доверенной) ОС ТКО из образа;
- после обновления ПО СПО «SR».

Перезагрузка ПО СПО «SR» может проводиться автоматически или по команде Администратора СПО.

3. ПОРЯДОК РАБОТЫ С СПО «SR»

3.1. Работа пользователя с СПО «SR»

3.1.1. Общие положения

Выполнение предусмотренных ролями процедур (действий) разрешено пользователям СПО «SR» с активными учетными записями.

Доступ пользователей к СПО «SR» для управления объектами доступа (ТКО или СПО «SR») возможен только с разрешенных узлов (АРМ) по протоколу SSH.

Работа пользователя производится в рамках открытой сессии после успешного прохождения процедуры идентификации и аутентификации. В случае отсутствия активности со стороны пользователя СПО «SR» сессия разрывается через 15 минут. Для открытия новой сессии требуется повторная идентификация и аутентификация пользователя.

3.1.2. Идентификация и аутентификация

Процедура прохождения идентификации и аутентификации обязательна для всех пользователей СПО «SR».

Для прохождения процедуры идентификации необходимо ввести активную (незаблокированную) учетную запись пользователя СПО «SR» (рис. 3.1.1).

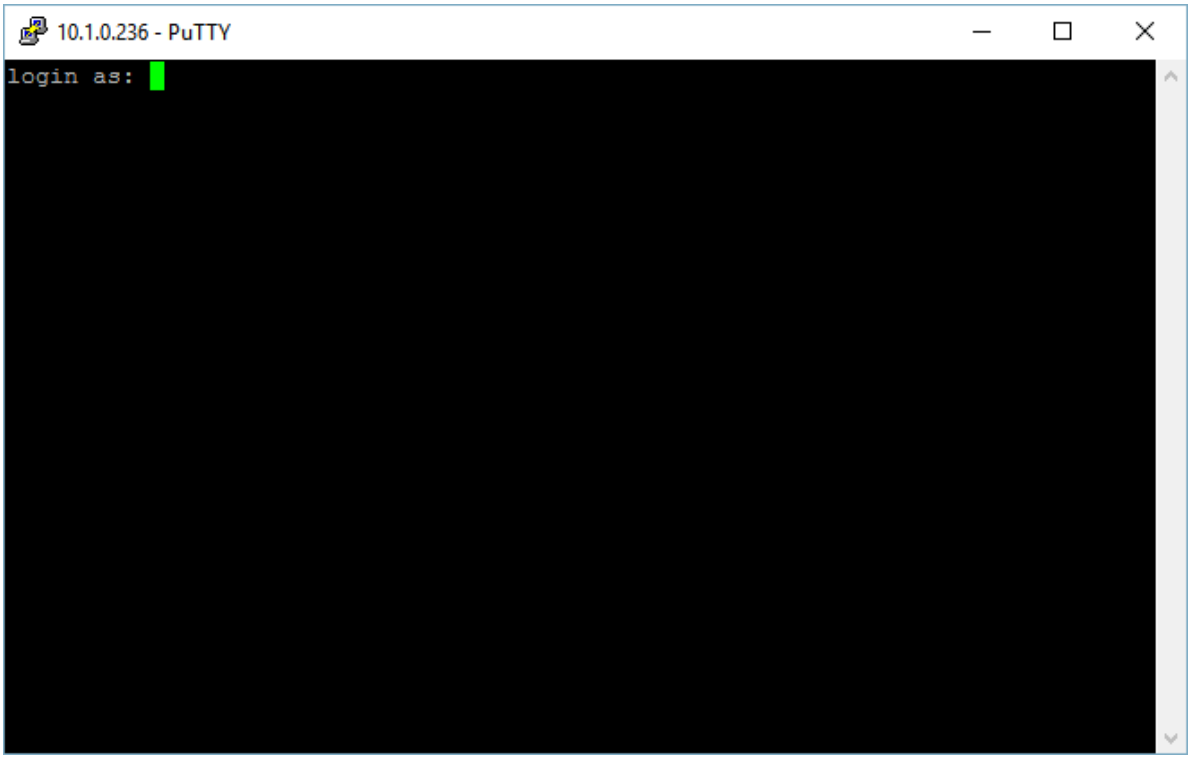

Рис. 3.1.1

После прохождения идентификации будет предложено пройти аутентификацию по паролю (рис. 3.1.2)

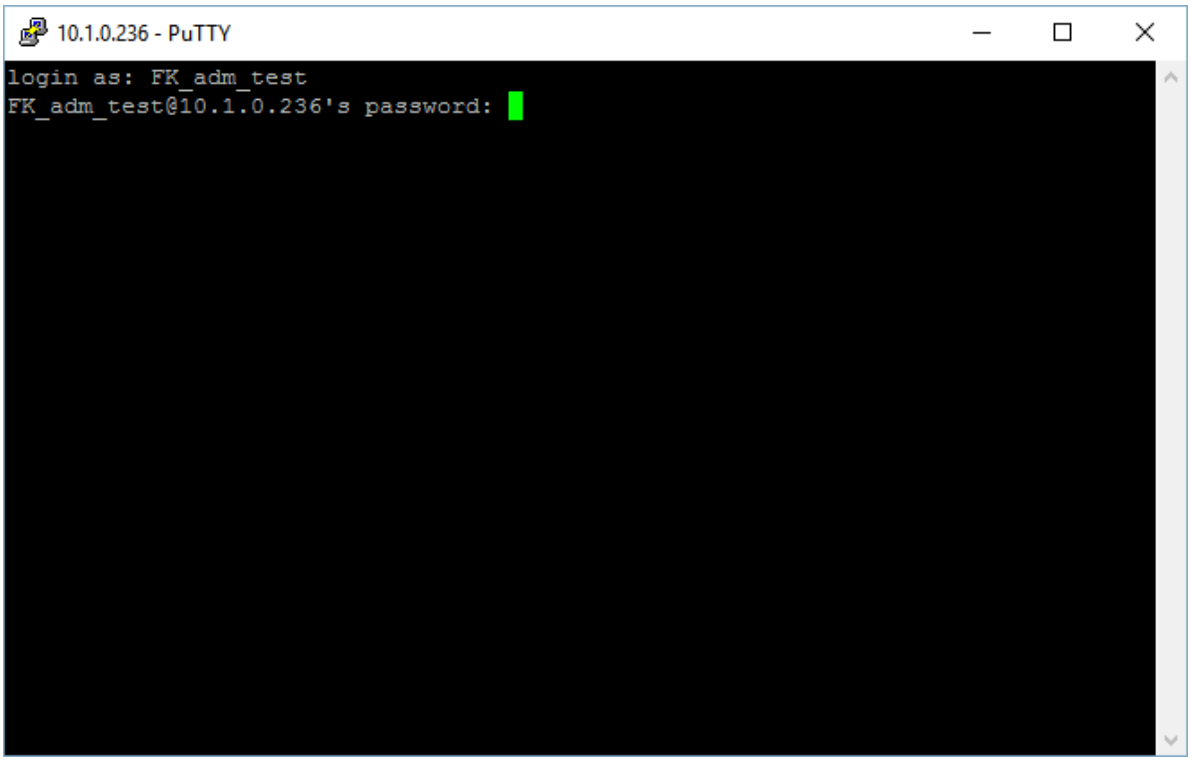

Рис. 3.1.2

В случае успешного прохождения процедур идентификации и аутентификации СПО SR предоставляет доступ к командной строке. На экран выводится сообщение, которое содержит информацию о текущей

версии СПО SR. Кроме того, отображается информация о последнем входе в систему (включая дату, время и интерфейс). Приглашение к вводу команд показано на рис. 3.1.3.

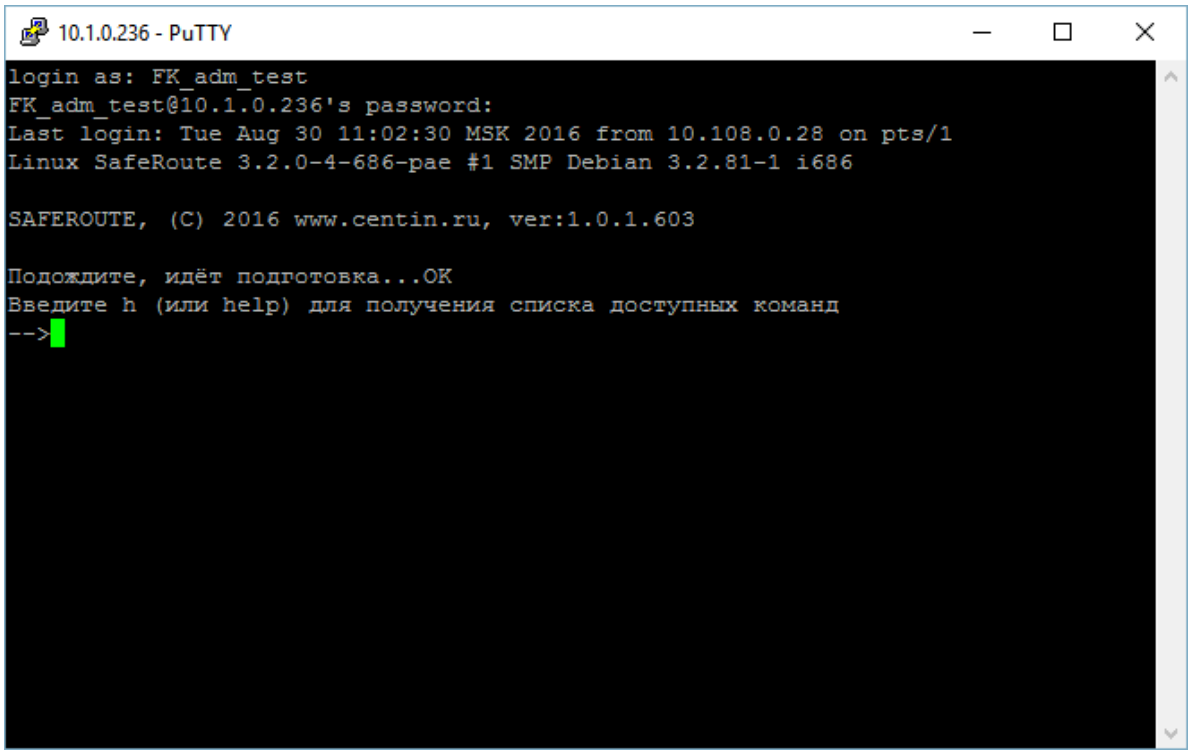

Рис. 3.1.3

В случае если не была пройдена процедура идентификация и/или аутентификации, пользователю будет выдано сообщение об отказе в доступе, не предоставив при этом подробности о том, какая именно процедура не была пройдена. Данный функционал реализован в соответствии с практиками систем Linux в целях затруднения получения несанкционированного доступа к системе.

3.1.3. Работа с командной строкой

В СПО «SR» работа пользователей организуется посредством ввода команд в командной строке.

Реакцией на ввод доступной команды является отображение в интерфейсе консоли пользователя предусмотренной информации (данных) в доступном для восприятия виде.

Для получения перечня доступных команд необходимо в открытой сессии ввести в командной строке h или help. Вывод на экран списка доступных команд показан на рис. 3.1.4:

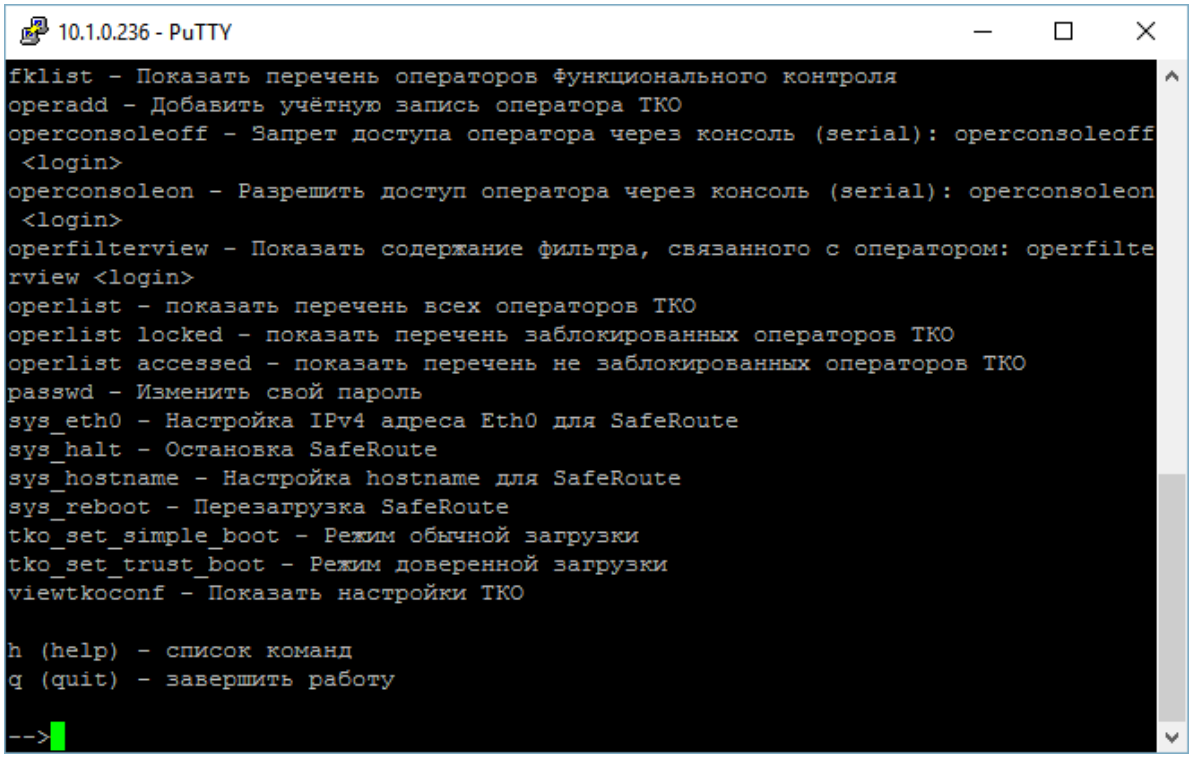

Рис. 3.1.4

Пользователю СПО SR доступна очистка экрана ввода-вывода. Для ее вызова необходимо выполнить команду clear. Результат выполнения работы команды clear показан на рис. 3.1.5:

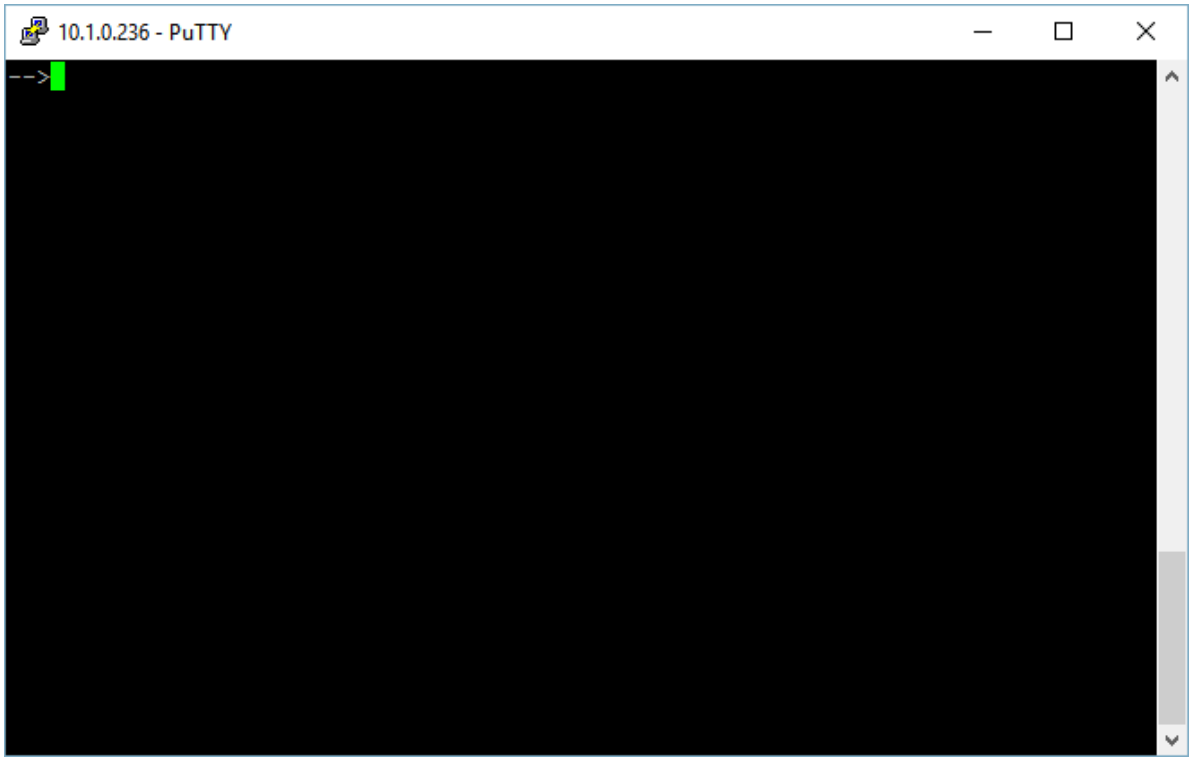

Рис. 3.1.5

3.1.4. Смена пароля

Смена своего пароля доступна любому пользователю СПО «SR». Для смены своего пароля пользователю необходимо выполнить команду passwd, после чего ввести свой текущий (действующий пароль), а затем дважды новый пароль.

Предустановленными настройками СПО SR контролируются длина и сложность пароля, а также ведется история ранее использованных паролей.

Результат успешного выполнения команды смены пароля показан на рис. 3.1.6 – 3.1.8.

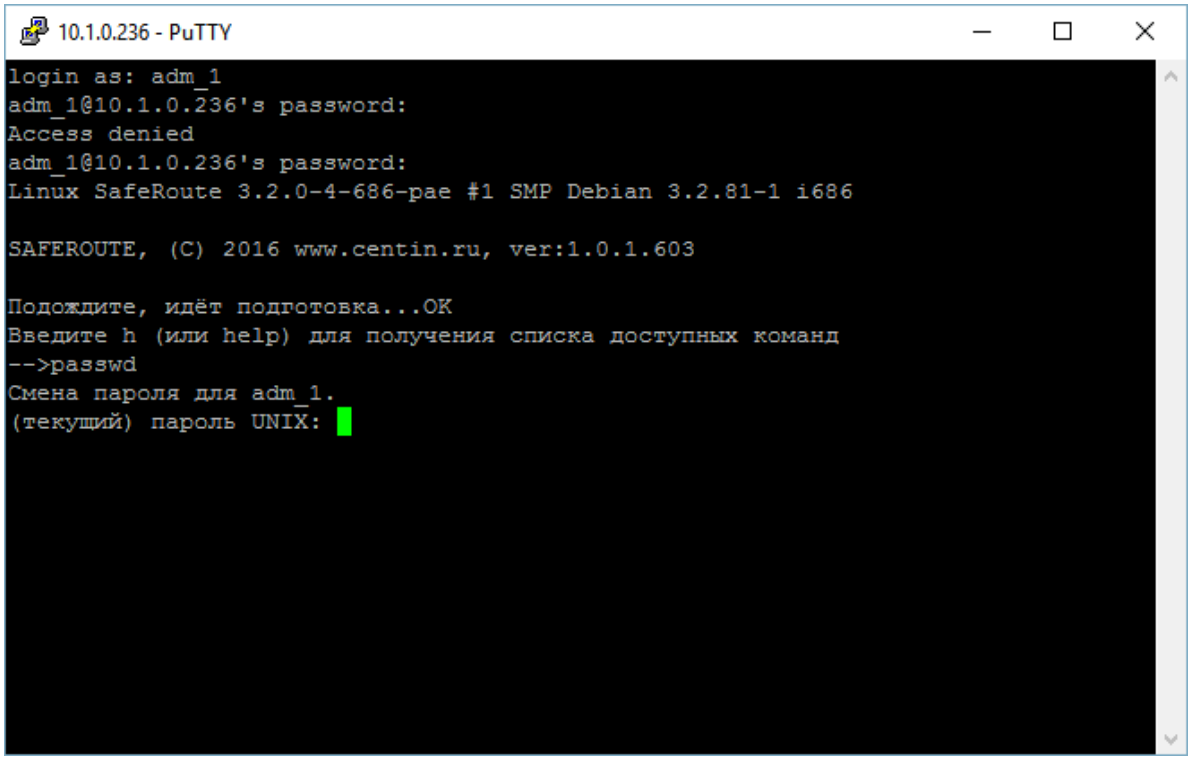

Рис. 3.1.6

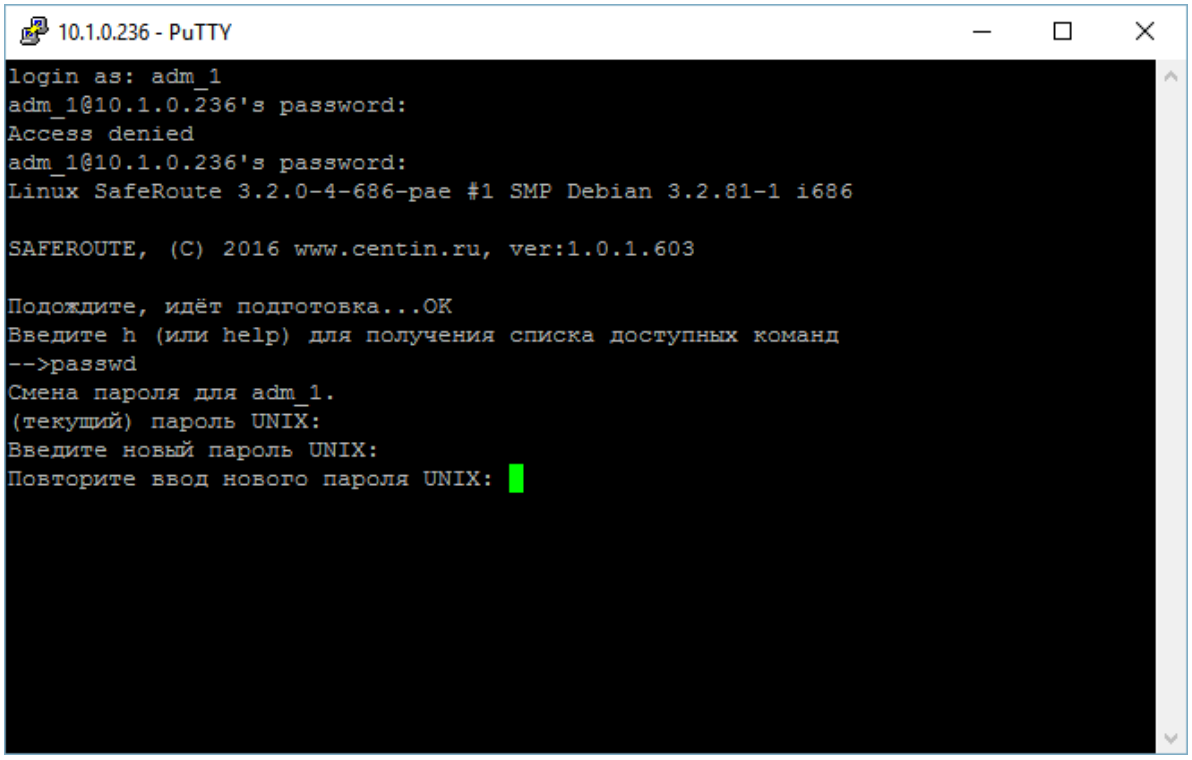

Рис. 3.1.7

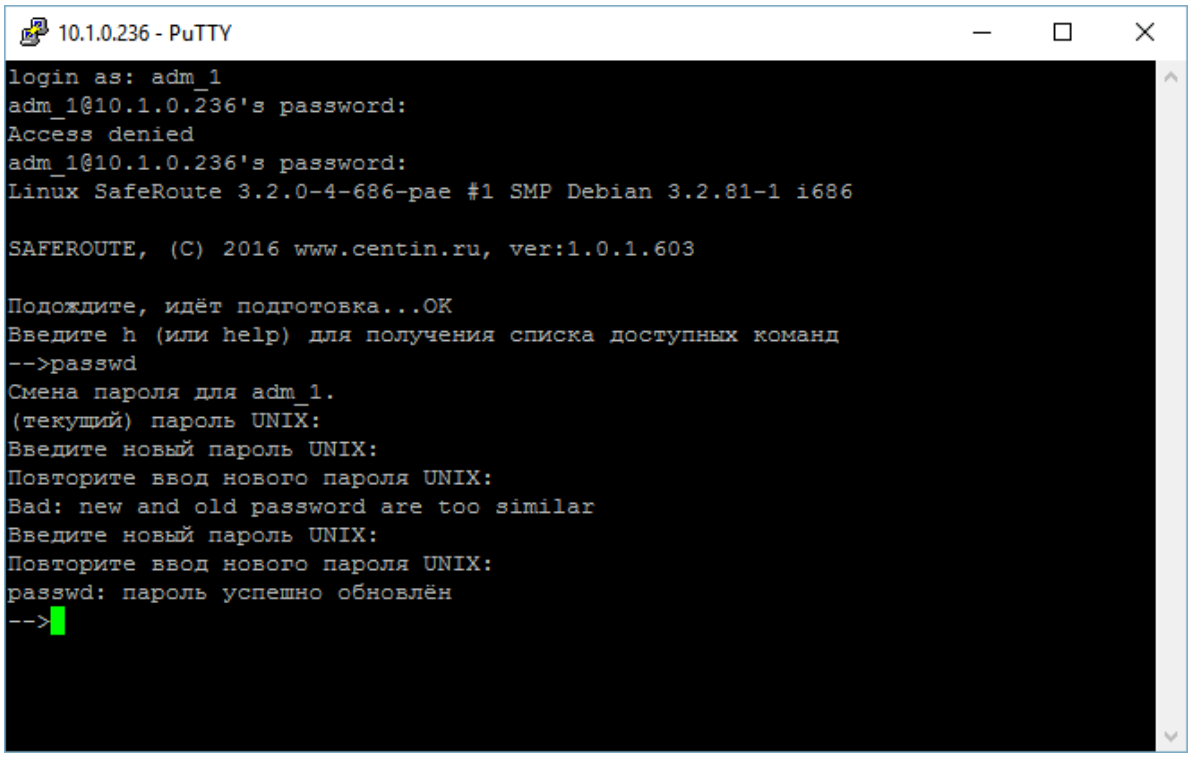

Рис. 3.1.8

3.2. Работа Администратора

3.2.1. Добавление учетной записи администратора СПО

Для добавления учетной записи Администратора СПО необходимо ввести команду addadm. На рис. 3.2.1 – 3.2.4 показан пример добавления администратора СПО с учетной записью adm_1

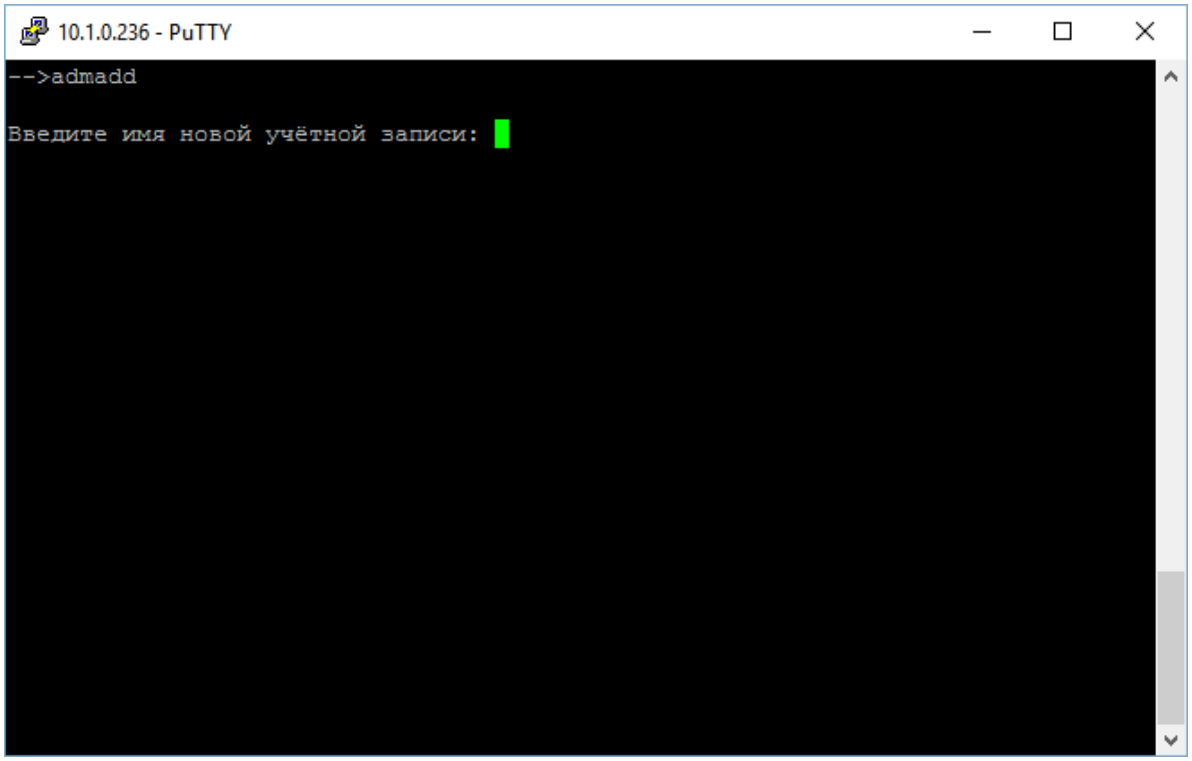

Рис. 3.2.1

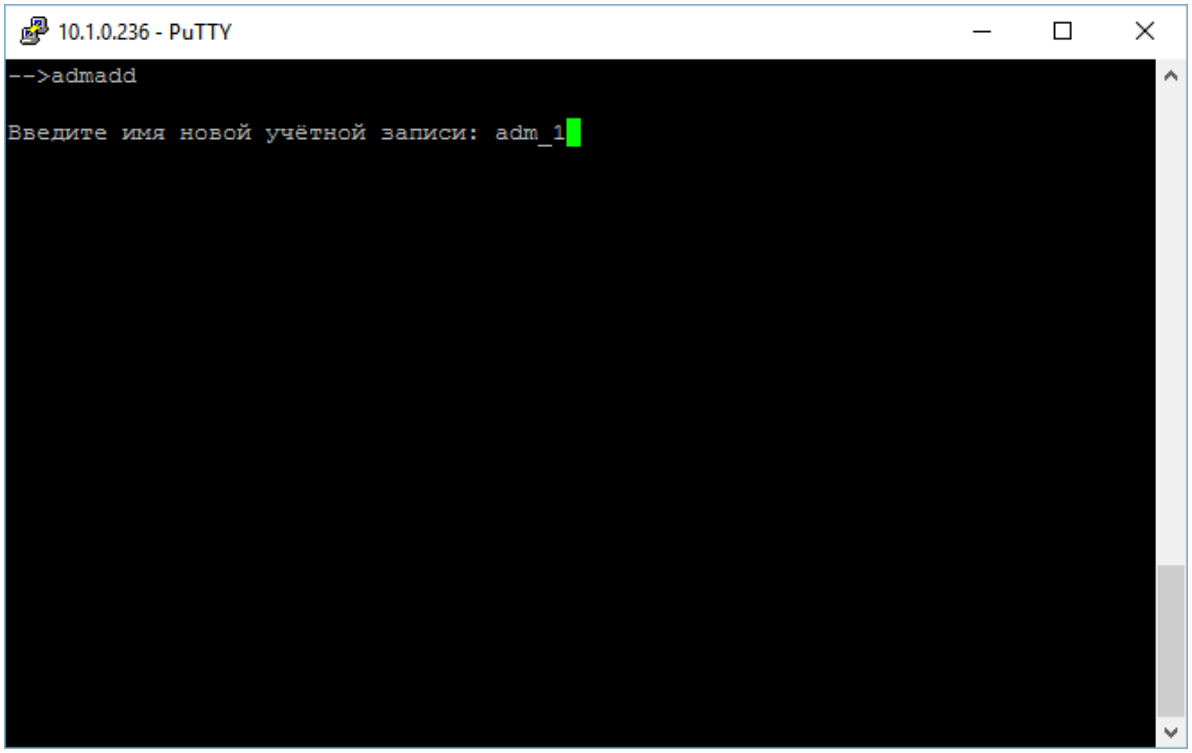

Рис. 3.2.2

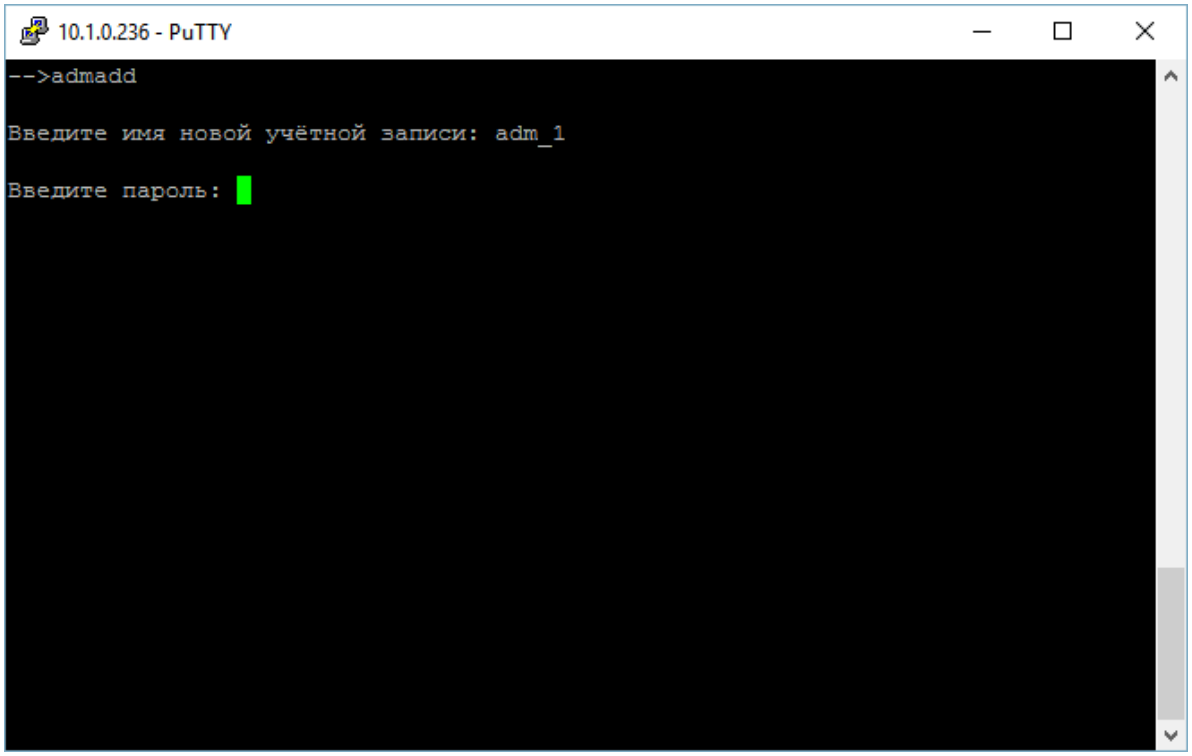

Рис. 3.2.3

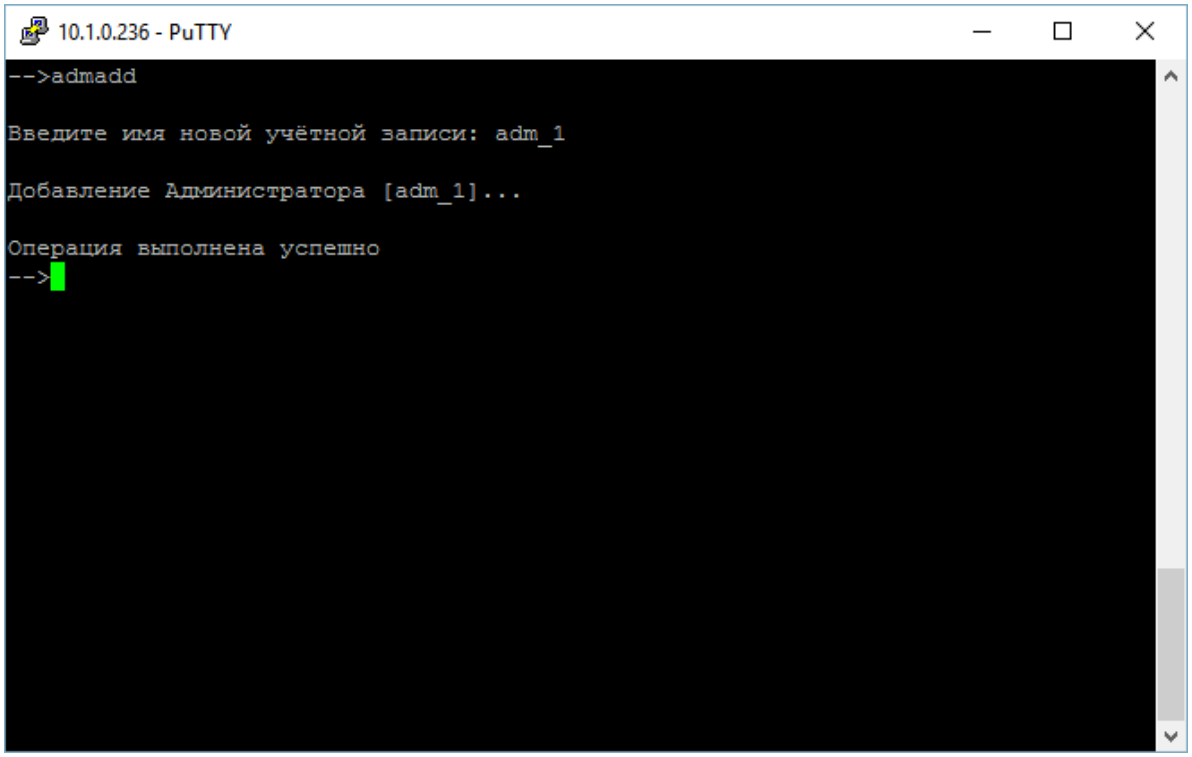

Рис. 3.2.4

3.2.2. Просмотр учетных записей Администраторов СПО

Для просмотра списка Администраторов СПО необходимо выполнить команду admlist. Результат выполнения команды показан на рис. 3.2.5:

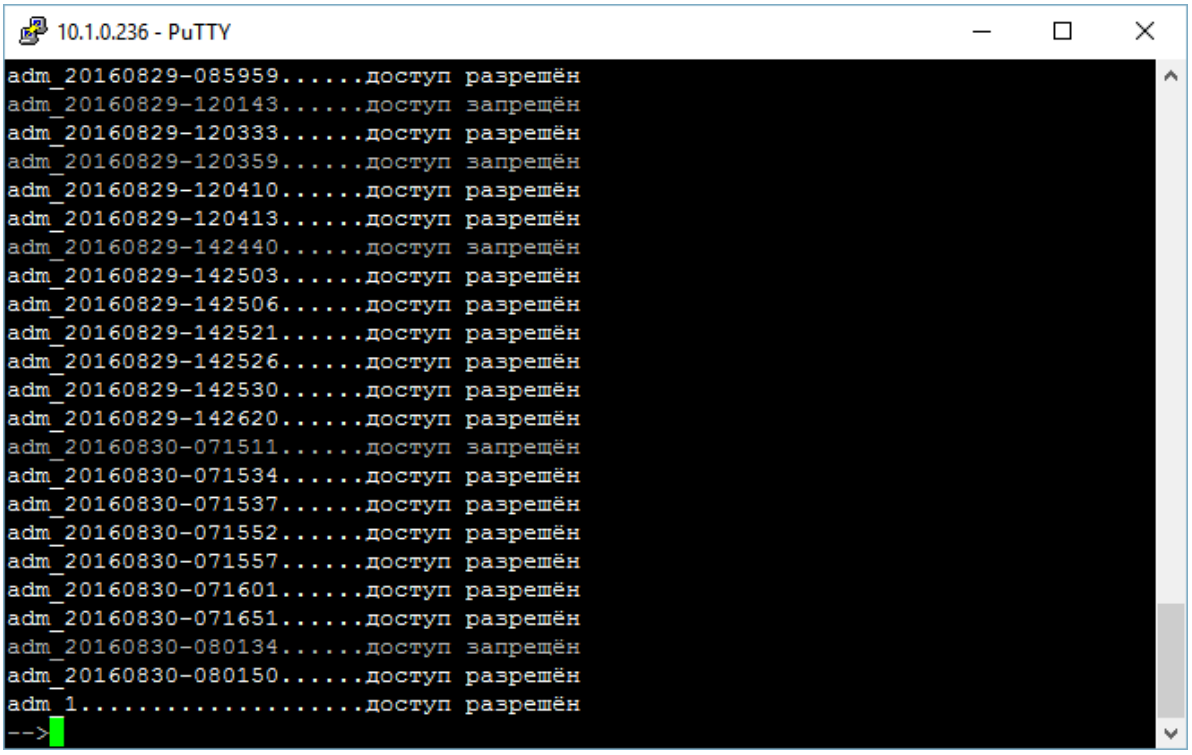

Рис. 3.2.5

3.2.3. Добавление учетной записи Администратора аудита

Чтобы добавить новую учетную запись Администратора аудита необходимо использовать команду audadd. Пример ее использования показан на рис. 3.2.6 – 3.2.8.

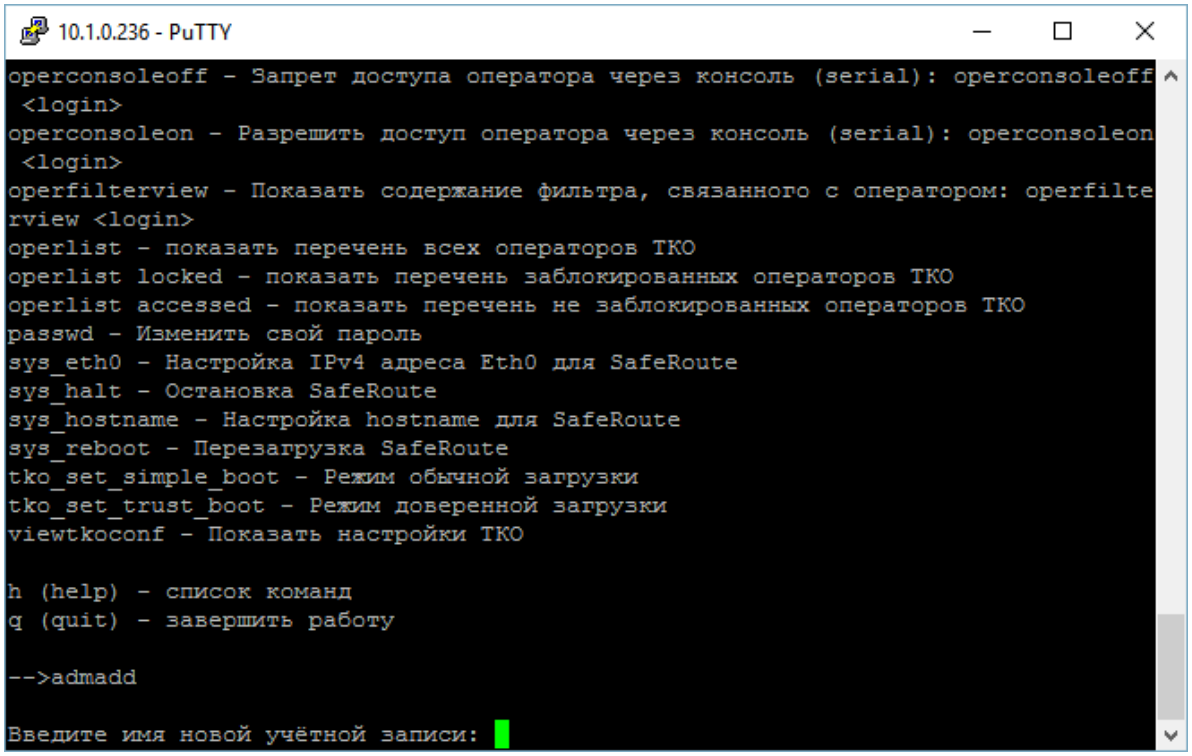

Рис. 3.2.6

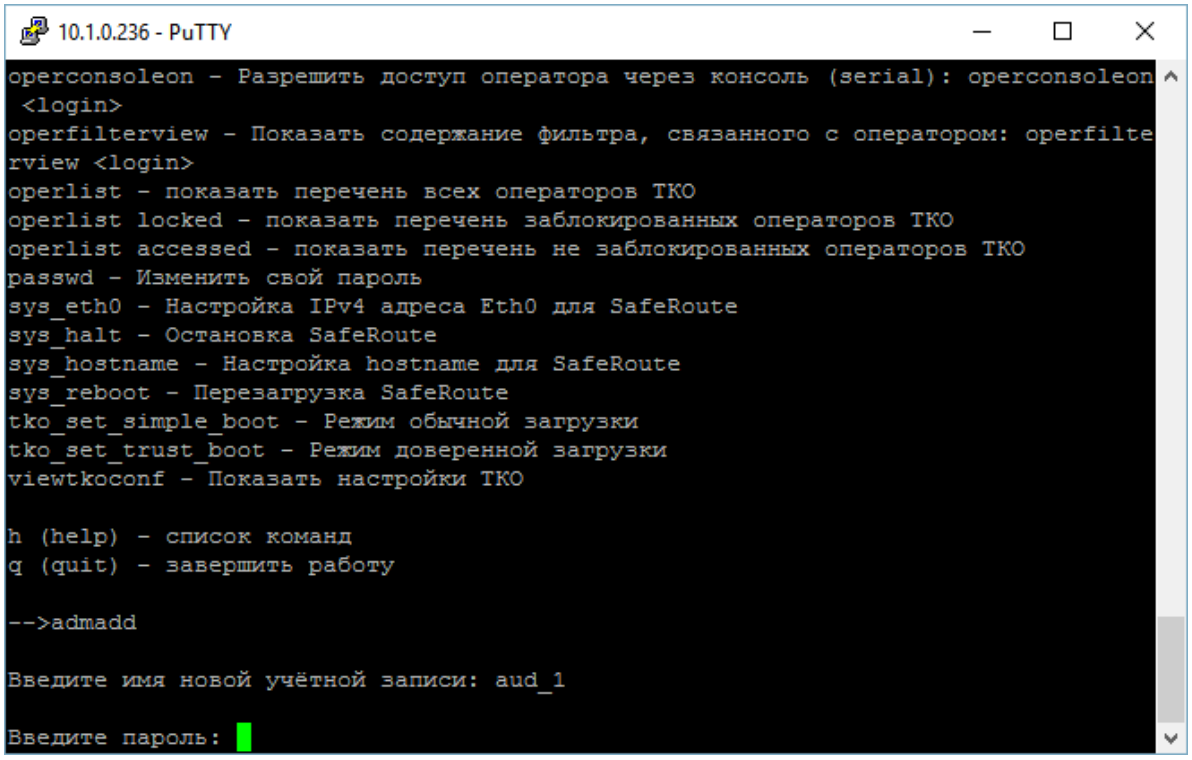

Рис. 3.2.7

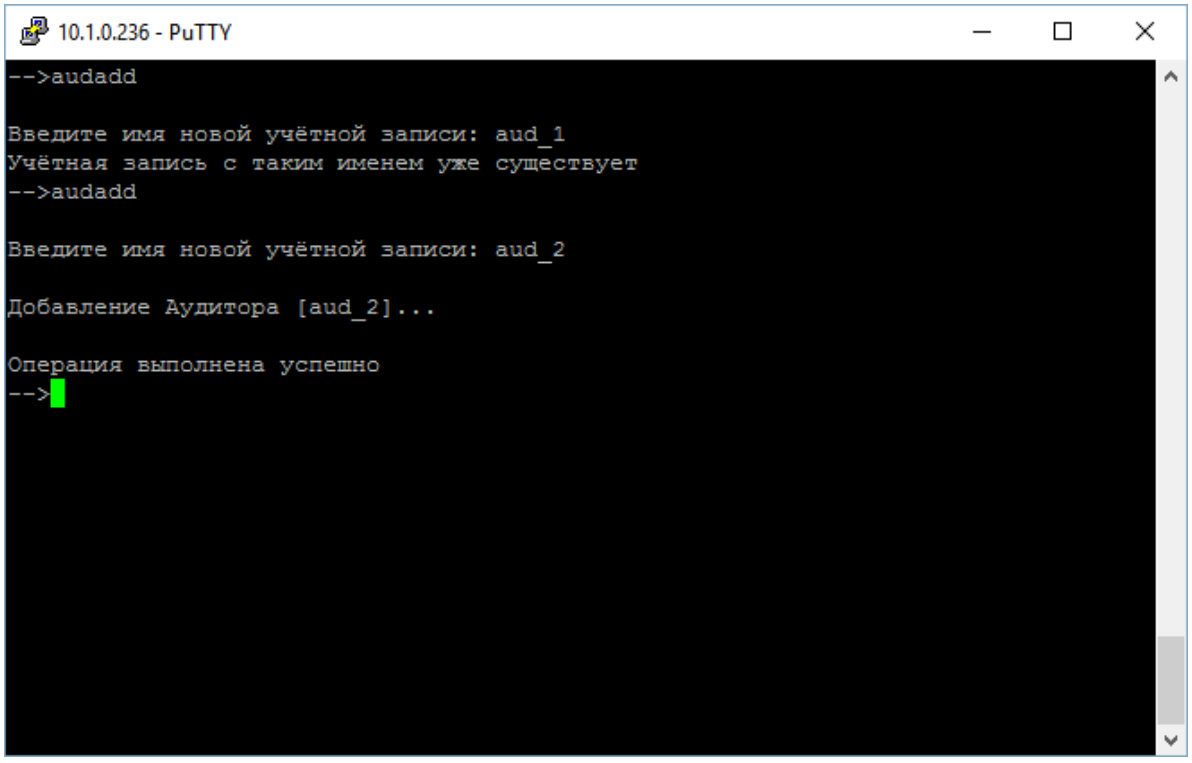

Рис. 3.2.8

3.2.4. Просмотр списка учетных записей Администраторов аудита

Чтобы просмотреть список учетных записей Администраторов аудита необходимо выполнить команду audlist. Пример её использования приведён на рис. 3.2.9.

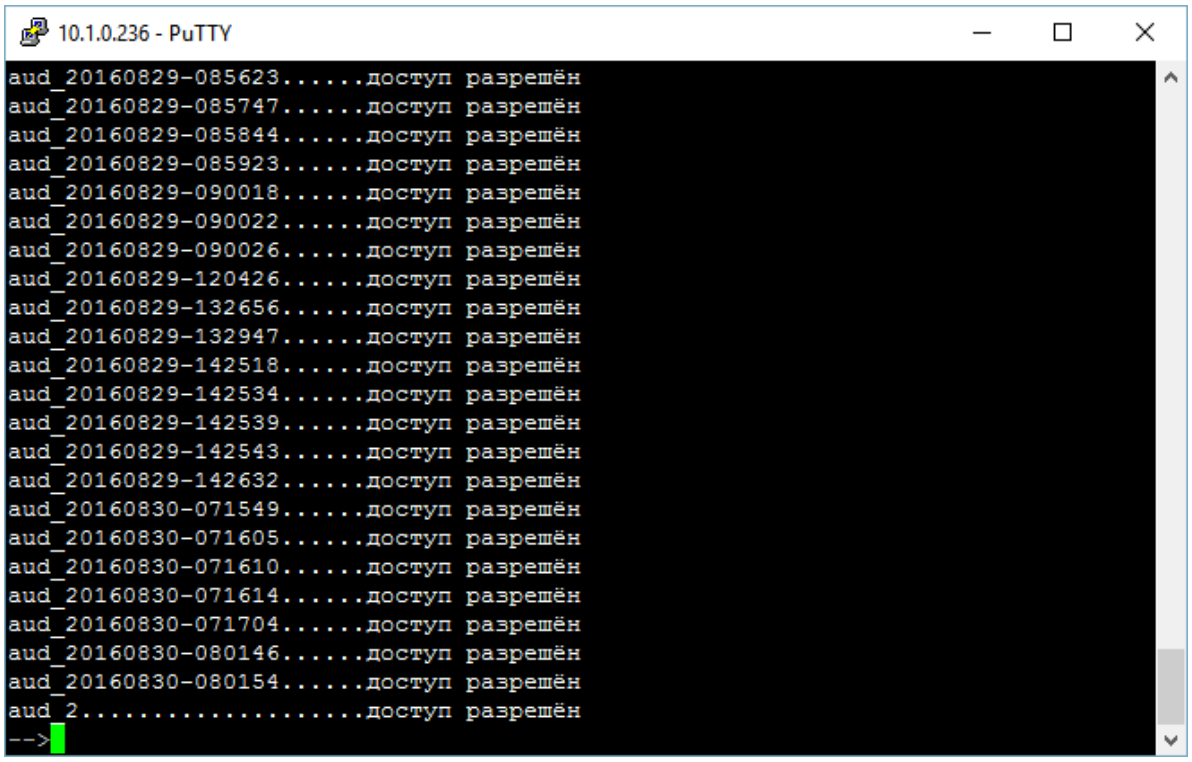

Рис. 3.2.9

3.2.5. Добавление учетной записи Функционального контролера

Чтобы добавить новую учетную запись Функционального контролера необходимо использовать команду fkadd. Пример ее использования показан на рис. 3.2.10, 3.2.11.

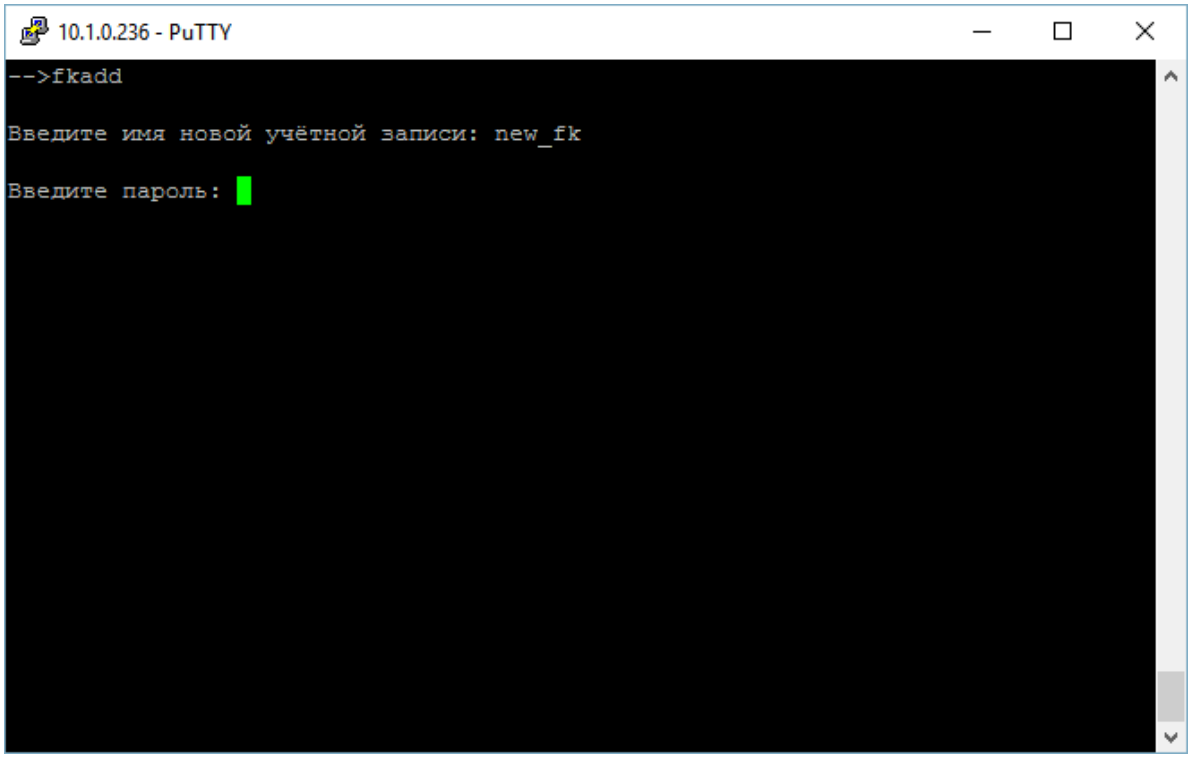

Рис. 3.2.10

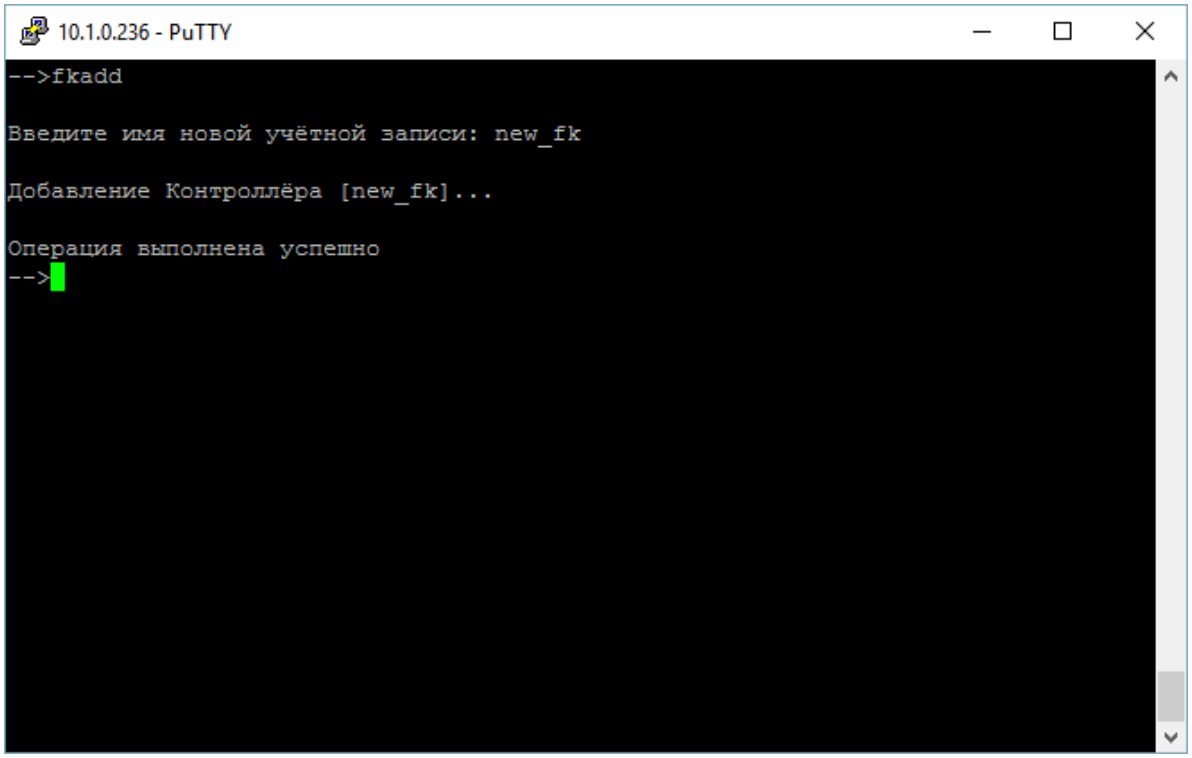

Рис. 3.2.11

3.2.6. Просмотр списка учетных записей Функциональных контролеров

Чтобы посмотреть список учетных записей Функциональных контролеров, нужно ввести команду fklist (рис. 3.2.12).

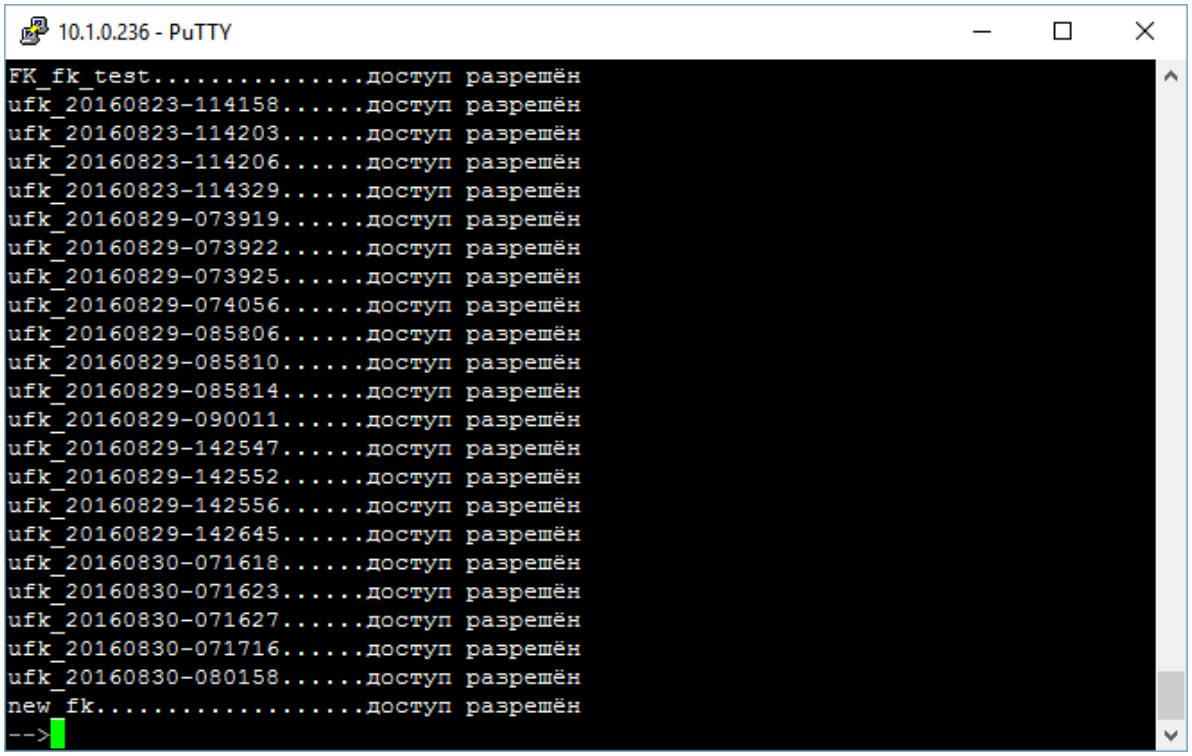

Рис. 3.2.12

3.2.7. Добавление учетной записи Оператора ТКО

Чтобы добавить новую учетную запись Оператора ТКО необходимо использовать команду operadd. Пример ее использования показан на рис. 3.2.13, 3.2.14:

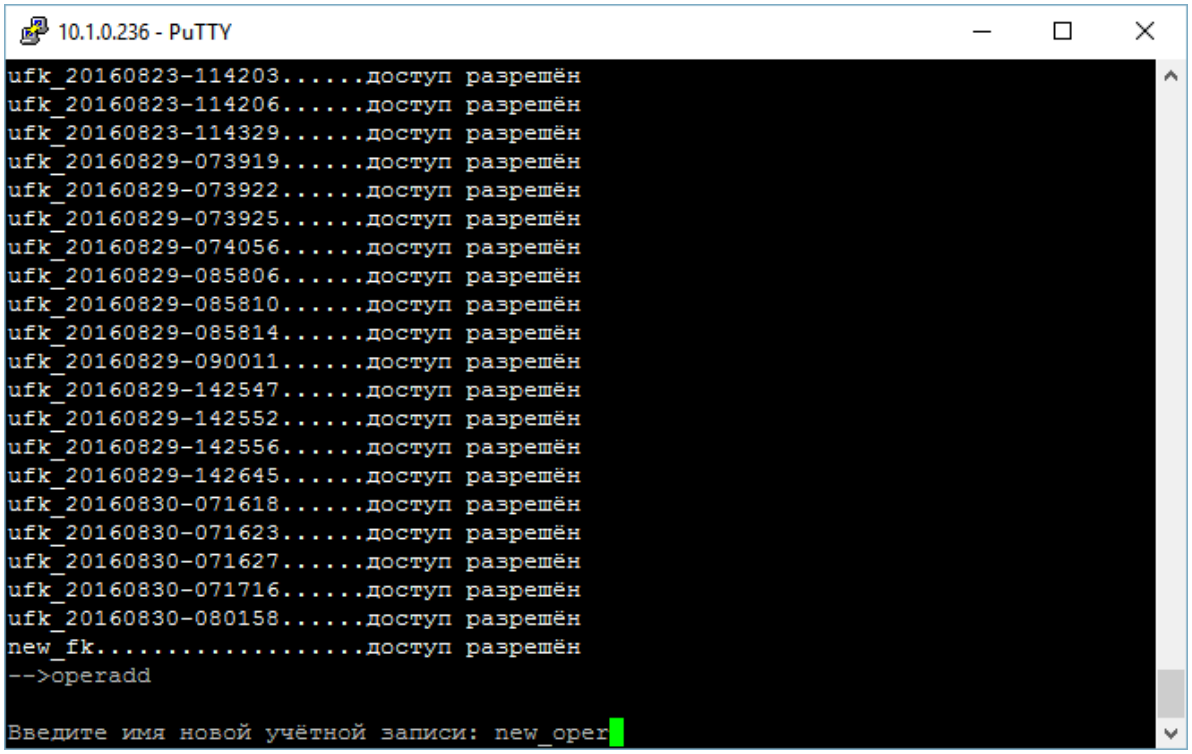

Рис. 3.2.13

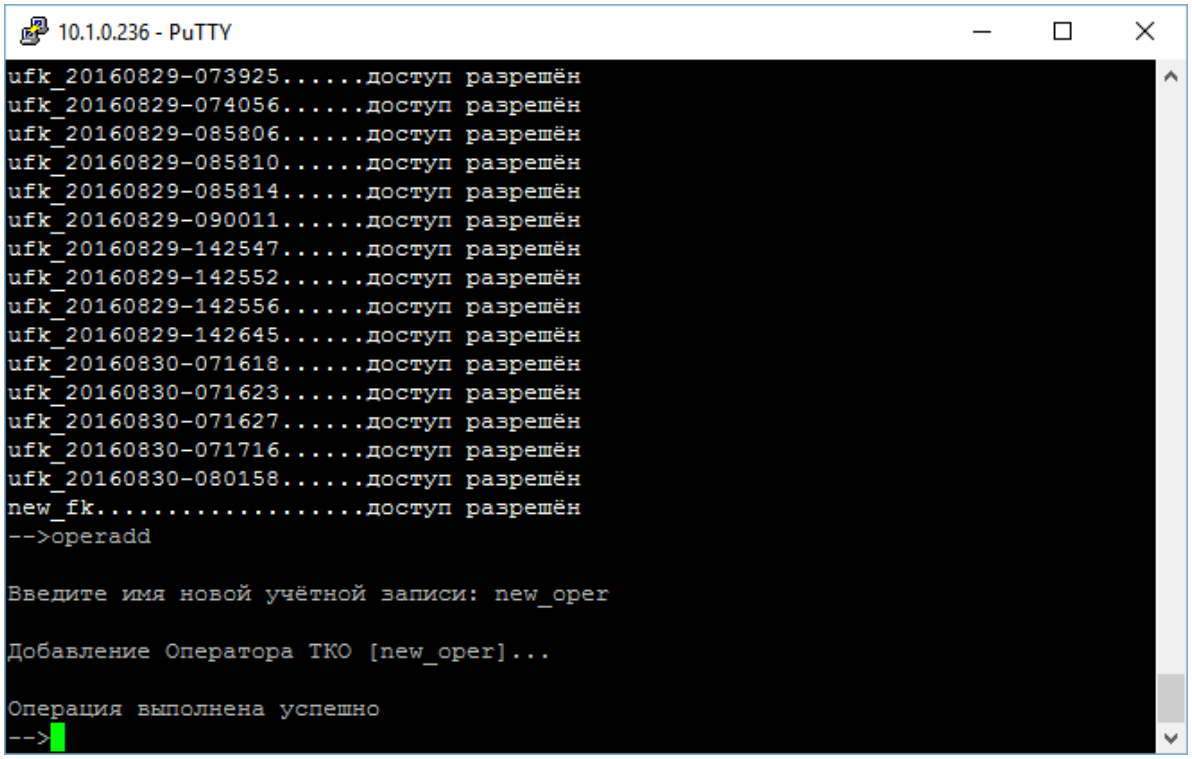

Рис. 3.2.14

3.2.8. Просмотр списка учетных записей Операторов ТКО

Чтобы посмотреть список учетных записей Операторов ТКО, нужно ввести команду operlist. Пример ее использования показан на рисунке 3.2.15.

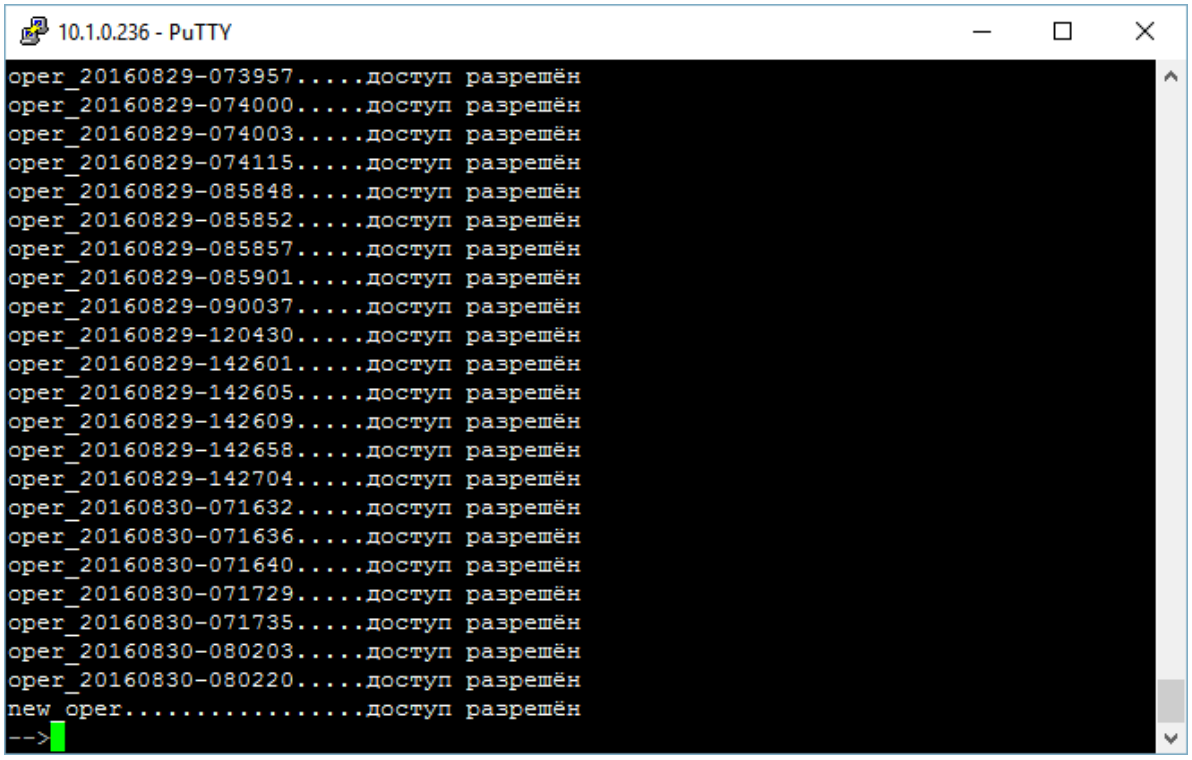

Рис. 3.2.15

3.2.9. Блокировка учетной записи пользователя

Для блокировки учетной записи пользователя нужно выполнить команду accountlock. Результат её выполнения показан на рис. 3.2.16 – 3.2.21:

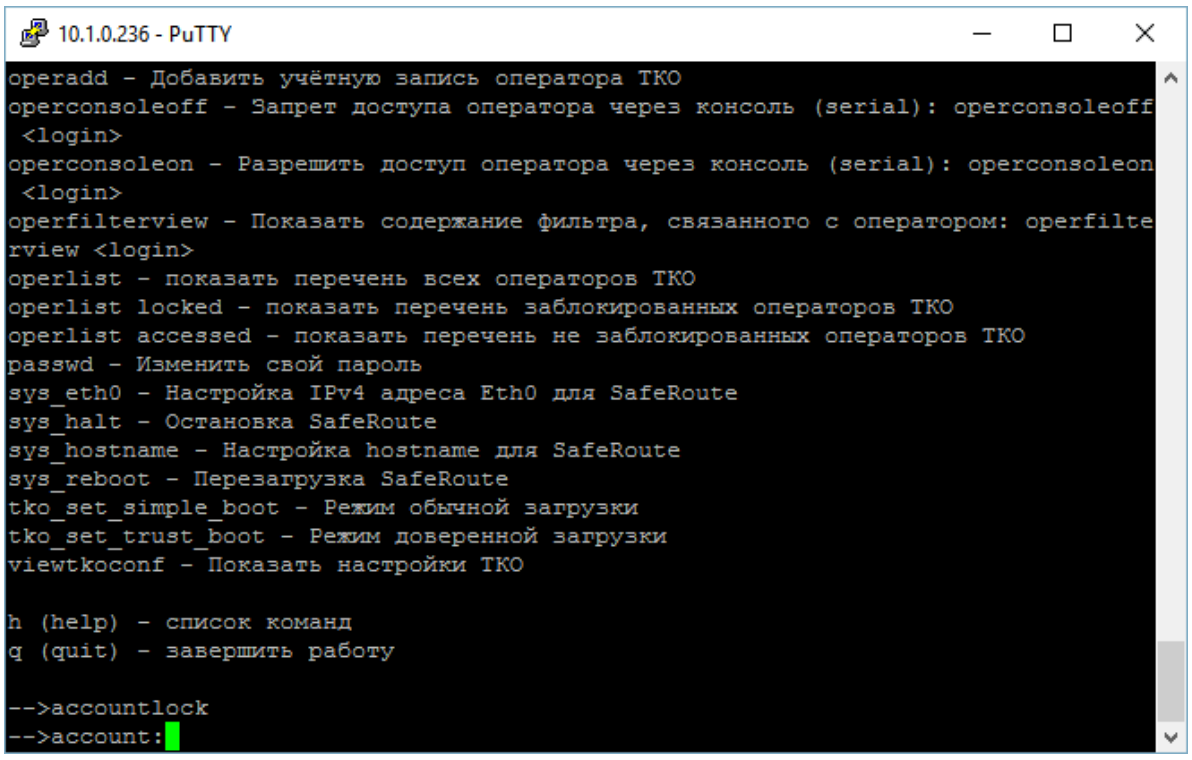

Рис. 3.2.16

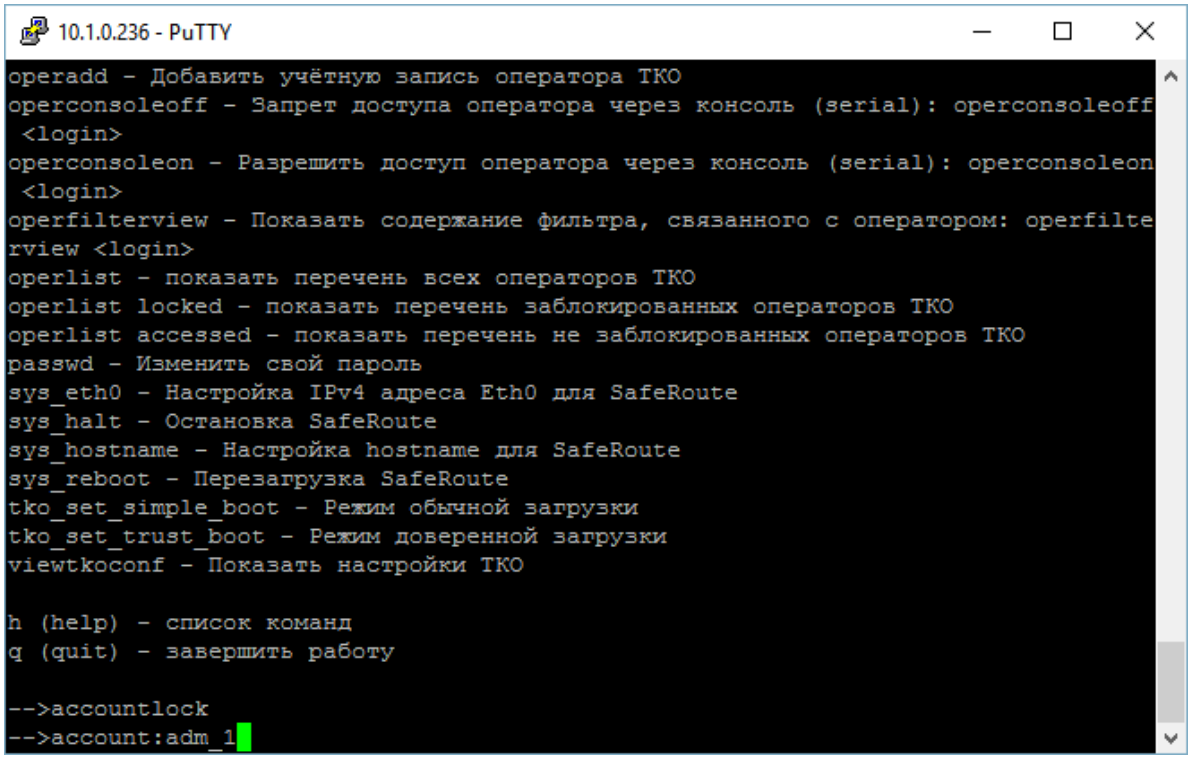

Рис. 3.2.17

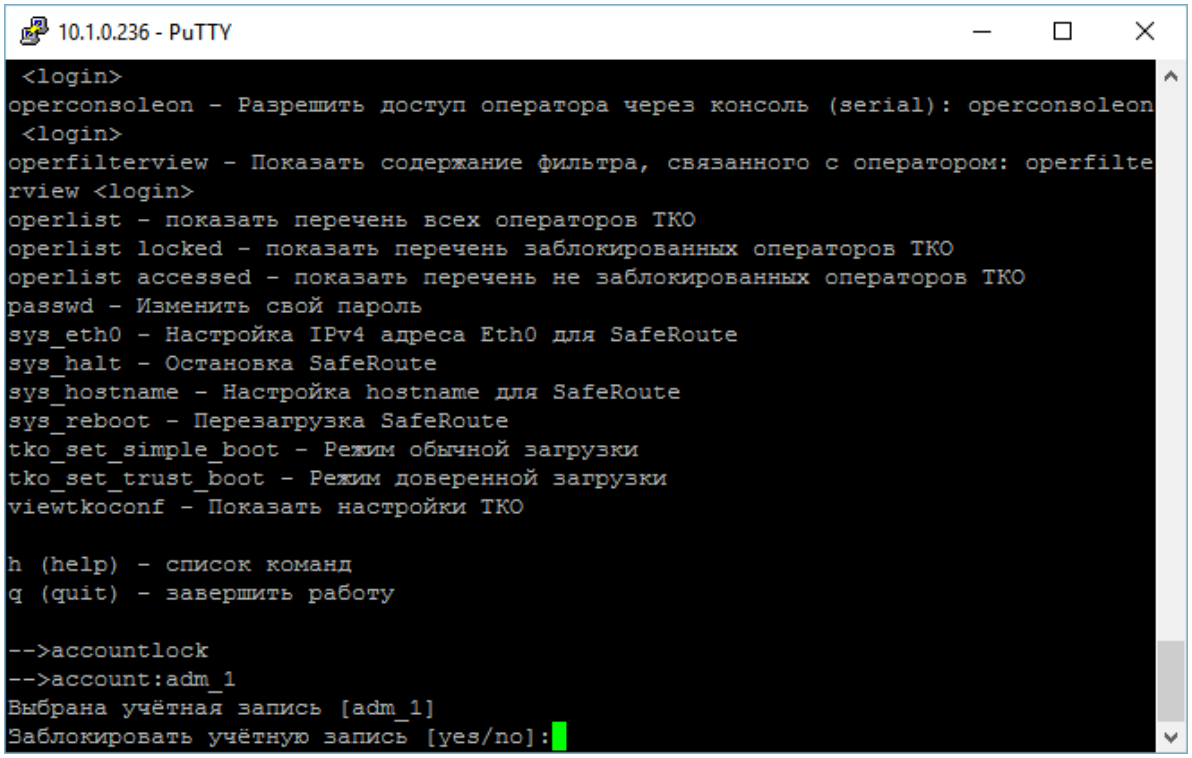

Рис. 3.2.18

Для блокировки учетной записи – ввести yes.

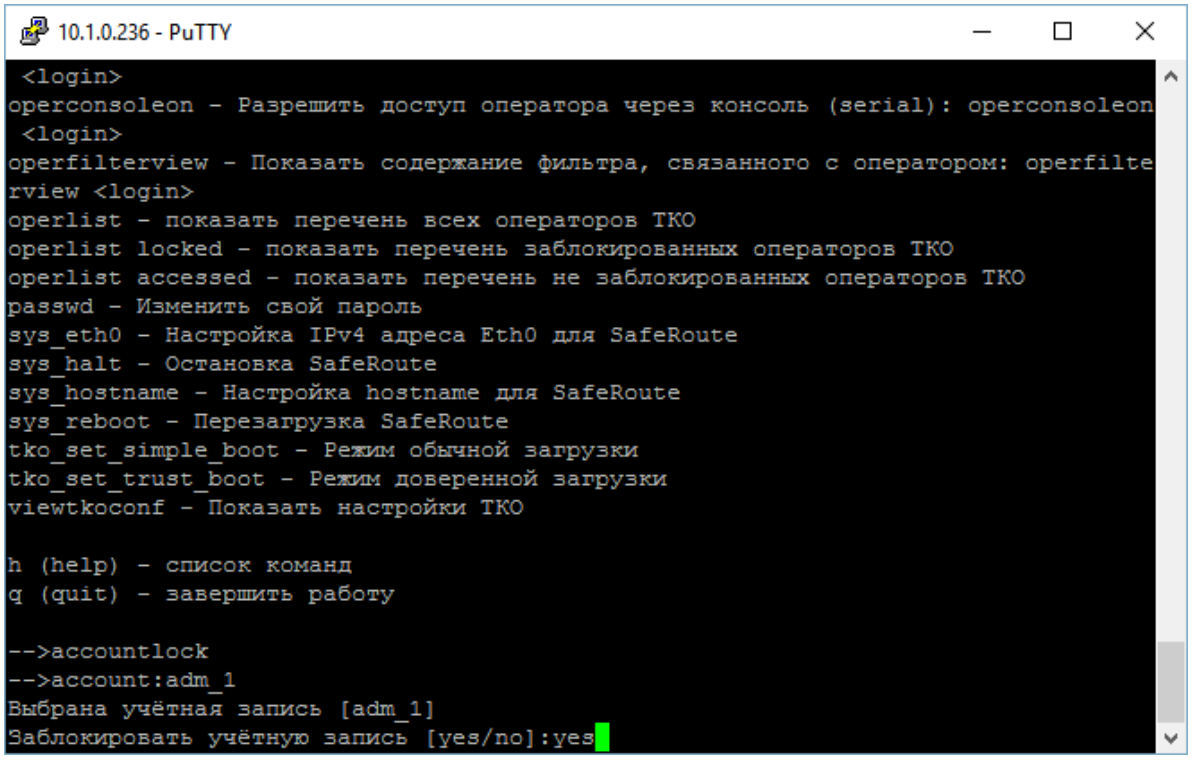

Рис. 3.2.19

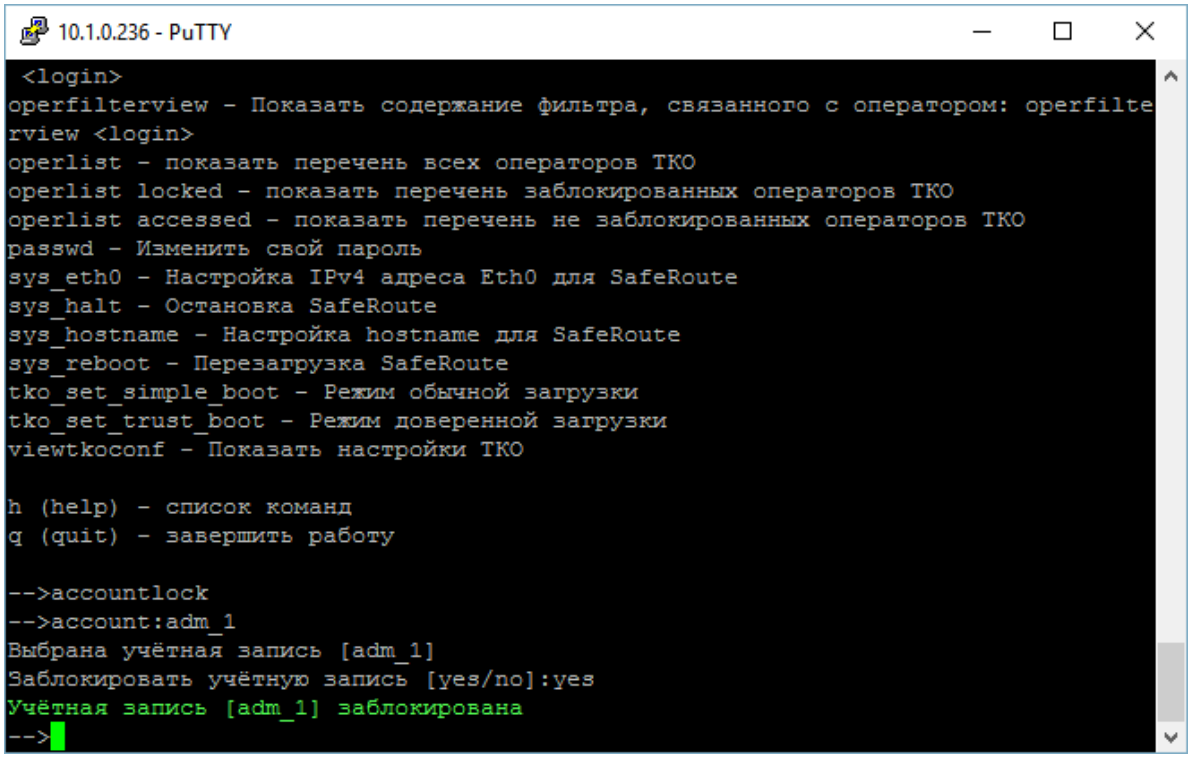

Рис. 3.2.20

Теперь adm_1 показан в списке с заблокированной учетной записью:

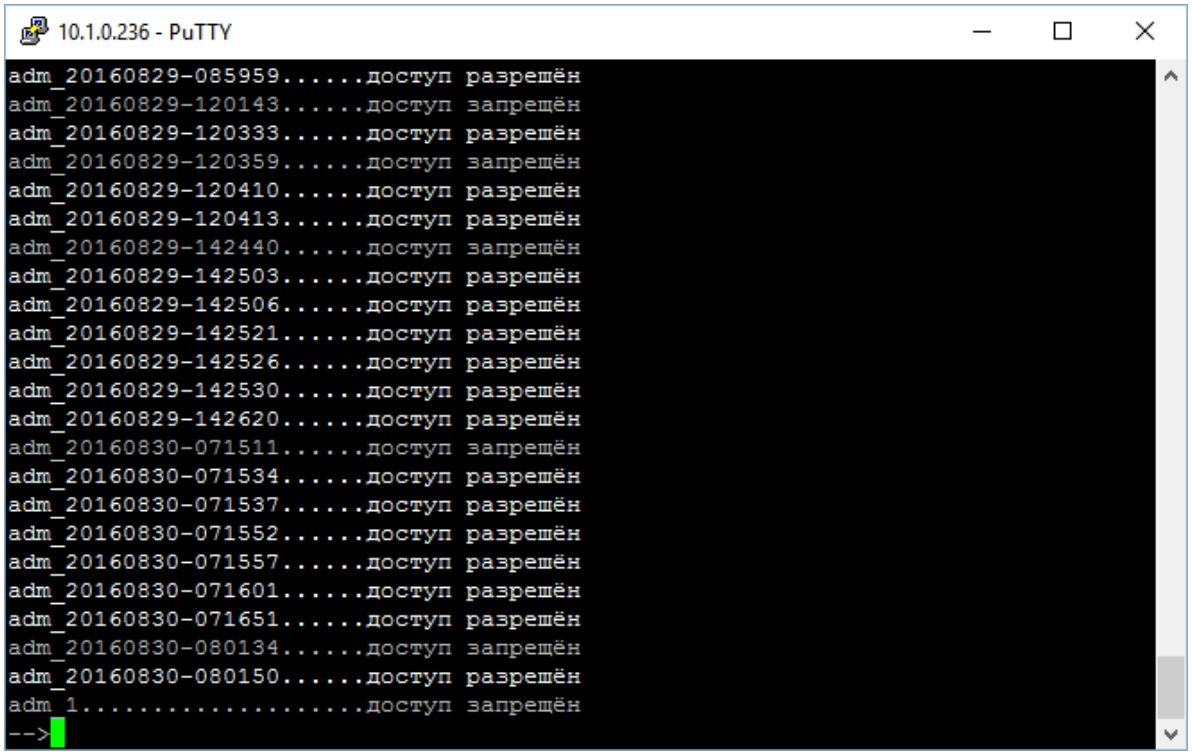

Рис. 3.2.21

3.2.10. Разблокировка учетной записи пользователя

Для разблокировки пользователя необходимо ввести команду accountunlock (рис. 3.2.22 – 3.2.25):

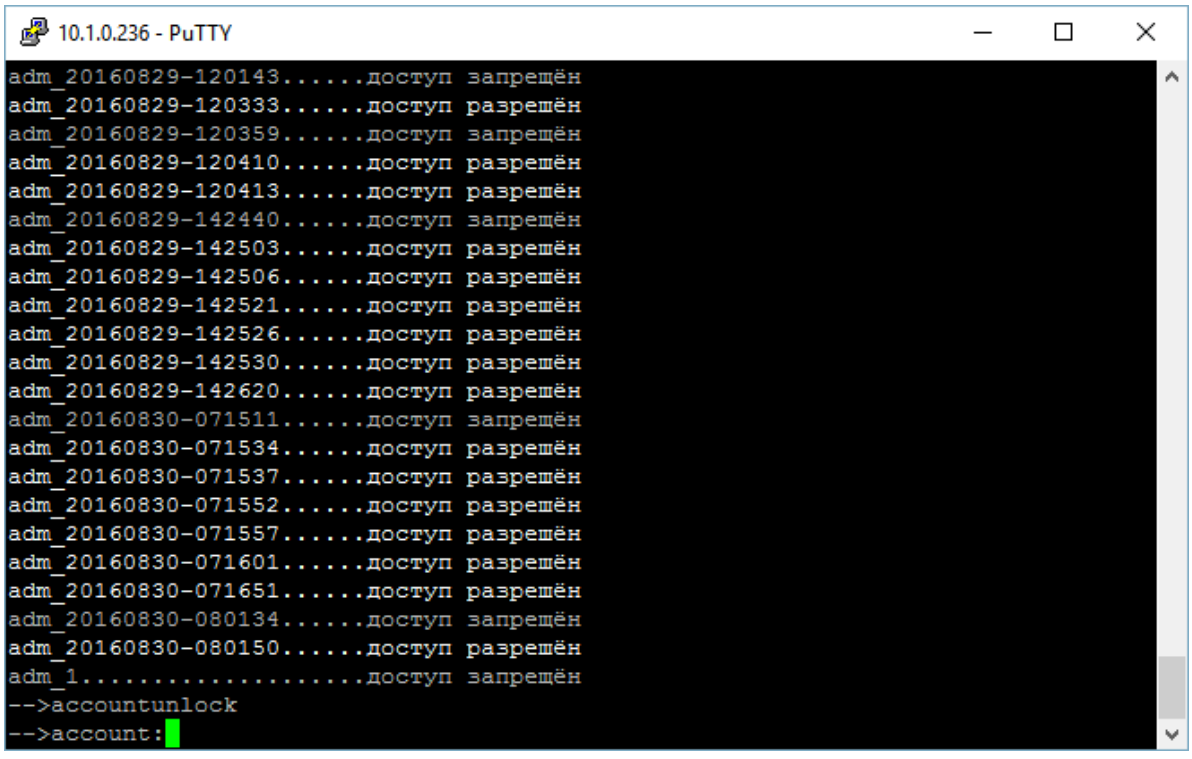

Рис. 3.2.22

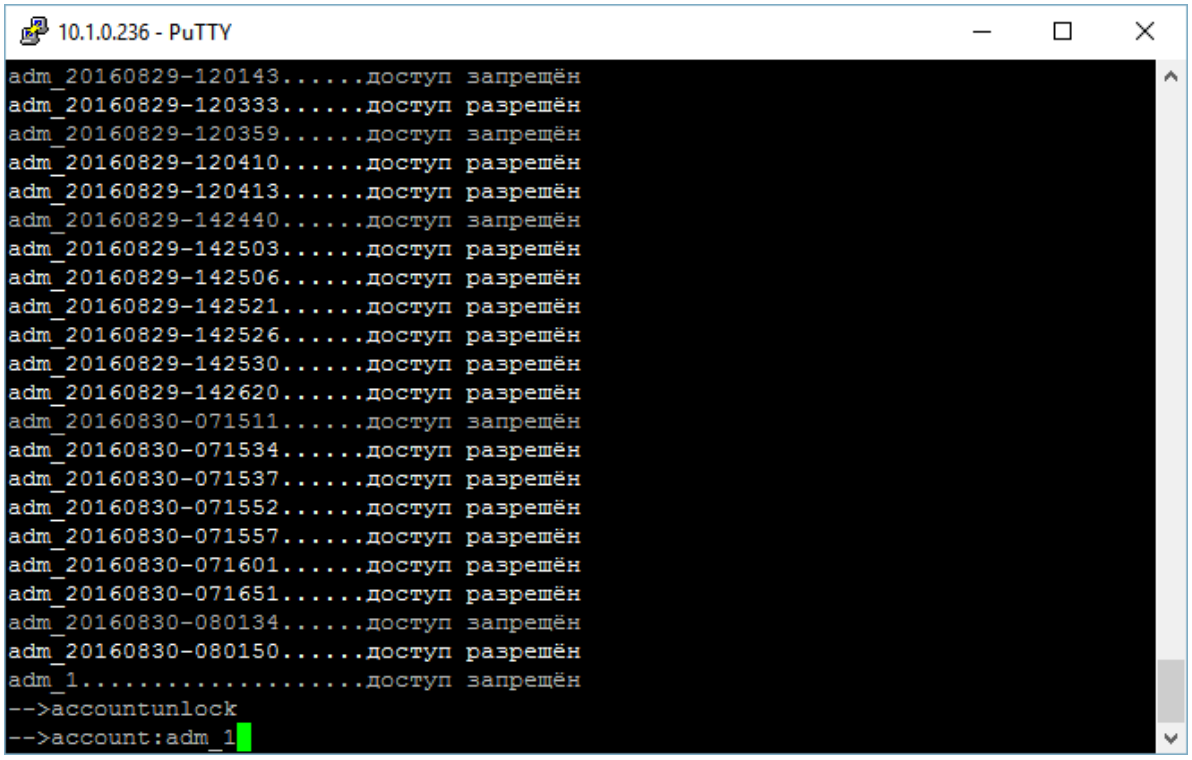

Рис. 3.2.23

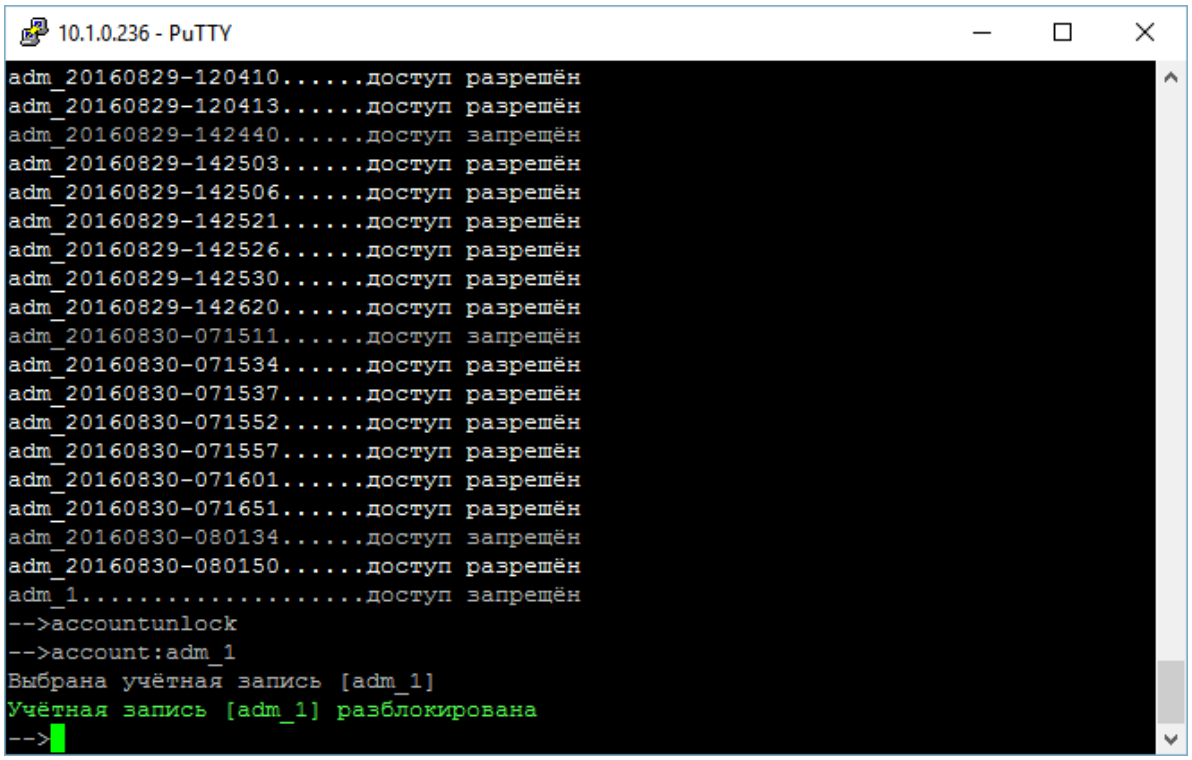

Рис. 3.2.24

После выполнения команды admlist видно, что учетная запись adm_1 разблокирована:

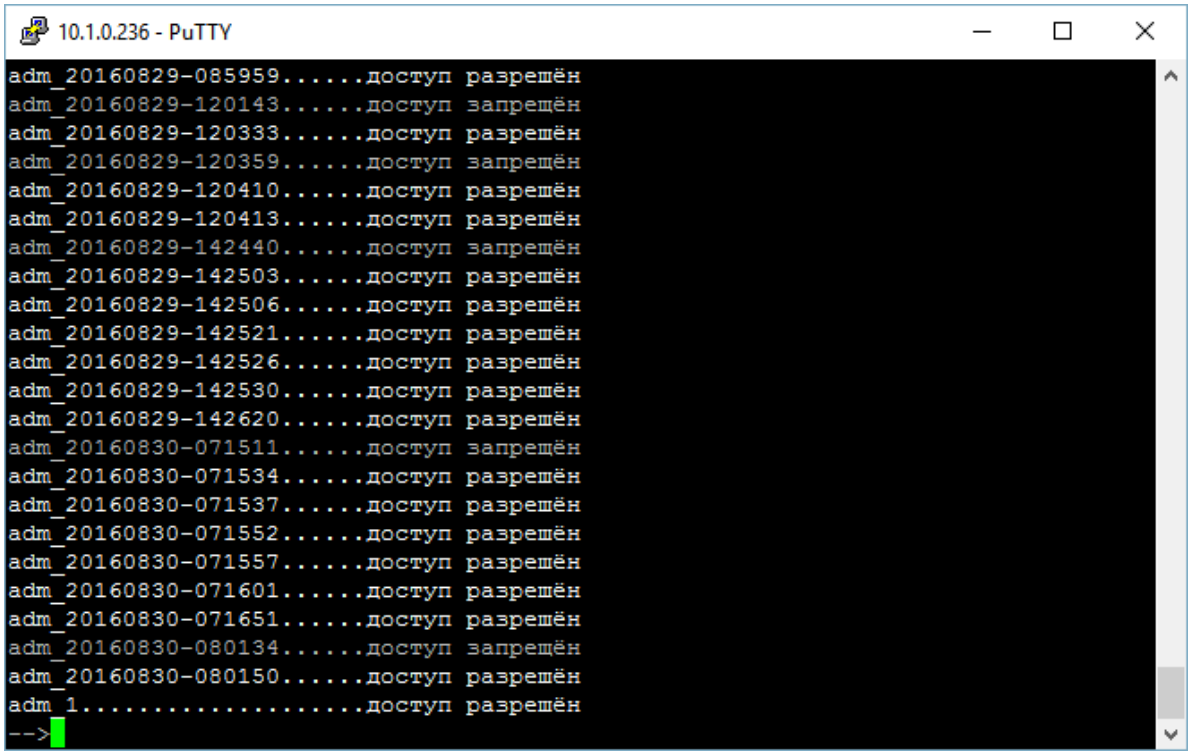

Рис. 3.2.25

3.2.11. Смена пароля для пользователя

Администратор СПО может заменить пароль любому пользователю СПО «SR». Для смены пароля необходимо выполнить команду accountpasswd, после чего ввести новый пароль. Для смены пароля Администратор СПО должен знать текущий (активный) пароль пользователя.

Предустановленными настройками СПО SR контролируются длина и сложность пароля, а также ведется история ранее использованных паролей. Результат успешного выполнения команды смены пароля показан на рис. 3.2.26 – 3.2.29:

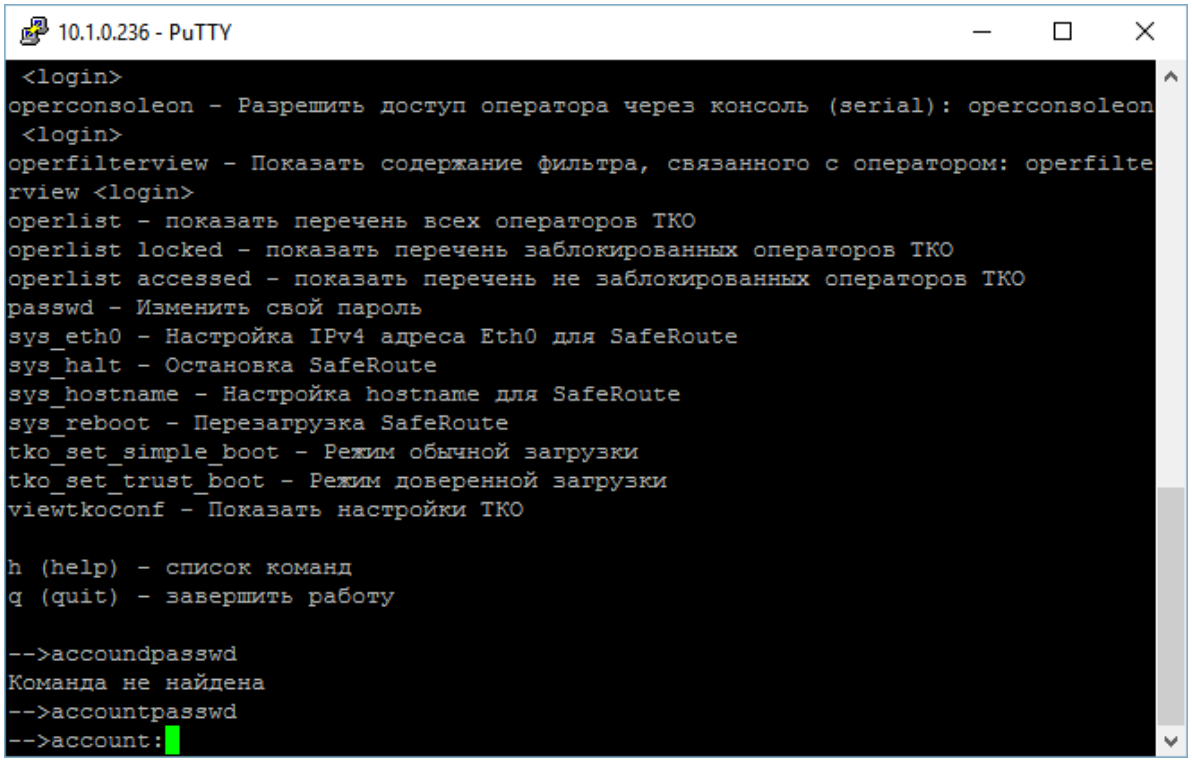

Рис. 3.2.26

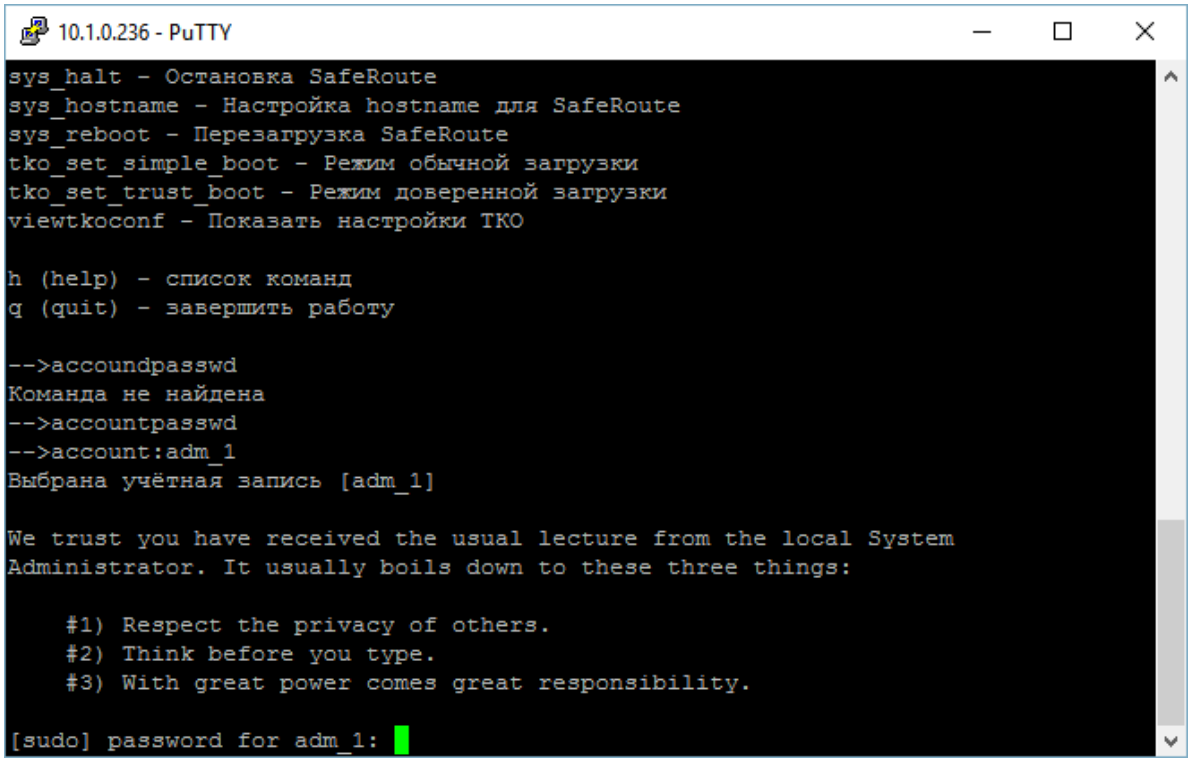

Рис. 3.2.27

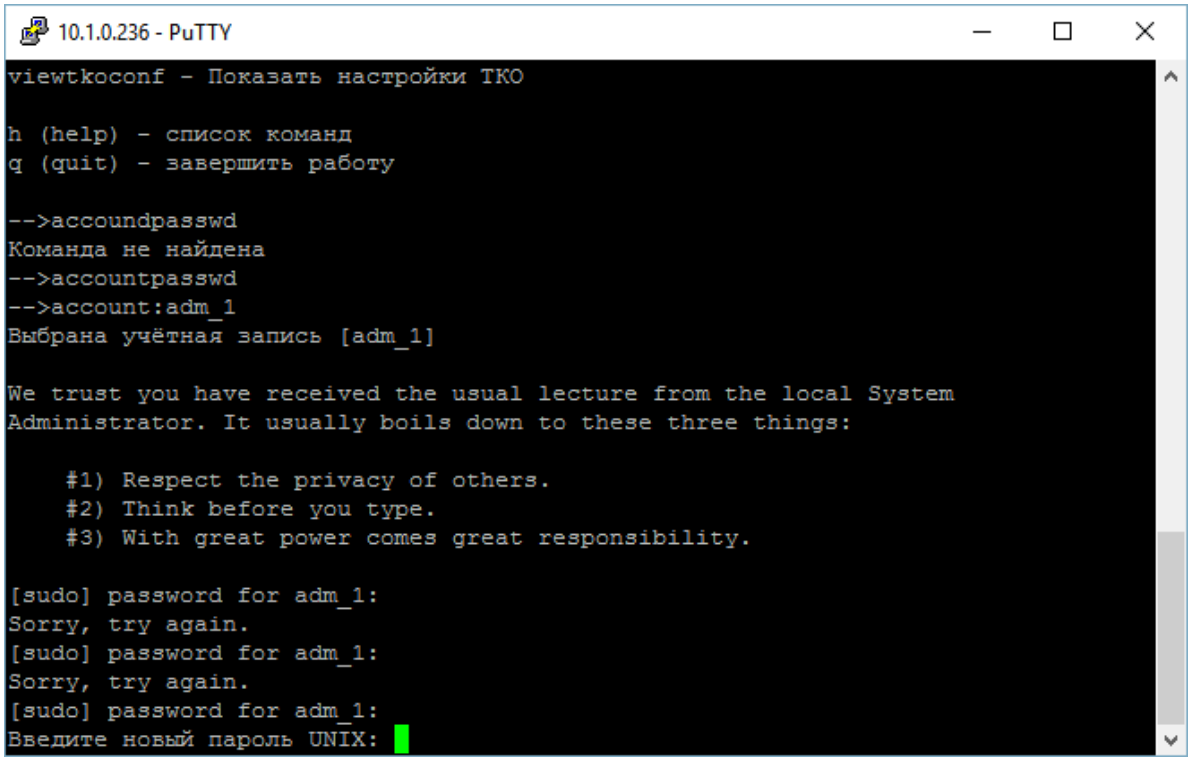

Рис. 3.2.28

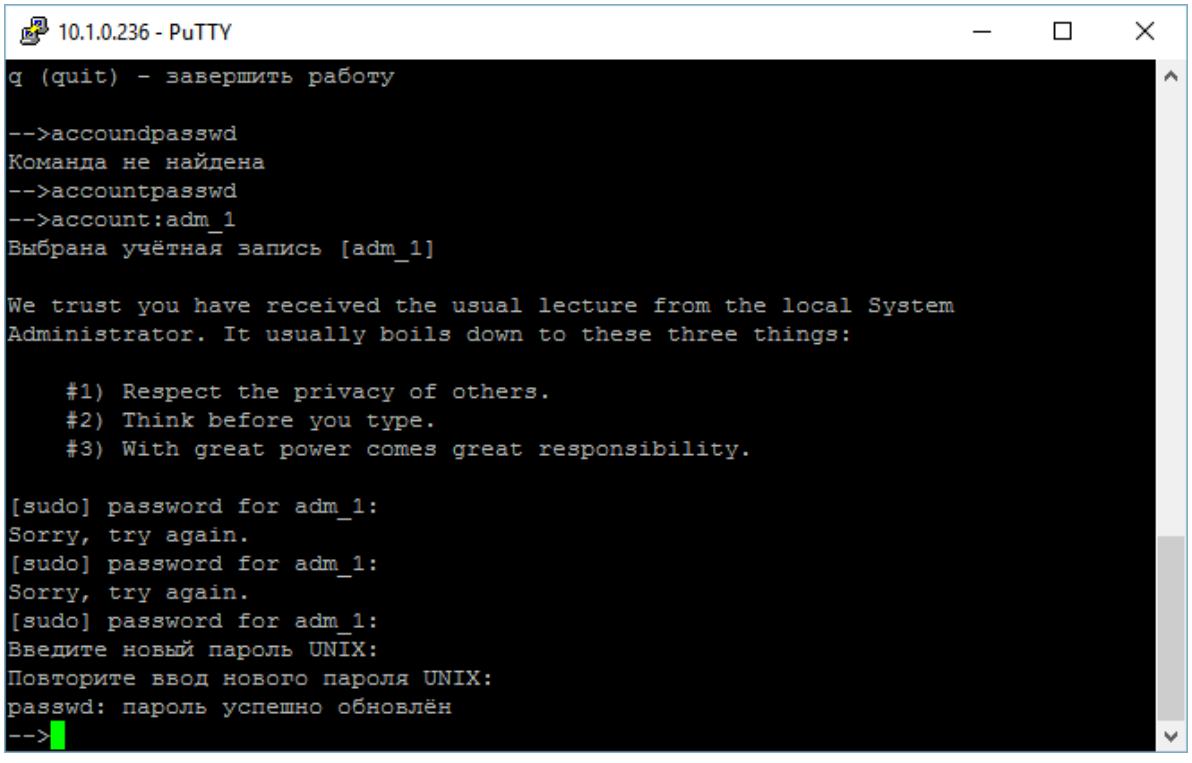

Рис. 3.2.29

3.2.12. Запрет доступа к консольному порту Оператору ТКО

Чтобы запретить Оператору ТКО доступ к консольному порту, нужно ввести команду operconsoleoff. Пример ее использования показан на рис. 3.2.30, 3.2.31:

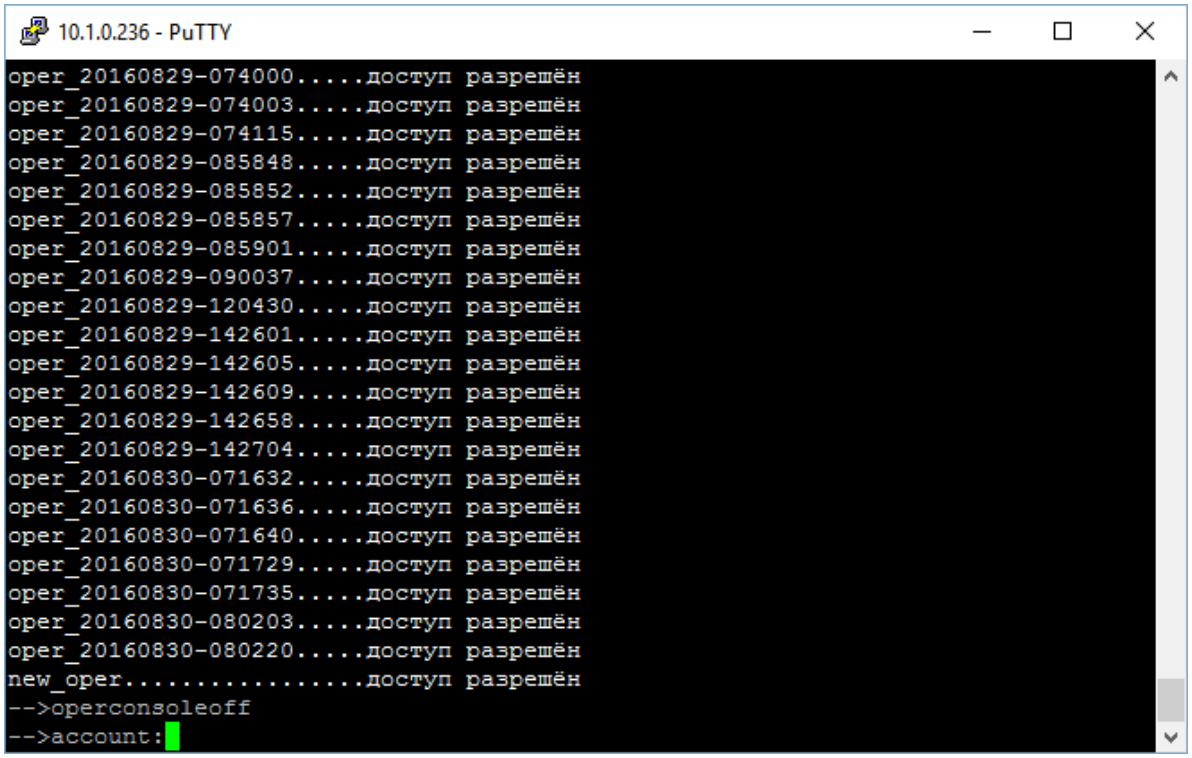

Рис. 3.2.30

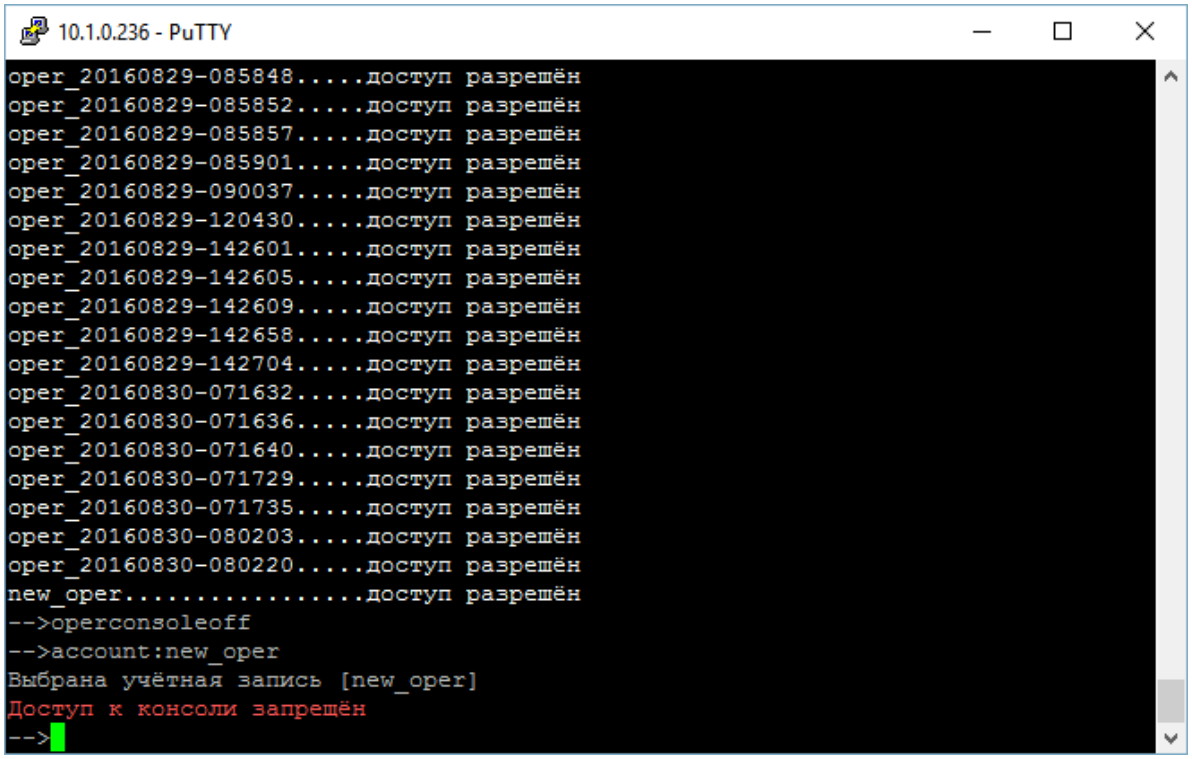

Рис. 3.2.31

3.2.13. Разрешение доступа к консольному порту Оператору ТКО

Чтобы разрешить Оператору ТКО доступ к консольному порту, нужно ввести команду operconsoleon. Пример ее использования показан на рис. 3.2.32, 3.2.33:

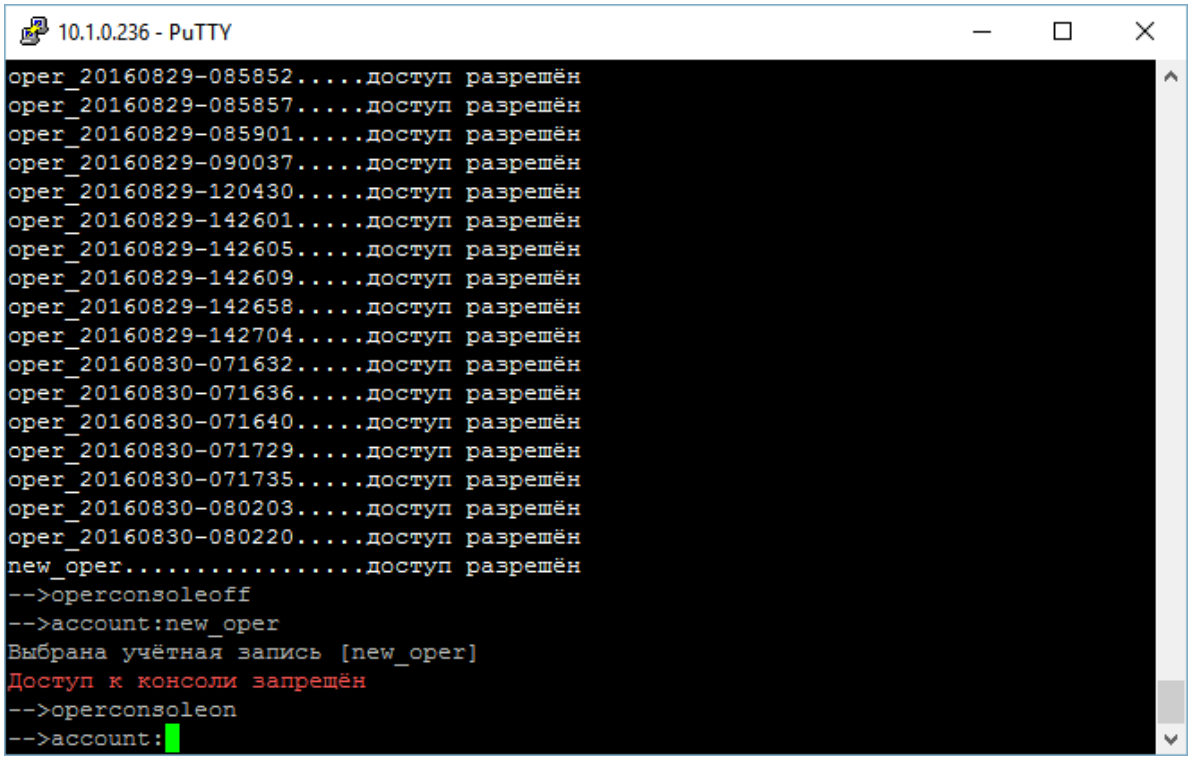

Рис. 3.2.32

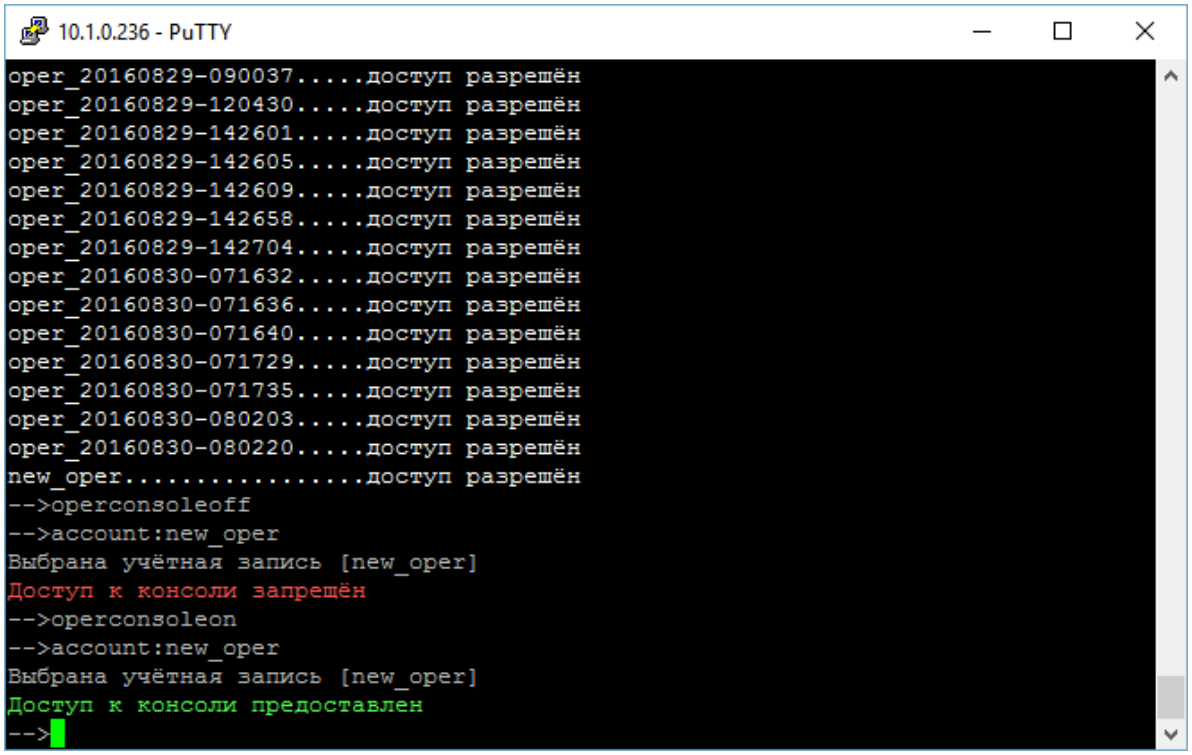

Рис. 3.2.33

3.2.14. Просмотр сведений о конфигурации ТКО

Для просмотра текущих настроек ТКО необходимо выполнить команду viewtkoconf. Результат выполнения команды вывода текущих настроек ТКО показан на рис. 3.2.34:

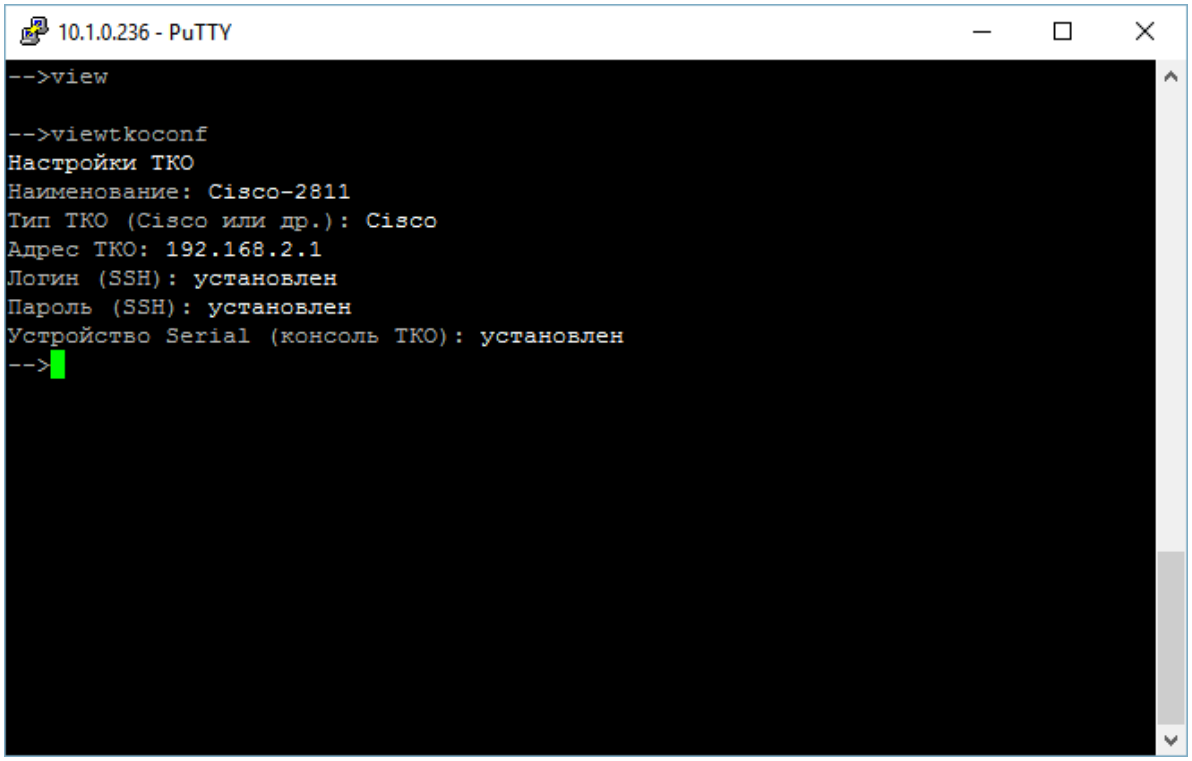

Рис. 3.2.34

4. ТРЕБОВАНИЯ К ПРОГРАММНО-АППАРАТНОЙ КОНФИГУРАЦИИ

Для выполнения установки СПО SR необходимо обеспечить следующую конфигурацию аппаратных и программных средств:

- СПО с предустановленным ОПО, имеющим доступ в локальную сеть, с IP-адресом 192.168.0.2

- Компьютер: Процессор: Intel(R) Xeon(R) CPU (E5520 @ 2.27GHz); Емкость ОЗУ: 8 Гб; Жесткий диск: 60 Гб. Установленная ОС – Debian 8 32-bit