Общество с ограниченной ответственностью «ДИАЛОГ-ТРАНС»
(ООО «ДИАЛОГ-ТРАНС»)

Программное обеспечение Автоматизированной системы диспетчерского управления движением поездов метрополитена «Диалог» (АСДУ ДПМ «Диалог»)

Политика пользователей АРМ АСДУ ДПМ «Диалог»

Руководство пользователя

Листов 34

Москва 2022

Содержание

СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

АСДУ ДПМ	Автоматизированная система диспетчерского управления движением поездов метрополитена
АРМ	Автоматизированное рабочее место
АРМ УДП	Автоматизированное рабочее место управления движением поездов
ДЦ ММ	Система диспетчерской централизации
ПО	Программное обеспечение
ЦДПШ	Дежурный инженер СЦБ центрального поста управления
СЦБ	Сигнализация, централизация и блокировка
ДЦ	Диспетчерская централизация
АРМ ДЦХ	Автоматизированное рабочее место поездного диспетчера – централизатора
ИБП	Источник бесперебойного питания
Идентификационная (ID) карта	Карта типа Mifare, используется для хранения и ввода идентификационных данных пользователей через считыватели (картридеры), подсоединенные к АРМ
Учетная запись пользователя	Информация по каждому пользователю, содержащая: имя пользователя, пароль, номер (ID) карты и прочие идентификационные данные, предусмотренные проектом АСДУ ДПМ. Информация хранится в базе идентификационных данных пользователей АРМ - «userpolicy»
База «userpolicy»	База данных под управлением СУБД posgreSQL содержащая учетные записи пользователей АРМ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ распространяется на программное обеспечение – «Политика пользователей АРМ АСДУ ДПМ «Диалог» (далее по тексту «ПО Политика пользователей АРМ» везде где не указано иное). ПО Политика пользователей АРМ предназначено для управления наборами прав и возможностей пользователей, имеющих допуск для работы на АРМ(ы) АСДУ ДПМ «Диалог».

Данное руководство вводит пользователя в предметную область, знакомит со всеми возможностями работы с программой, описывает конкретные процедуры, позволяющие решать прикладные задачи с помощью ПО Политика пользователей АРМ.

Знание данного документа обязательно для всех пользователей, которым предоставлено право работы с ПО Политика пользователей АРМ.

1.1. Общие сведения

Система АСДУ ДПМ «Диалог» представляет собой комплекс программно-аппаратных средств и предназначена для организации автоматизированного управления поездной и маневровой работой на линиях метрополитена.

Конкретный набор аппаратно-программных средств, количество АРМ и серверов их типы, конфигурация локальной сети системы АСДУ ДПМ «Диалог» определяется проектом.

ПО Политика пользователей АРМ устанавливается на все целевые АРМ, для которых проектом предусмотрен вход пользователей с применением системы аутентификации.

1.2. Функциональные возможности ПО

ПО Политика пользователей АРМ обеспечивает выполнение следующих функций:

- Ввод новых, удаление и редактирование существующих пользователей АРМ и их идентификационных данных.
- Хранение идентификационных данных пользователей АРМ в отдельной базе под управлением СУБД Postgresql на дублированных серверах (основном и резервном);

- Разделение пользователей АРМ по группам с назначением каждой группе определенного набора прав;
- Сохранение сообщений системы в процессе работы ПО Политика пользователей АРМ в журнал событий – log-файл.

1.3. Требования к аппаратным средствам

Для нормального функционирования ПО Политика пользователей АРМ необходимы аппаратные средства в следующем составе:

- системный блок в промышленном исполнении с конфигурацией не хуже:
  - Аппаратная платформа x86-64(AMD64/Intel64/EM64T),
  - Процессор X86_64 1.6ГГц 2 ядра,
  - Объем оперативной памяти от 2Гб и выше,
  - Свободное доступное место на жестком диске объемом не менее 4Гб,
  - Видеоадаптер с поддержкой режима SVGA 1920x1280 и выше,
  - Адаптер сетевых интерфейсов с двумя физическими портами, подсоединенный к общей локальной сети АСДУ ДПМ «Диалог».
- монитор с размером экрана не менее 19” с разрешением не менее 1920x1080.
- клавиатура, имеющая русскоязычную раскладку.
- манипулятор типа «мышь»;
- блок бесперебойного питания не менее 600ВА.
- картридер (считыватель) карт типа Mifare. Необходимость определяется проектом.

ПО Политика пользователей АРМ работает под управлением операционной системы РЕД ОС 7.3 и выше в конфигурации рабочая станция или сервер, что определяется проектом. На компьютере до установки ПО Политика пользователей АРМ должен быть создан пользователь с именем «dialog» и суперпользователь «root», а также установлена СУБД Postgresql 13 или выше.

Для хранения базы идентификационных данных пользователей АРМ необходимо наличие двух компьютеров выполняющих роль основного и резервного сервера. Минимальные требования к аппаратно-программной части

этих серверов аналогичны требованиям для нормального функционирования ПО Политика пользователей АРМ, изложенные выше.

2. ГРУППЫ ПОЛЬЗОВАТЕЛЕЙ АРМ

Система защиты идентификационных данных пользователей основана на разграничении прав пользователей по их принадлежности к определенной группе:

- Каждый сотрудник, имеющий допуск для работы на определенном(ых) АРМ АСДУ ДПМ «Диалог» заносится в базу идентификационных данных при помощи ПО Политика пользователей АРМ и обладает одним из следующих типов прав:
- **Операторы** – могут работать на разрешённых АРМах;
- **Инженеры** – обладают всеми правами **Оператора**, а также могут создавать новых, редактировать и удалять существующих **Операторов**;
- **Администраторы** – обладают всеми правами **Инженеров**, а также могут создавать новых, редактировать и удалять существующих **Инженеров**;
- **Директор** – супер-администратор, который обладает всеми правами **Администраторов**, а также может создавать новых, редактировать и удалять существующих **Администраторов**.
- Все данные пользователей хранятся в отдельной базе данных («userpolicy» – база идентификационных данных пользователей АРМ) на двух серверах (основном и резервном);
- На каждом АРМе располагается специализированный стартовый конфигурационный файл «start.config» с настройками доступа к базе идентификационных данных пользователей АРМ – «userpolicy».

3. НАБОРЫ ПРАВ ПОЛЬЗОВАТЕЛЕЙ АРМ

Как отмечалось выше пользователи делятся на **Операторов**, **Инженеров** и **Администраторов**, а также обладающего максимальными правами **Директора**. Ниже приведен перечь операций доступных каждой группе пользователей.

Операторы:

- Могут изменять только свой пароль и идентификационную (ID) карту;
- Удаление собственной учетной записи или изменение собственного имени и режима **Оператор** невозможно.

Инженеры:

- Могут редактировать имена, пароли, ID карты и права доступа к АРМам как свои, так и всех **Операторов**;
- Создавать новых и удалять существующих **Операторов**;
- Могут изменять свой пароль и идентификационную (ID) карту;
- Для выполнения вышеперечисленных операций **Инженерам** достаточно войти в ПО Политика пользователей АРМ под своим паролем или при помощи идентификационной (ID) карты;
- Удаление собственной учетной записи или изменение собственного имени и режима **Инженер** невозможно.

Администраторы:

- Могут редактировать имена, пароли, ID карты и права доступа к АРМам как свои, так и всех **Операторов**, и **Инженеров**;
- Создавать новых и удалять существующих **Операторов** и **Инженеров**;
- Могут изменять свой пароль и идентификационную (ID) карту;
- Для выполнения вышеперечисленных операций **Администраторам** достаточно войти в ПО Политика пользователей АРМ под своим паролем или при помощи идентификационной (ID) карты;
- Удаление собственной учетной записи или изменение собственного имени и режима **Администратор** невозможно.

Директор:

- Может редактировать имена, пароли, ID карты и права доступа к АРМам как свои, так и всех **Операторов**, **Инженеров** и **Администраторов**;
- Создавать новых и удалять существующих **Операторов**, **Инженеров** и **Администраторов**;
- Может изменять своё имя пароль и идентификационную (ID) карту;
- Для выполнения вышеперечисленных операций **Директору** достаточно войти в ПО Политика пользователей АРМ под своим паролем или при помощи идентификационной (ID) карты;
- Удаление собственной учетной записи или изменение режима **Директор** при работе в данном режиме невозможно.

4. СОЗДАНИЕ УЧЕТНОЙ ЗАПИСИ - ДИРЕКТОР

Первоначально после установки на основной и резервный сервер базы идентификационных данных пользователей – «userpolicy» в ней присутствуют два пользователя:

- **Иванов** – инженер с паролем **qQ111111111#**
- **Петров** – оператор с паролем **aA222222222#**

Как отмечалось ранее **Инженер** (**Иванов**) может создавать и редактировать только **Операторов**, другого **Инженера** он уже создать не может. Для создания и редактирования **Инженеров** и **Администраторов** следует создать учетную запись **Директора**.

Учетная запись **Директора**, позволяющая получить полный контроль над всей системой защиты идентификационных данных пользователей, вводится вручную. Для создания такой учетной записи следует запустить ПО Политика пользователей АРМ (см. п. 5.). Войти в меню команд (см. п. 5.2.). Далее осуществить вход по паролю в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных под учетной записью **Инженера Иванова,** так как описано в п.п. 5.4. Если все сделано правильно, то откроется - «Окно управления безопасностью пользователей», как показано на рис. 4.1.

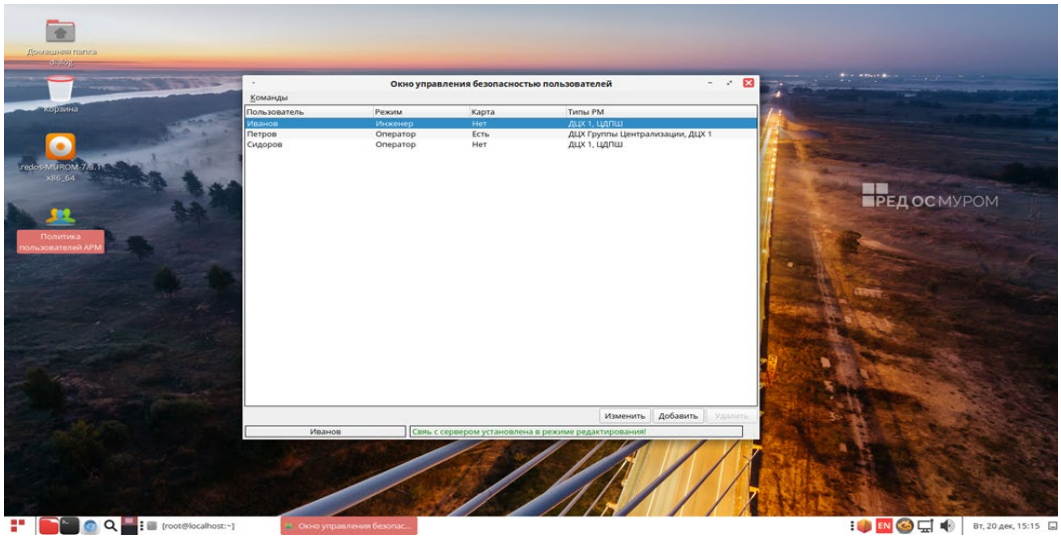


Рис. 4.1.

В этом окне, необходимо нажать на кнопку – «Добавить», расположенную в нижней части окна (см. рис. 4.1.). Далее на экран будет выведено диалоговое окно – «Новый пользователь», как показано на рис. 4.2.

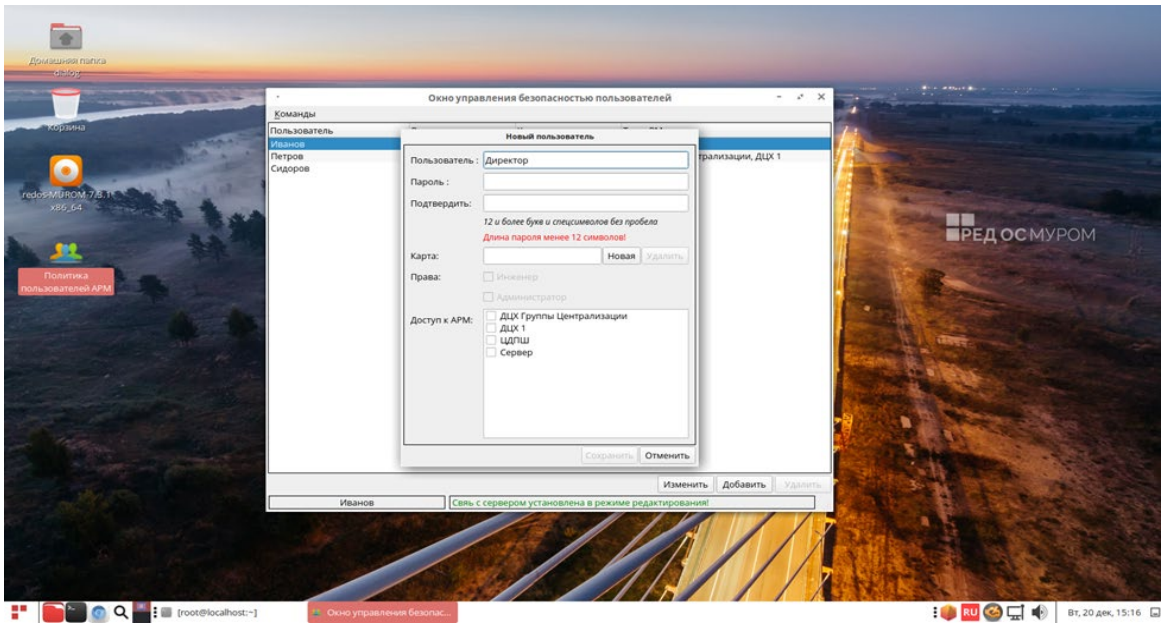


Рис. 4.2.

В этом диалоговом окне в поле – «Пользователь» нужно ввести с клавиатуры – Директор, как изображено на рис. 4.2. и не убирая курсора с этого поля нажать одновременно комбинацию клавишей: левый Shift левый Ctrl левый Alt F12 (все четыре клавиши надо нажать одновременно и отпустить). Если все сделано правильно, то вид диалогового окна на экране станет таким, как на рис. 4.3.

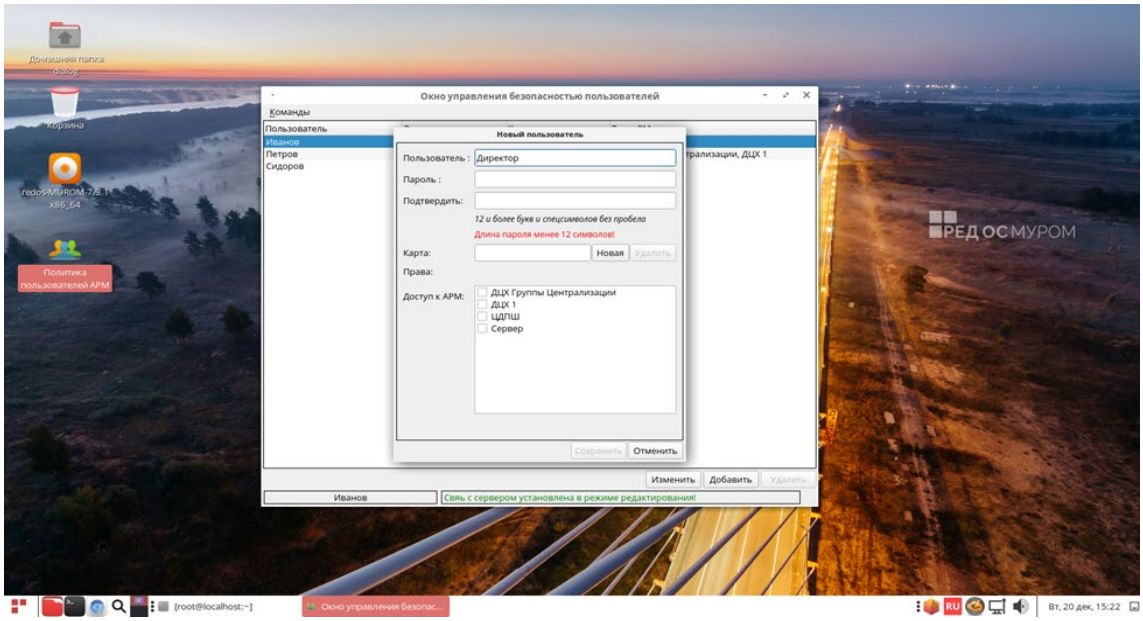


Рис. 4.3.

После этого можно ввести пароль и заполнить другие поля идентификационных данных Пользователя – Директор. Более подробно по заполнению полей см. п.п. 5.7. Если все сделано правильно, то становится доступна кнопка – «Сохранить», как изображено на рис. 4.4.

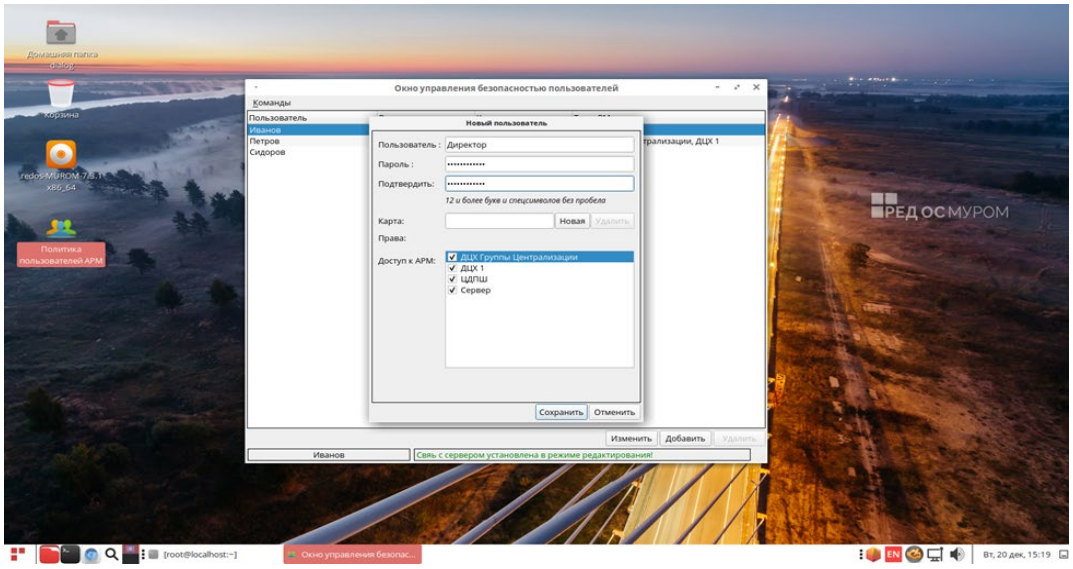


Рис. 4.4.

После нажатия на кнопку – «Сохранить», пользователь – Директор должен появиться в списке пользователей, как изображено на рис. 4.5.

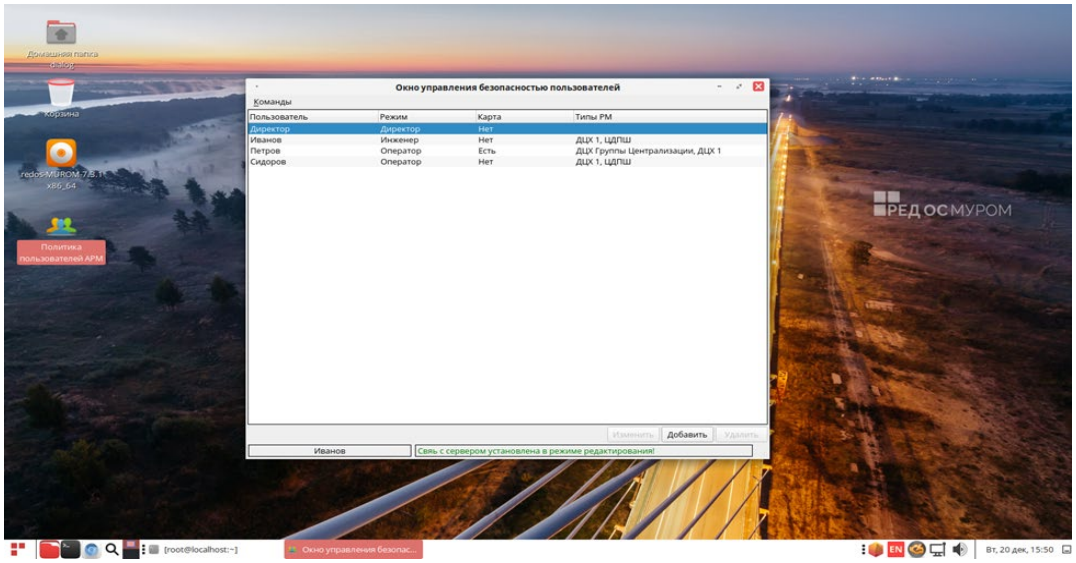
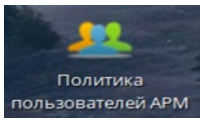


Рис. 4.5.

Теперь если запустить ПО Политика пользователей АРМ и осуществить вход по паролю в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных под учетной записью – «Директор», то появится возможность получить полный контроль над всей системой защиты идентификационных данных пользователей АРМ.

5. РАБОТА С ПО ПОЛИТИКА ПОЛЬЗОВАТЕЛЕЙ АРМ

5.1. Запуск программы

Для запуска ПО Политика пользователей АРМ необходимо осуществить двойной клик левой кнопки мыши по ярлыку запуска 

на рабочем столе, либо ярлык запуска может находиться в нижней информационной строке рабочего стола, как показано на рис. 5.1.1.

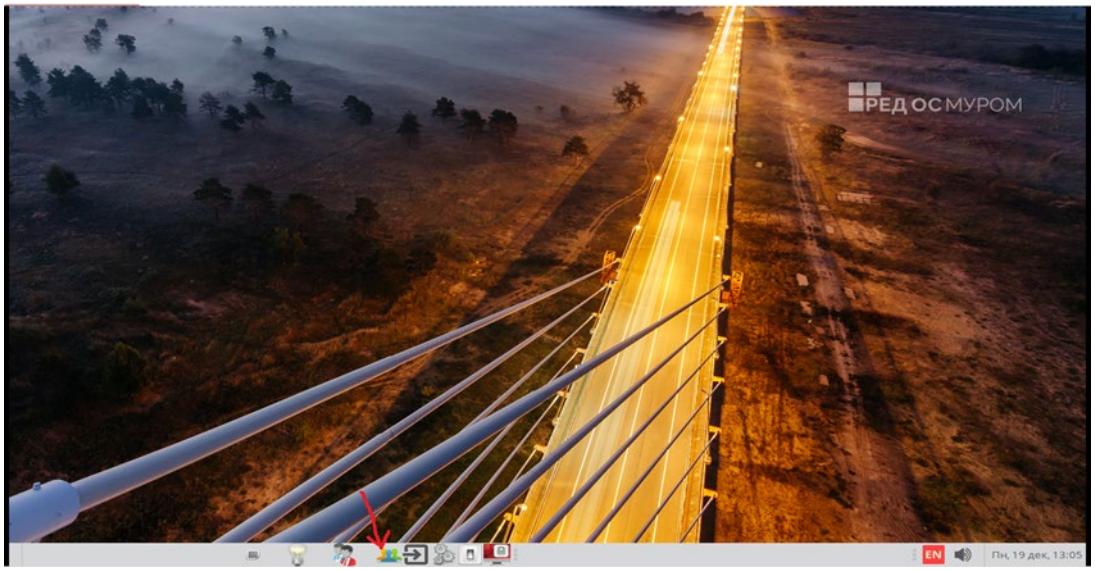


Рис. 5.1.1.

После этого на экране монитора появится главное окно программы – «Окно управления безопасностью пользователей», как показано на Рис. 5.1.2.

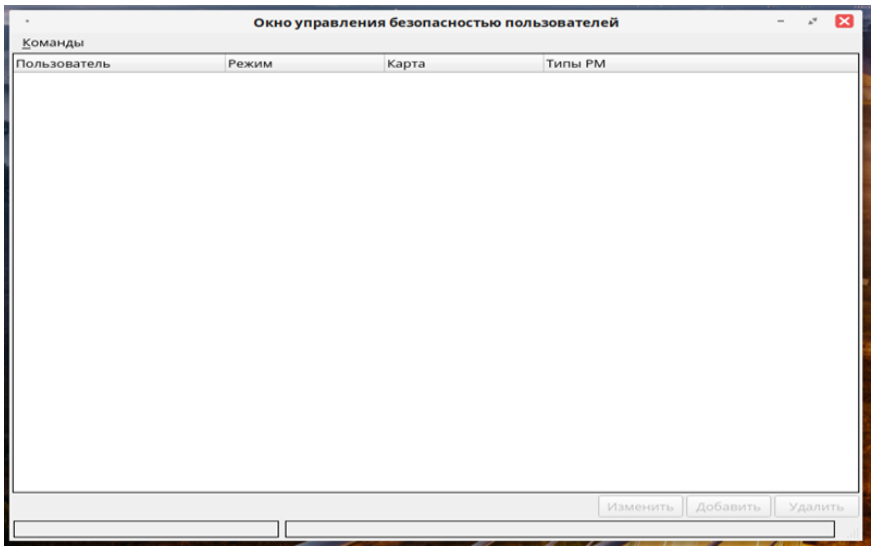


Рис. 5.1.2.

При этом запускается процесс подключения к серверу хранения базы идентификационных данных пользователей – сначала к основному, а при его отсутствии к резервному. Процесс подключения сопровождается мерцанием предупреждающей строки шрифтом красного цвета в нижней части главного окна программы как показано на Рис. 5.1.3:

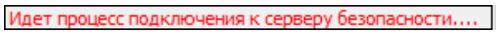


Рис. 5.1.3.

После успешного подключения в нижней части главного окна программы появится строка со шрифтом зеленого цвета - 

как показано на рис. 5.1.4:

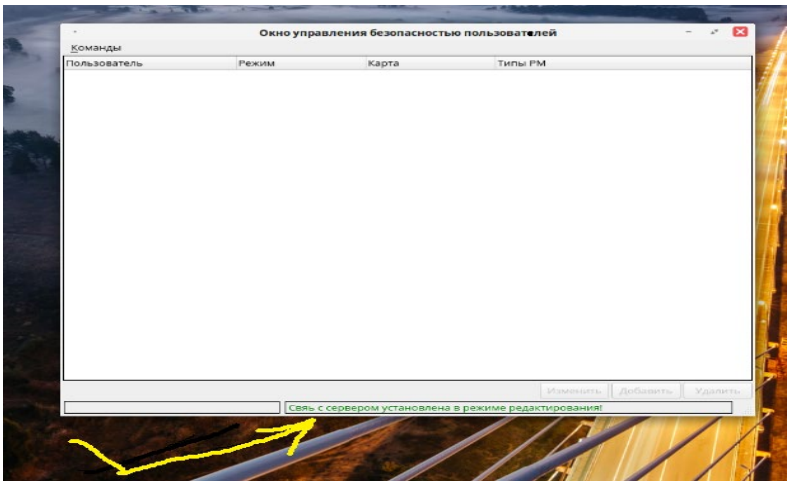


Рис. 5.1.4.

При этом в случае отсутствия сетевого подключения к основному и(или) резервному серверу хранения базы «userpolicy» на экран монитора будет выведено соответствующее предупреждение как показано на Рис. 5.1.5.

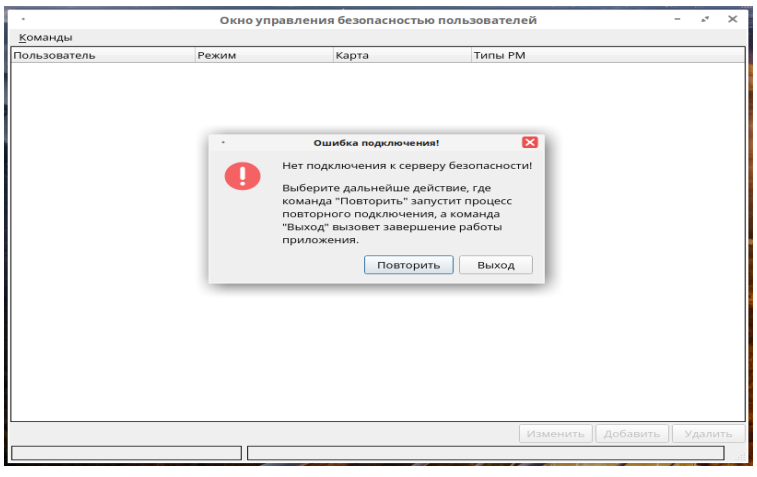


Рис. 5.1.5.

5.2. Вход в меню команд

В случае успешного подключения к серверам (см. рис. 5.1.4) становится доступно меню команд при нажатии левой кнопки мыши на кнопку «Команды», расположенную в левом верхнем углу, как показано на Рис. 5.2.1.

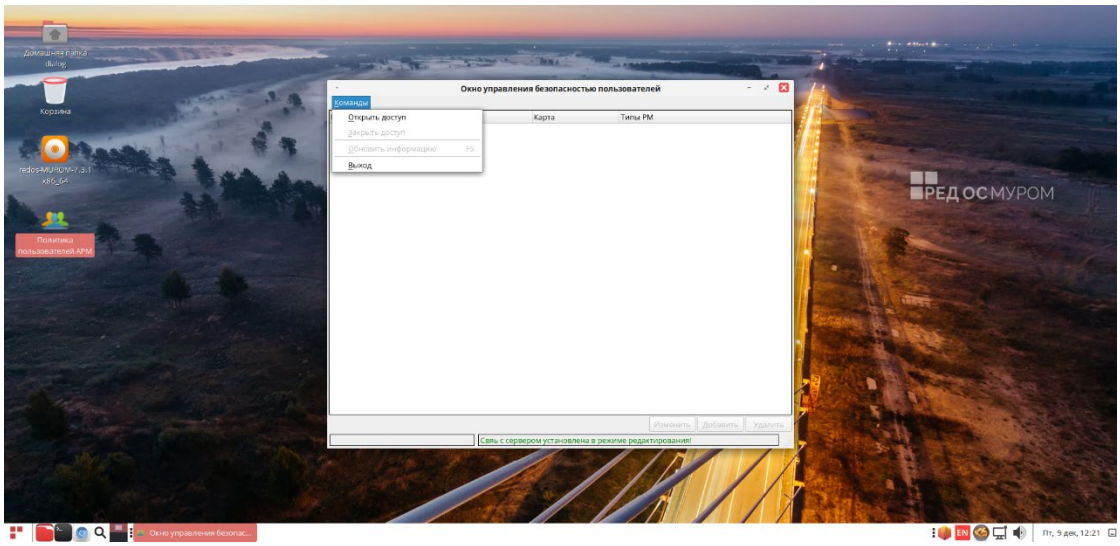
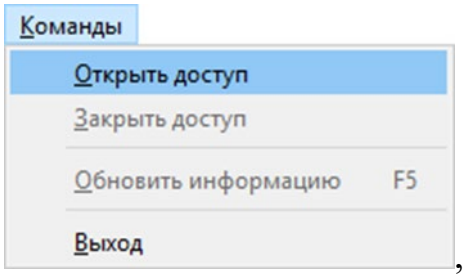


Рис. 5.2.1.

При нажатии на кнопку «Команды» появляется всплывающее диалоговое окно «меню команд» - 

, которое обеспечивает вход в режим просмотра/редактирования идентификационных данных пользователей, при нажатии на кнопку – «Открыть доступ». Также в данном диалоговом окне могут быть доступны другие кнопки в зависимости от состояния, в котором находится ПО Политика пользователей АРМ. Недоступные кнопки диалогового окна подсвечены серым цветом. Для выхода из меню команд достаточно кликнуть левой кнопкой мыши в любое место белого поля главного окна программы.

5.3. Завершение работы с программой

Для выхода из программы и завершения работы необходимо войти в меню команд и в появившемся диалоговом окне нажать на кнопку – «Выход», как изображено на Рис. 5.3.1.

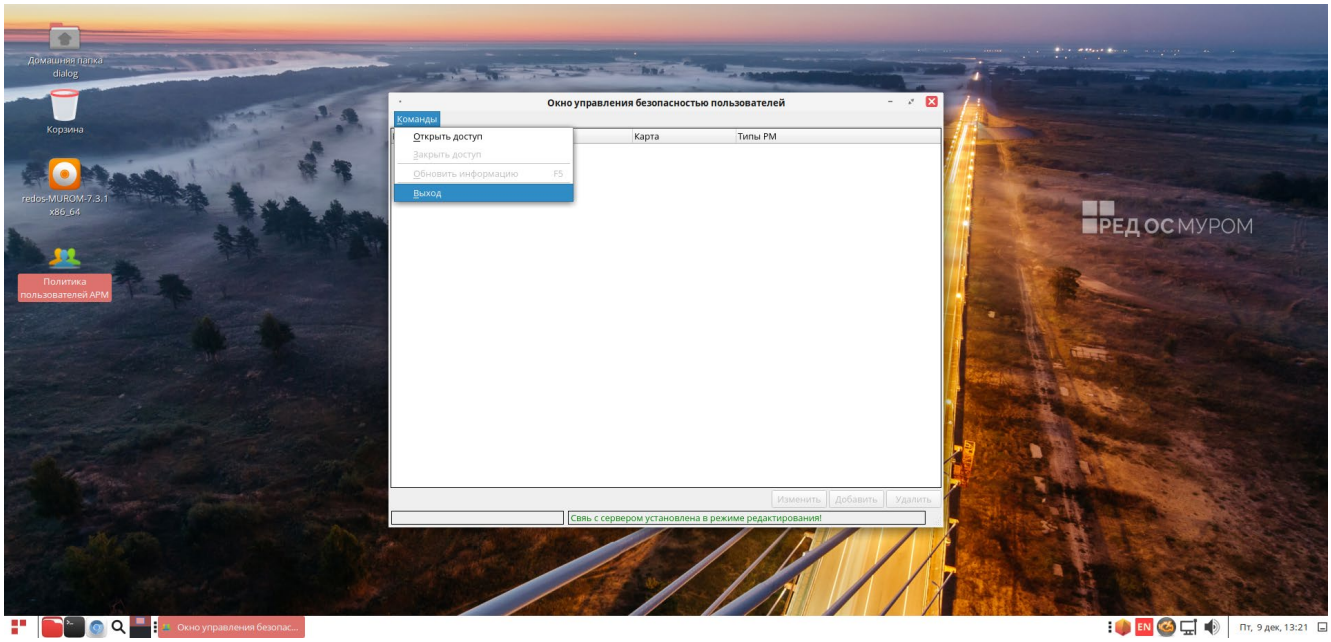


Рис. 5.3.1.

5.4. Вход по паролю в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных

Для входа в режим **добавления, удаления пользователей и изменения/просмотра идентификационных данных** по паролю необходимо войти в меню команд (п.п. 5.2.) и в появившемся диалоговом окне левой кнопкой мыши нажать клавишу – «Открыть доступ», как показано на Рис. 5.4.1.

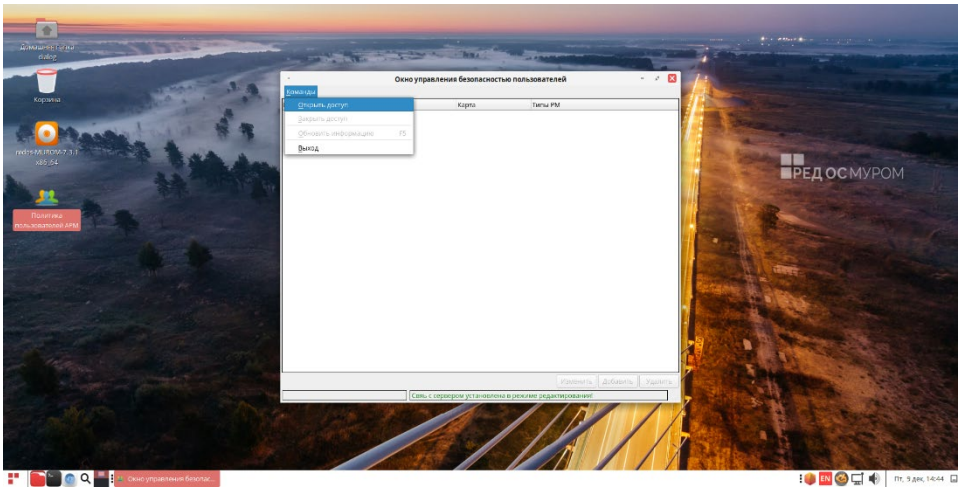


Рис. 5.4.1.

Далее появится диалоговое окно – «Подключить», как показано на Рис. 5.4.2.

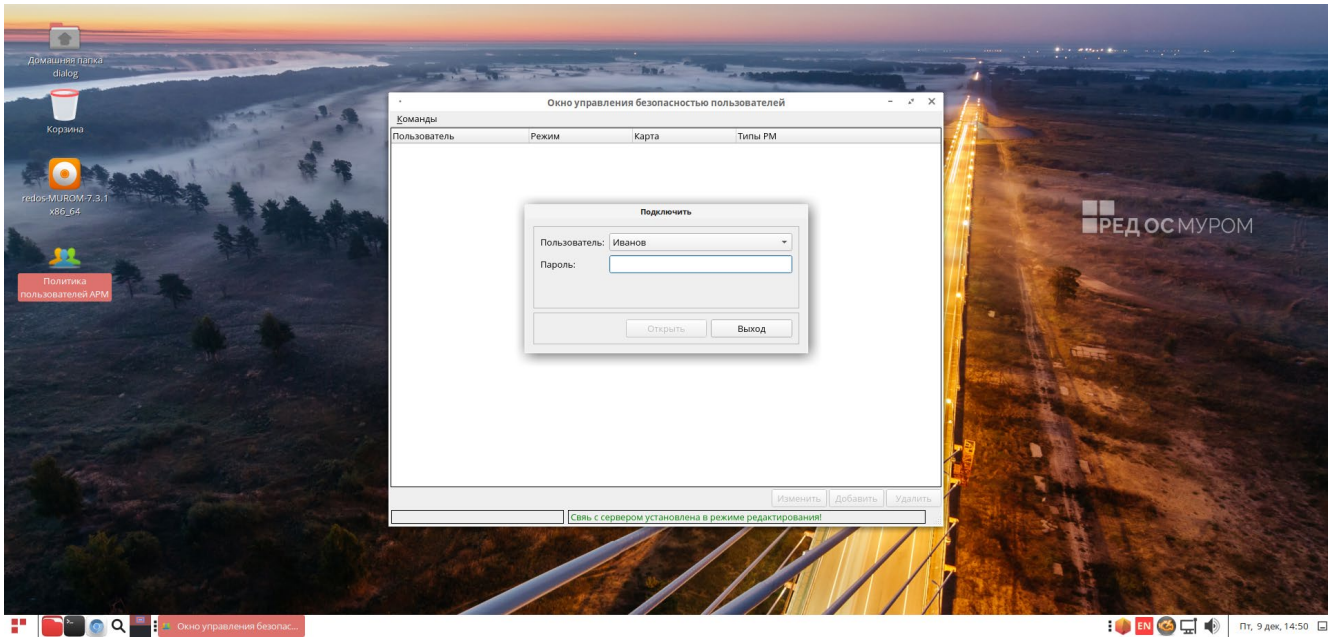


Рис. 5.4.2.

Далее в этом окне в поле справа от надписи - Пользователь необходимо левой кнопкой мыши кликнуть «треугольничек», как показано на Рис. 5.4.3.

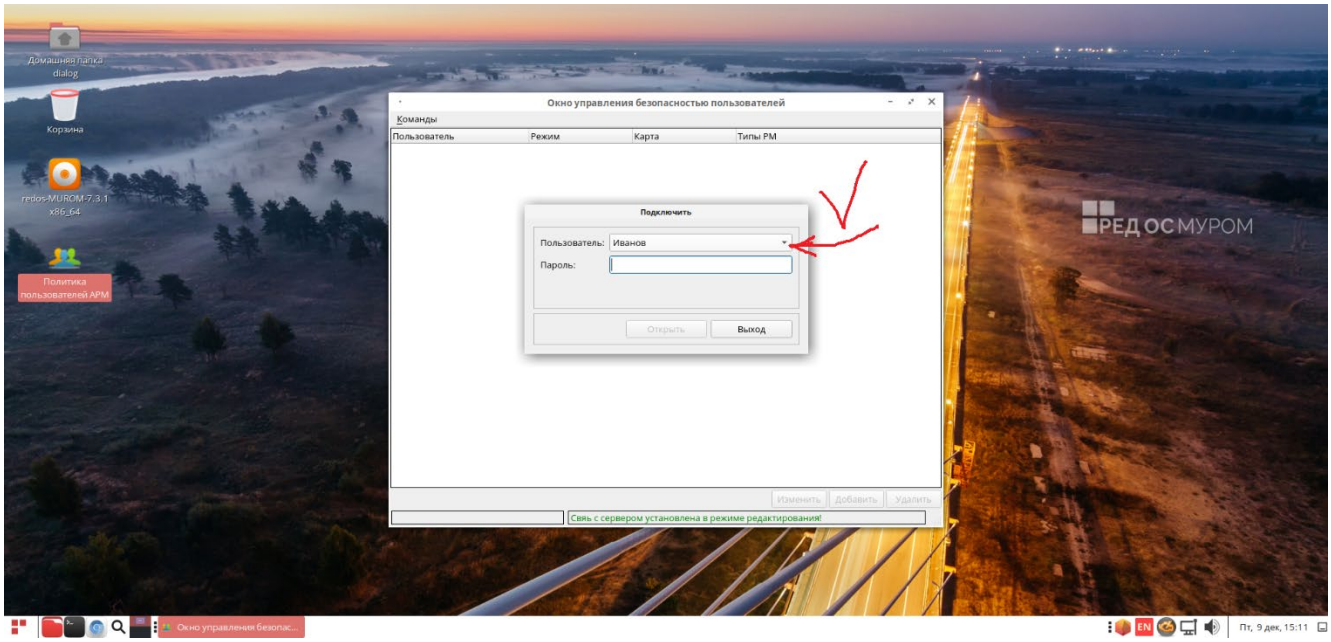


Рис. 5.4.4.

Далее в выпадающем списке следует левой кнопкой мыши выбрать то имя, которое назначено вам как пользователю и переместив курсор в поле справа от надписи –

«Пароль» ввести пароль при помощи клавиатуры. После чего нажать на кнопку «Открыть», как показано на Рис. 5.4.5 для пользователя – Иванов.

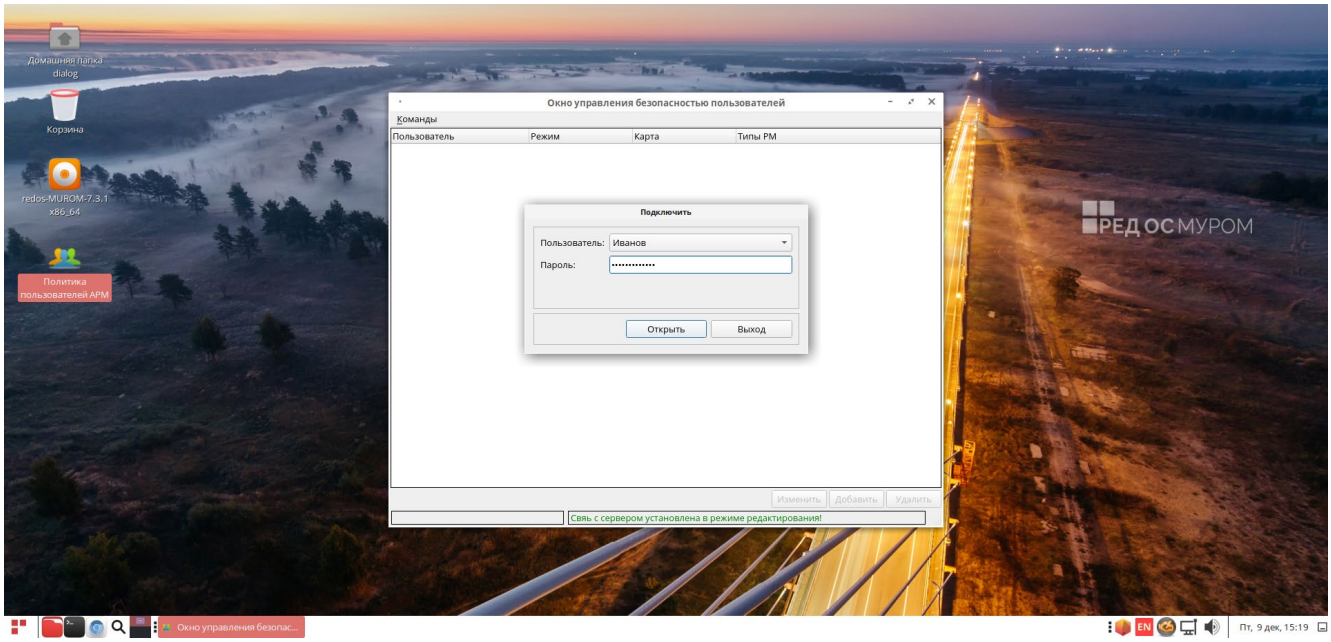


Рис. 5.4.5.

Если пароль введен неправильно будет предложено ввести пароль повторно, как показано на Рис. 5.4.6.

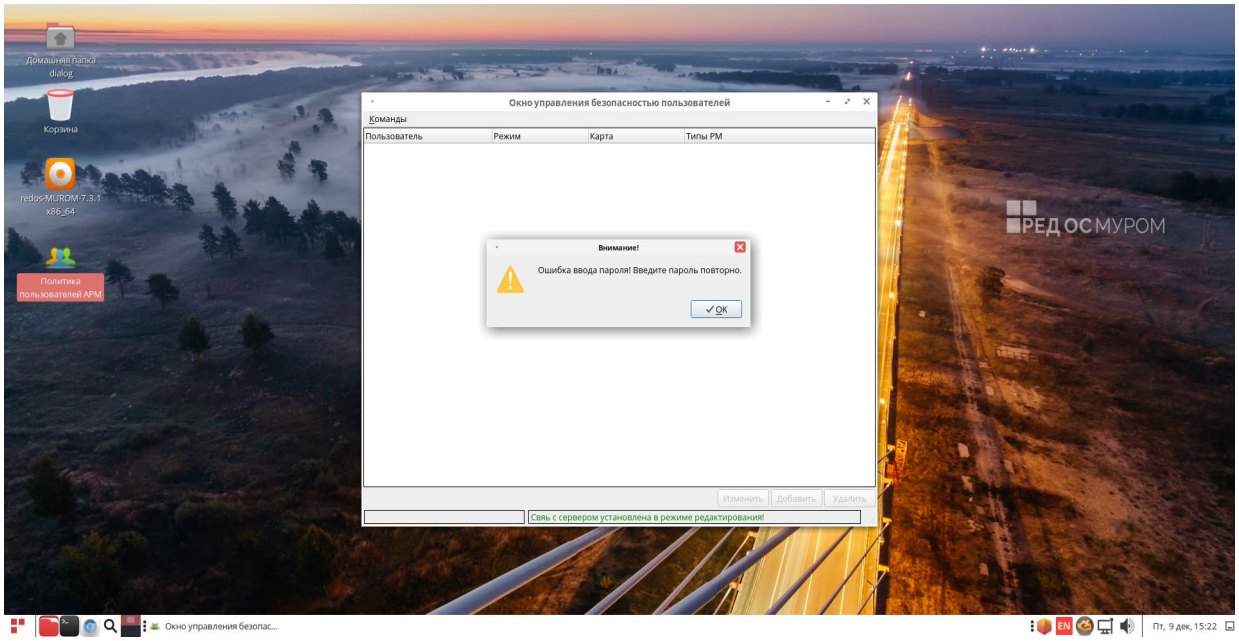


Рис. 5.4.6.

Нажав на кнопку – «ОК», выходим из режима меню команд. Далее можно либо снова повторить действия п. 5.4. либо выйти из программы п. 5.3.

Если пароль введен правильно, .т.е. пользователь с таким именем и паролем присутствует в базе идентификационных данных – «userpolicy», то далее на экране появится – «Окно управления безопасностью пользователей», как показано на Рис. 5.4.7, а в левом нижнем углу окна программы выводится имя этого пользователя.

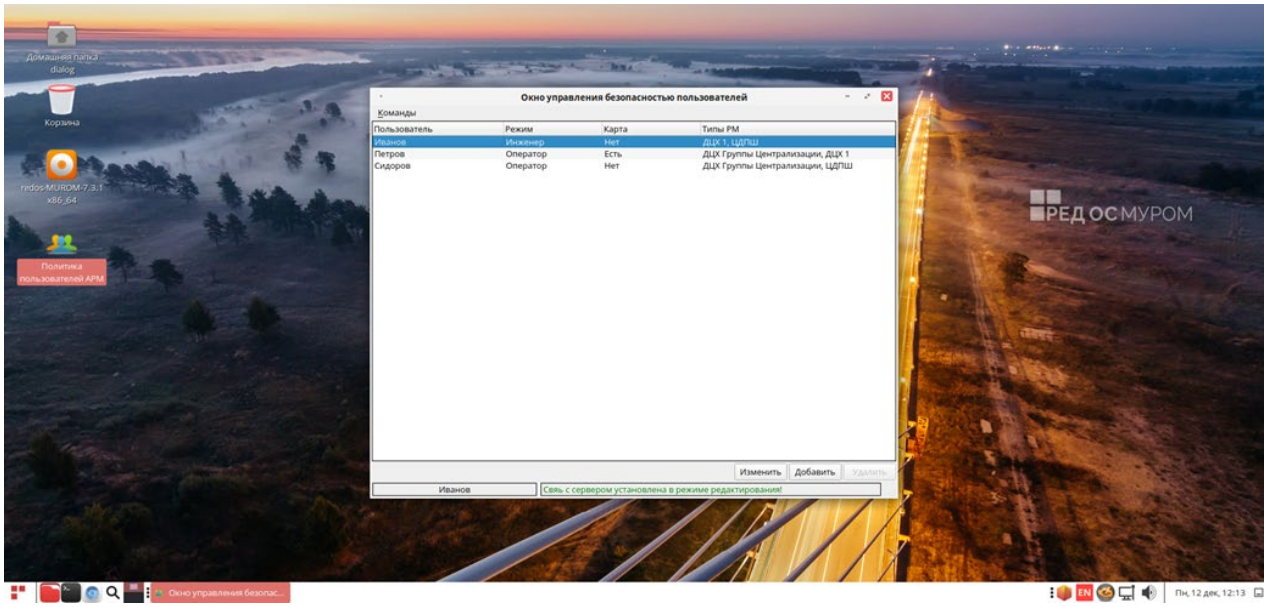
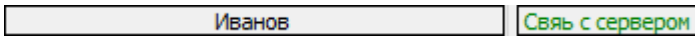


Рис. 5.4.7.

Пример на Рис. 5.4.7. Приведен для входа пользователя – Иванов.



В верхней части окна управления безопасностью пользователей, представлены названия столбцов: Пользователь, Режим, Карта, Типы РМ.

Пользователь	Режим	Карта	Типы РМ
Иванов	Инженер	Нет	ДЦХ 1, ЦДПШ
Петров	Оператор	Есть	ДЦХ Группы Централизации, ДЦХ 1

Где столбец с названием:

Пользователь – содержит имена пользователей АРМ;

Режим – показывает группу, к которой принадлежит пользователь с данным именем;

Карта – показывает есть или нет у пользователя с данным именем идентификационная ID карта;

Типы РМ – показывает типы АРМ, на которых пользователю с данным именем разрешена работа.

При работе в данном режиме в правой нижней части окна управления безопасностью пользователей, появляются кнопки: «Изменить», «Добавить», «Удалить». Причем в зависимости от принадлежности пользователя к определенной группе, часть кнопок может быть недоступна (подсвечены светло-серым цветом), т.к. каждая группа обладает определенным набором прав (см. п. 3). Например, для текущего пользователя – Иванов, (от имени которого произведен вход в данный режим), принадлежит группе **Инженеры**, при наведении курсора на строку – Иванов будут доступны две кнопки: «Изменить», «Добавить». Кнопка «Удалить» будет недоступна, т.к. **Инженеры** не могут удалять сами себя. Если далее навести курсор на строку пользователя – Петров, принадлежит группе Операторы, то становятся доступны все три кнопки: «Изменить», «Добавить», «Удалить», т.к. **Инженер** может удалять **Операторов**, как показано на Рис. 5.4.8.

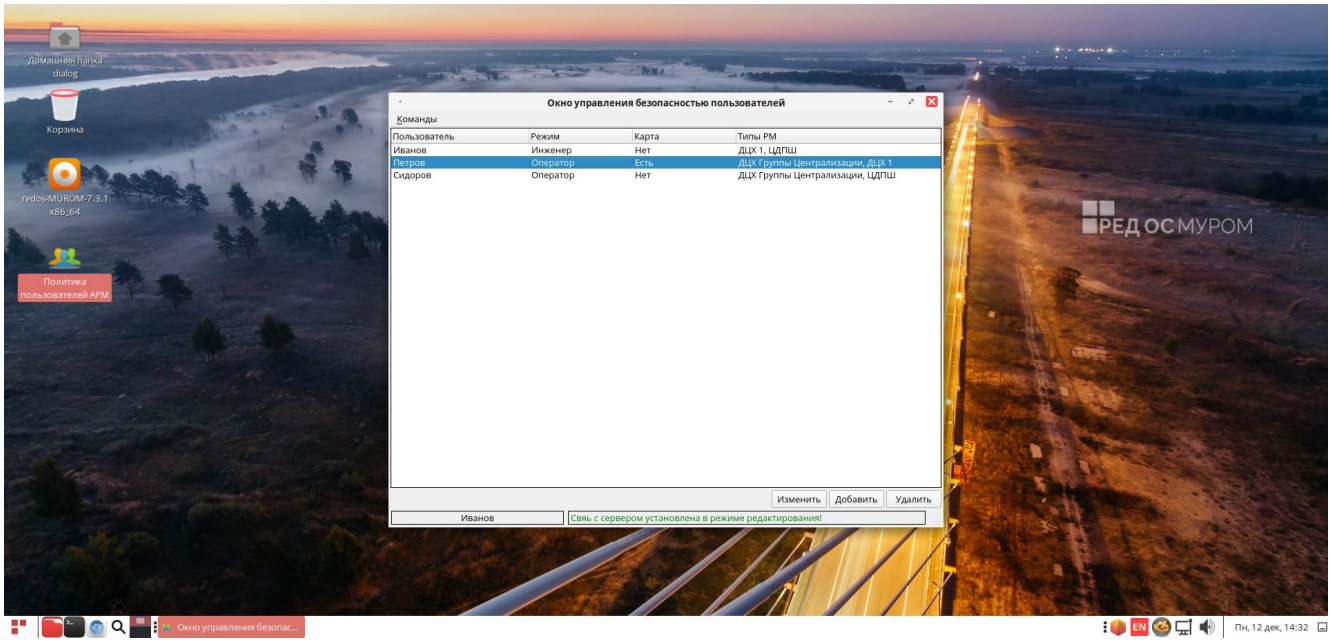


Рис. 5.4.8.

5.5. Выход из режима добавления, удаления пользователей и изменения/просмотра идентификационных данных

Для выхода из данного режима достаточно кликнуть левой кнопкой мыши на кнопку – Команды как показано на Рис. 5.5.1.

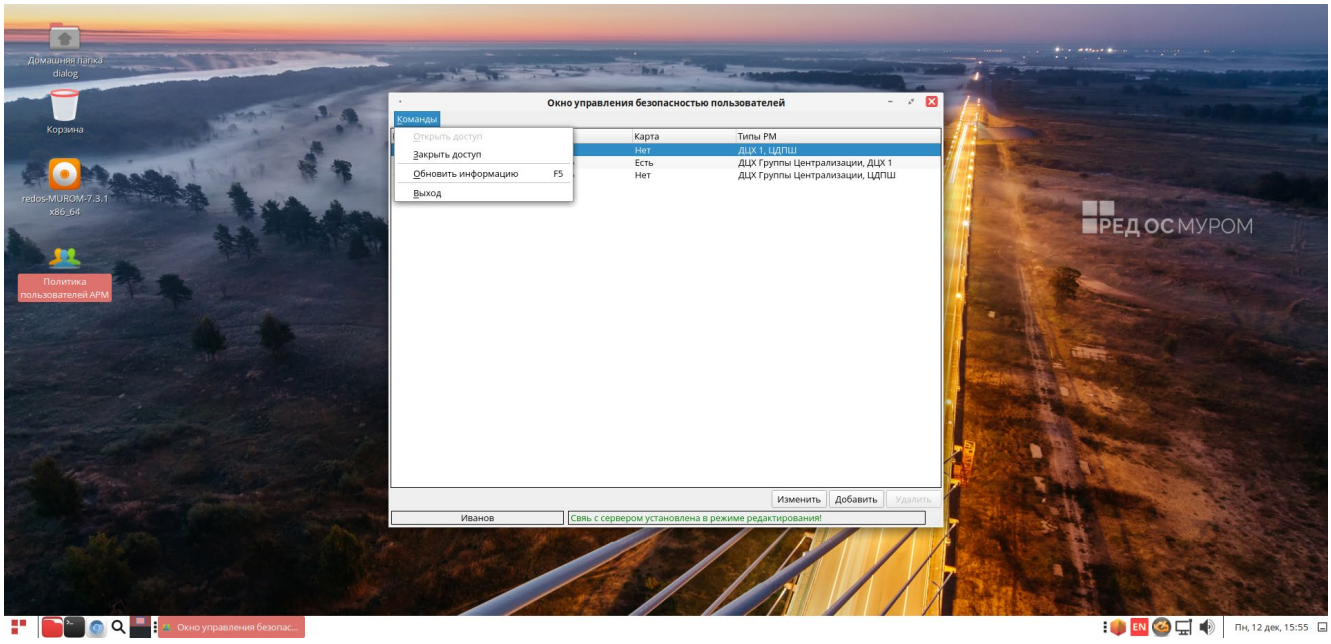


Рис. 5.5.1.

И далее в появившемся диалоговом окне нажать на кнопку - «Закрыть доступ», как показано на Рис. 5.5.2.

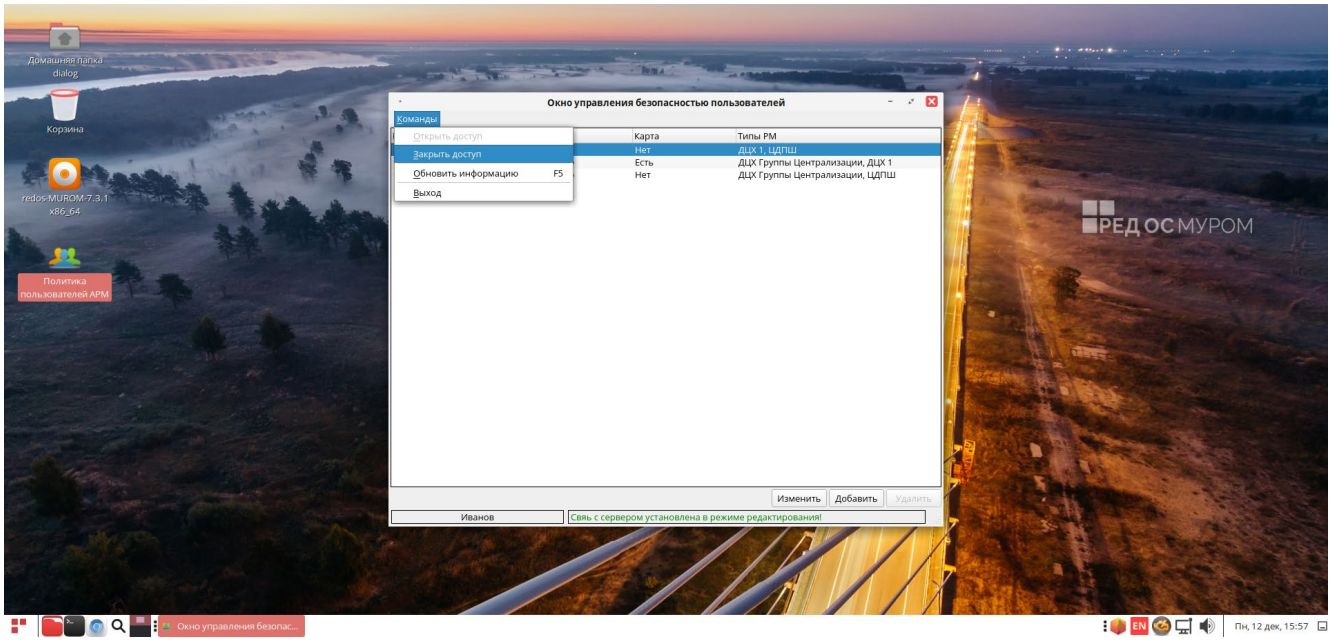


Рис. 5.5.2.

После этого будет осуществлен выход из данного режима и одновременно выход из меню команд (закрытие окна меню команд) и переход в главное окно программы. Вид главного окна после указанных действий показан на Рис. 5.5.3.

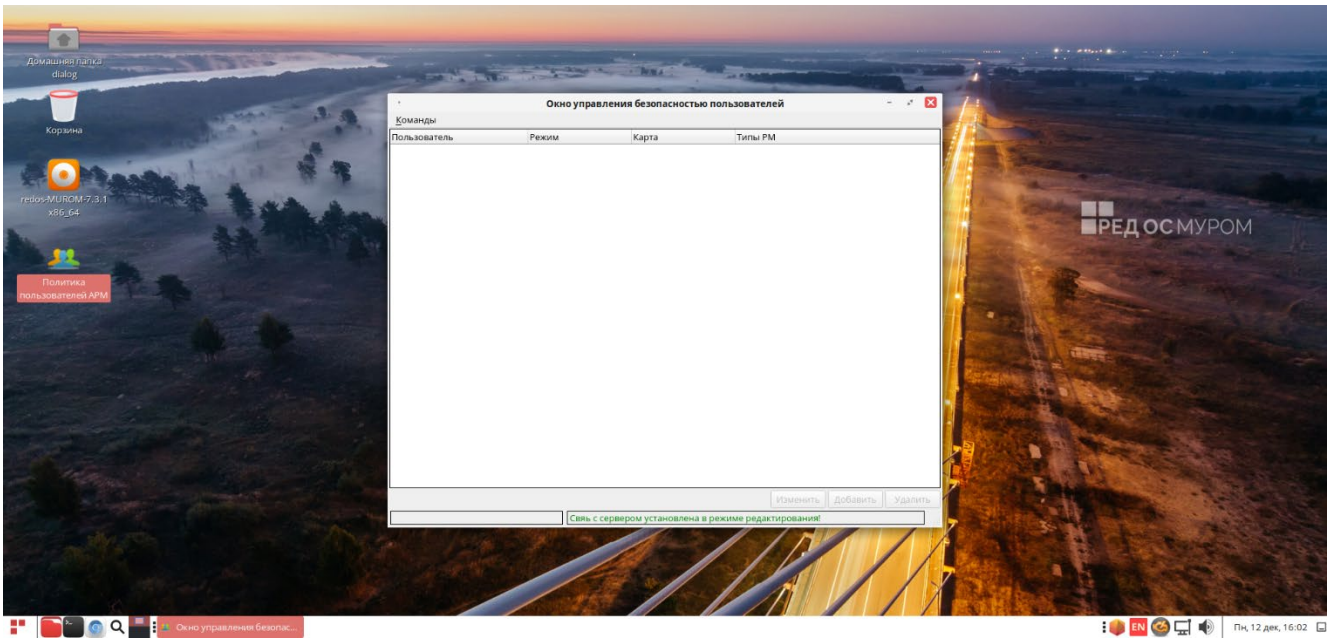


Рис. 5.5.3.

5.6. Вход с применением идентификационной (ID) карты в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных

Для этого нужно, при закрытом меню команд (вид главного окна программы при закрытом меню команд показан на Рис. 5.5.3.) нажать клавишу «Ctrl» на клавиатуре и приложить карту к считывающему устройству (картридеру).

5.7. Добавление нового пользователя

Для выполнения данной операции необходимо войти в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных (см. п.п. 5.4., 5.6.) и при помощи левой кнопки мыши нажать на кнопку – «Добавить», в правом нижнем углу «Окна управления Безопасностью пользователей», как показано на Рис. 5.7.1.

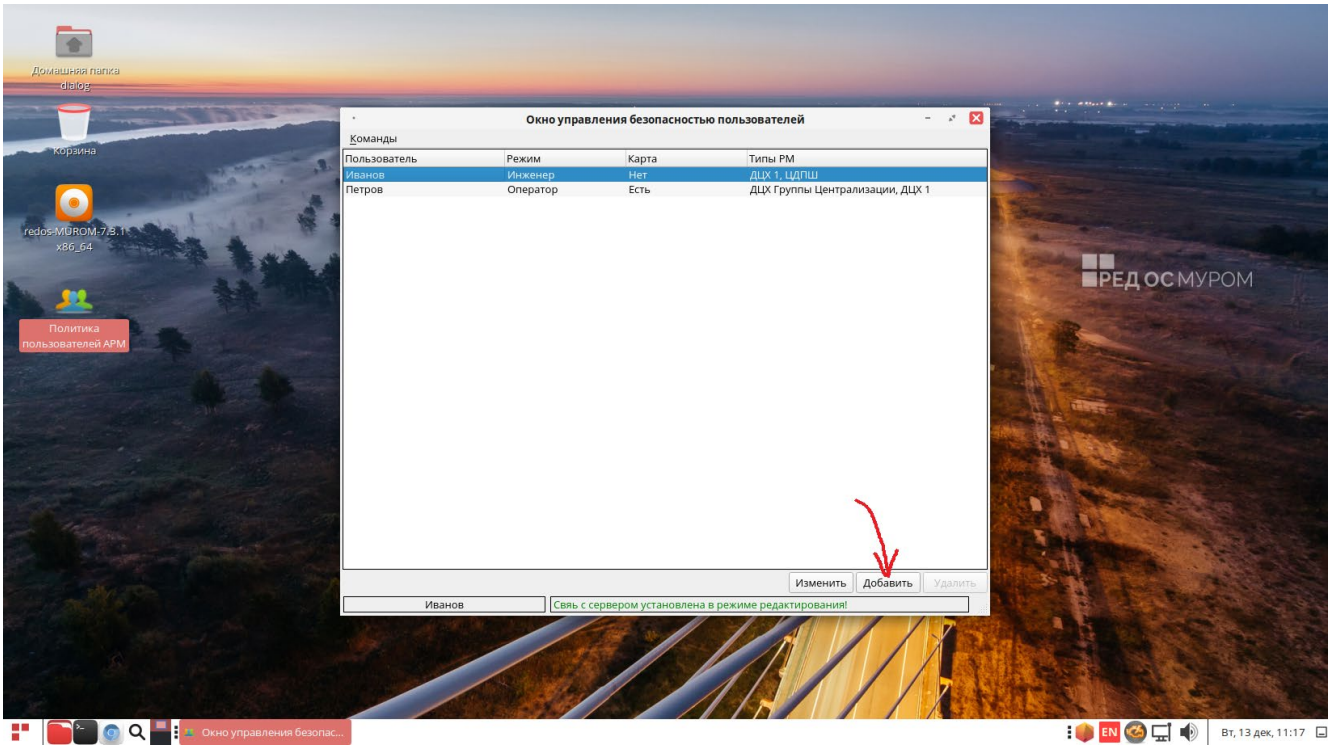


Рис. 5.7.1.

После этого на экран будет выведено окно – «Новый пользователь», как показано на Рис. 5.7.2.

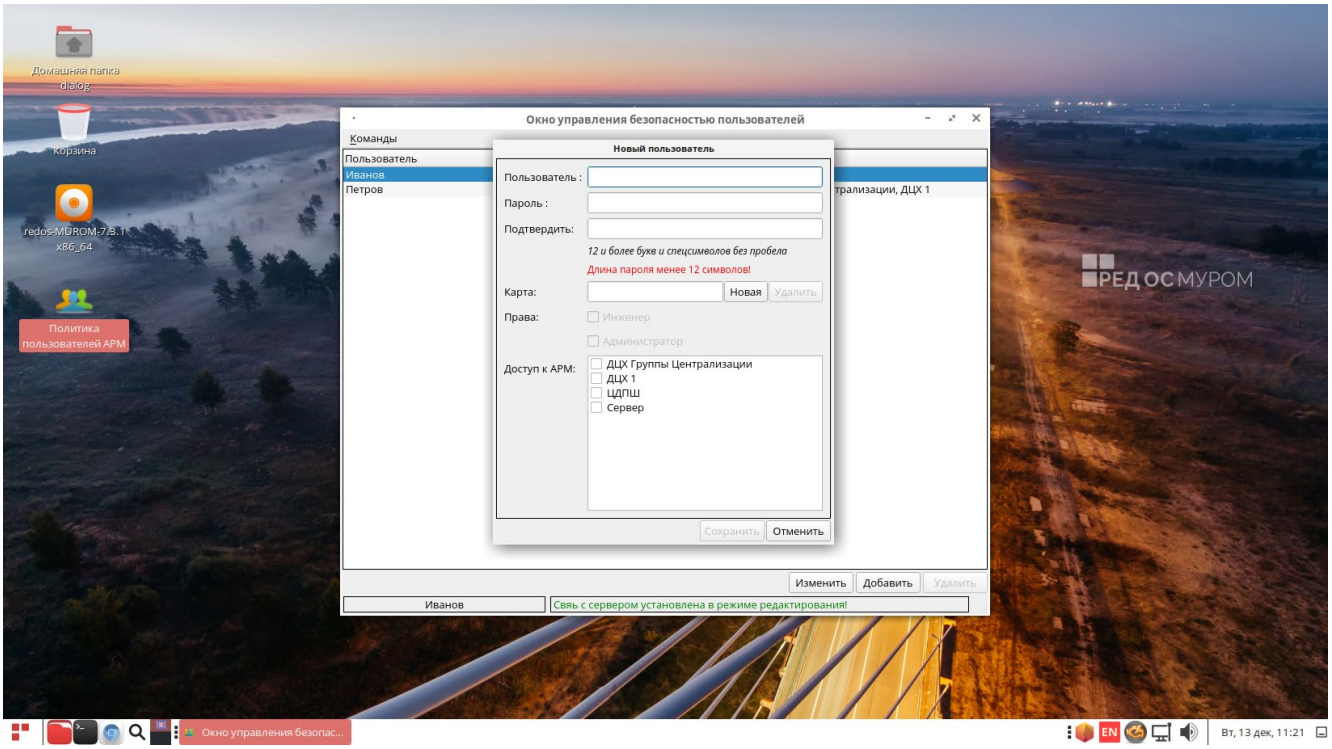


Рис. 5.7.2.

В этом окне становятся доступны следующие поля для ввода идентификационных данных нового пользователя: Пользователь; Пароль; Подтвердить; Карта; Права; Доступ к АРМ.

Ввод идентификационного имени пользователя осуществляется с клавиатуры после установки курсора на свободное поле справа от надписи с названием поля (Пользователь, Пароль и т.п.).

Ниже подробно рассмотрены все эти поля и особенности их заполнения.

- «Пользователь» - идентификационное имя пользователя, под которым данный пользователь может осуществлять вход на АРМ(ы), а также в данную программу - ПО Политика пользователей АРМ. Для упрощения идентификации, можно использовать фамилию сотрудника;

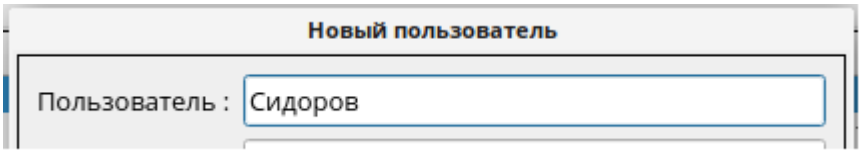


Рис. 5.7.3.

Пример ввода имени пользователя – Сидоров, на Рис. 5.7.3.

- «Пароль» - пароль пользователя, должен содержать буквы (заглавные и прописные), а также спец. символы. Минимальная длина пароля должна быть не менее 12 символов;
- «Подтвердить» - подтверждение введенного пароля. В это поле необходимо ввести пароль пользователя повторно. В случае неверного ввода пароля или его подтверждения выводится сообщение об ошибке:

Пример сообщения об ошибке при вводе пароля на Рис. 5.7.4.

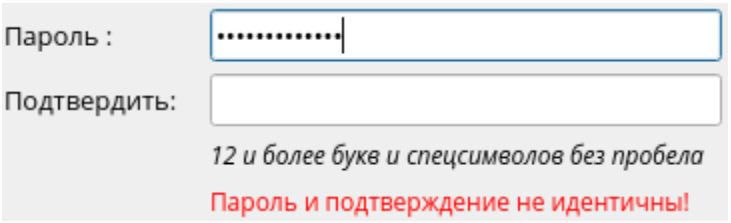


Рис. 5.7.4.

Пример правильного ввода пароля на Рис. 5.7.5. При этом становится доступна кнопка – «Сохранить».

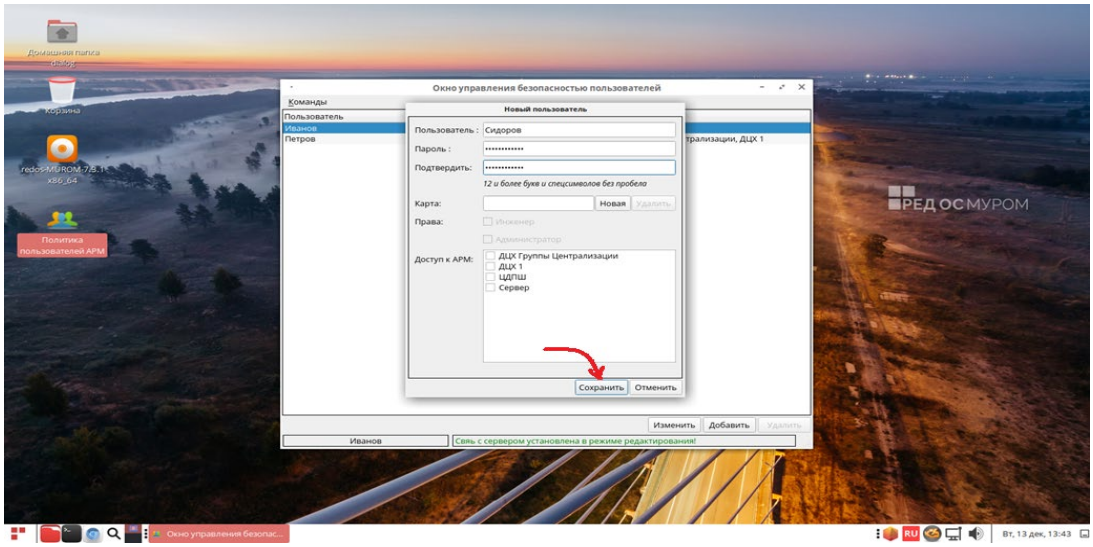


Рис. 5.7.5.

- «Карта» - код идентификационной (ID) карты пользователя при ее наличии.

Для ввода карты следует нажать на кнопку «Новая», при этом появится диалоговое окно – **Карта пользователя**, как показано на Рис. 5.7.6, сообщающее о том, что следует приложить карту к считывателю (картридеру). Для отмены ввода карты нажмите кнопку «Отменить» в диалоговом окне – **Карта пользователя** (Рис. 5.7.6).

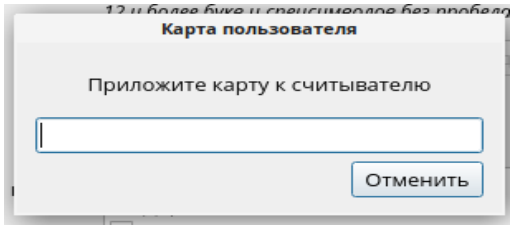


Рис. 5.7.6.

При этом если приложить карту к считывателю (картридеру), то код карты считывается и заносится в поле ввода и диалог автоматически закрывается, а новый код попадает в поле «Карта», как показано на Рис. 5.7.7.

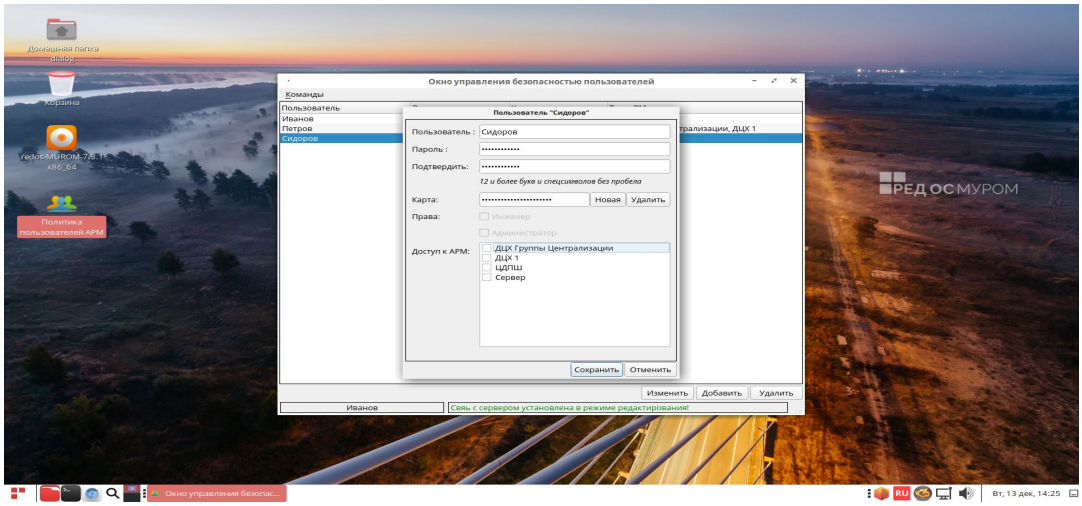


Рис. 5.7.7.

Для удаления уже введенной карты, необходимо нажать на кнопку – «Удалить» в диалоговом окне – **Новый пользователь,** как показано на Рис. 5.7.8.

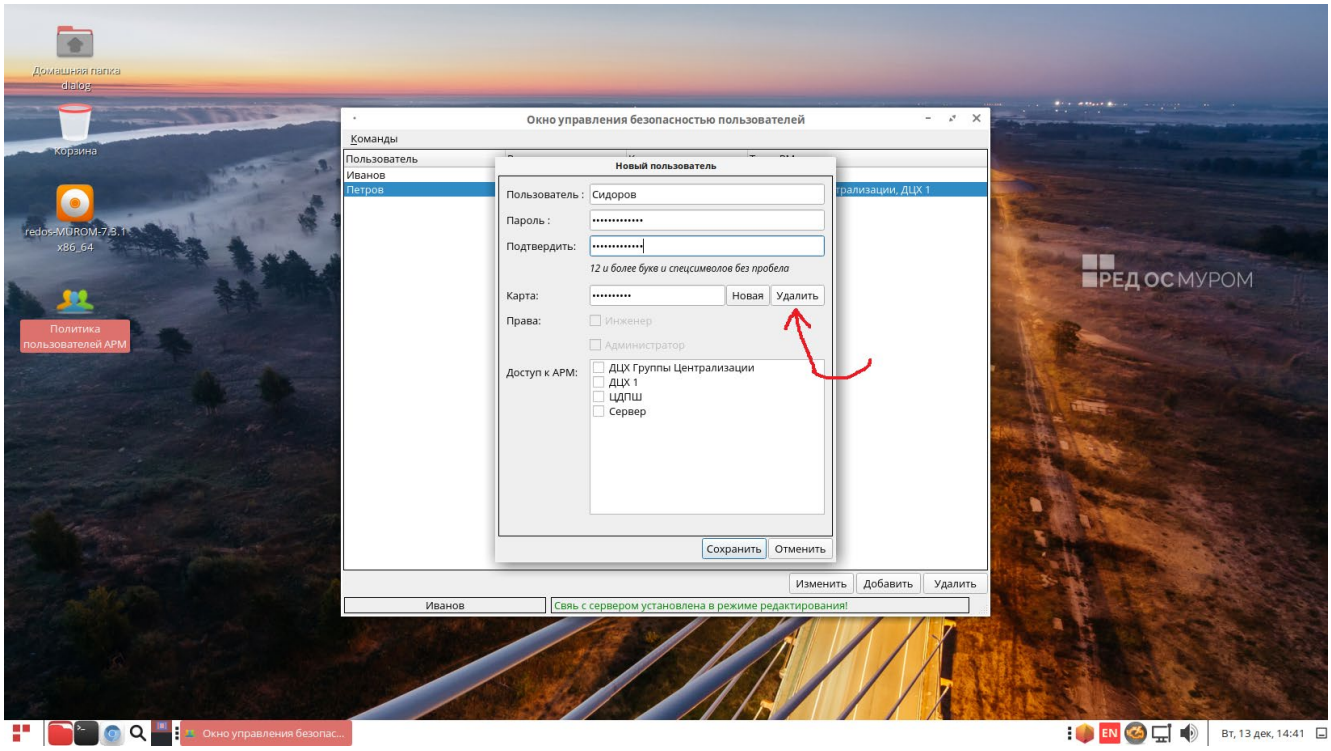
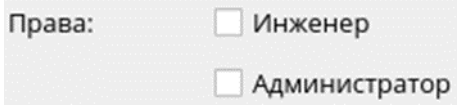


Рис. 5.7.8.

После удаления карты поле – «Карта» должно стать пустым.

• «Права» - Присваивание пользователю набора прав путем прикрепления к определенной группе (Оператор, Инженер, Администратор). Если пользователь от имени которого был осуществлен вход обладает правами Директора, то ему доступны права для ввода данных всех остальных пользователей (см. п. 3.).

Галочка в чекбоксе присваивает пользователю соответствующие права – Инженер или Администратор. Отсутствие галочек означает что данный пользователь Оператор.



Если недоступен ни один из чекбоксов, как на Рис. 5.7.8, то это означает, что был осуществлен вход от имени пользователя с правами Инженер – Иванов, и будет создан новый пользователь – Сидоров с правами Оператор.

- «Доступ к АРМ» - перечень типов АРМов, где галочками помечаются те – доступ к которым возможен для создаваемого нового пользователя, в нашем случае – Сидоров, как показано на Рис. 5.7.9.

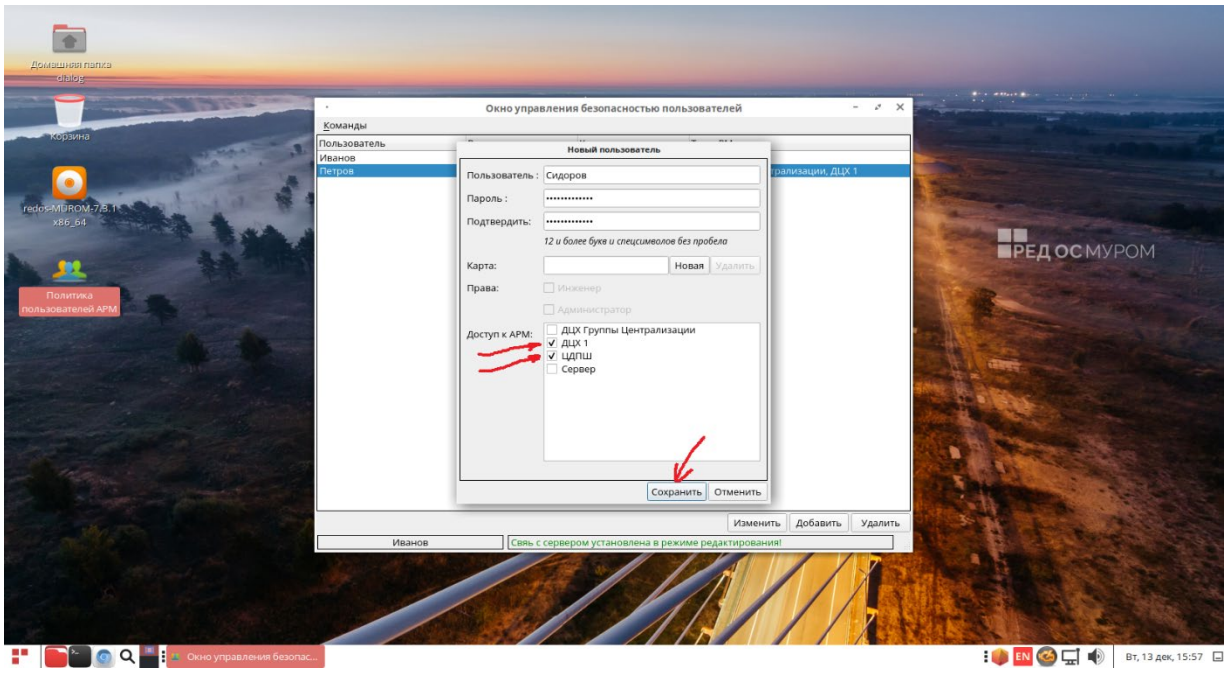


Рис. 5.7.9.

Завершение ввода нового пользователя осуществляется по нажатию кнопки «Сохранить» в нижней части диалогового окна (см. Рис. 5.7.9). Нажатие кнопки «Отменить» приведет к отмене ввода нового пользователя.

После нажатия – «Сохранить», «Окно управления безопасностью пользователей» будет выглядеть как показано на Рис. 5.7.10, пользователь Сидоров (Оператор) будет добавлен в конец списка в соответствии с алфавитным порядком расположения идентификационных имен.

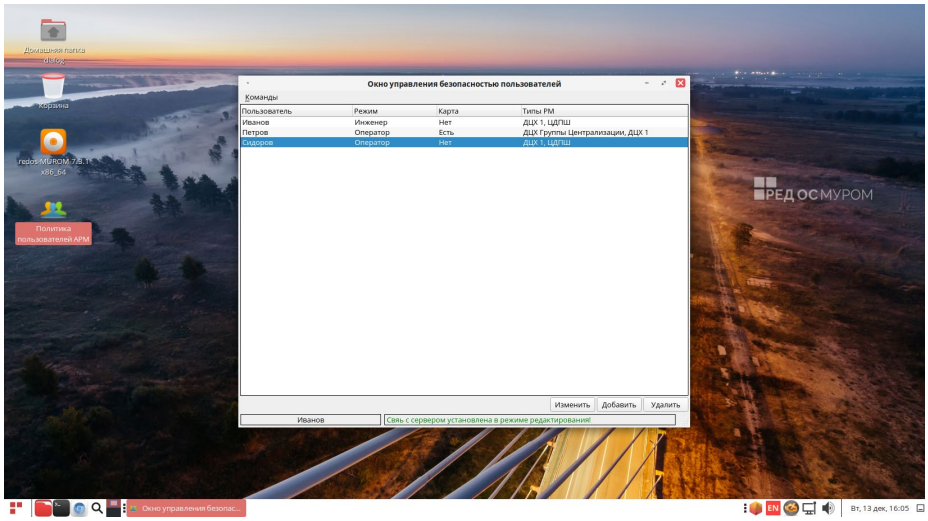


Рис. 5.7.10.

5.8. Удаление существующего пользователя

Для выполнения данной операции необходимо войти в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных (см. п.п. 5.4., 5.6.) и при помощи левой кнопки мыши нажать на строку с пользователем, которого необходимо удалить, строка будет подсвечена синим цветом. Для примера на Рис. 5.8.1 показана ситуация при входе от имени пользователя – Иванов, принадлежит группе – Инженеры. Соответственно кнопка «Удалить» будет доступна только для строк, содержащих Операторов, например – Сидоров. В соответствии с наборами прав пользователей (см. п. 2) Инженеры могут удалять только Операторов и не могут удалять Инженеров и конечно Администраторов и Директора.

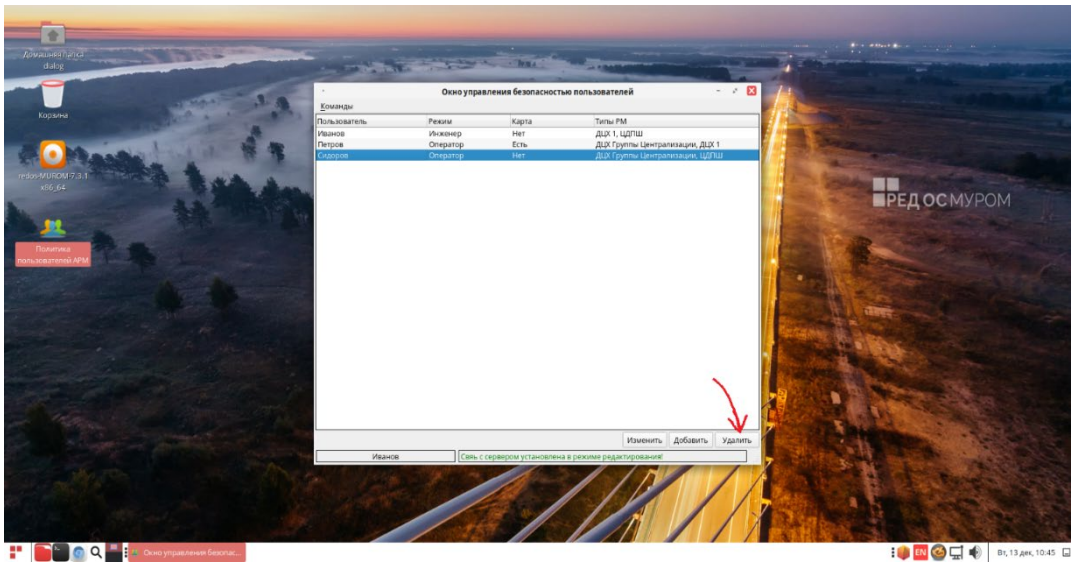


Рис. 5.8.1.

Далее необходимо нажать кнопку – Удалить, в правом нижнем углу «Окна управления Безопасностью пользователей», как показано на Рис. 5.8.1.

Перед окончательным удалением пользователя на экран будет выведено окно – «Внимание» с контрольным вопросом как показано на Рис. 5.8.2.

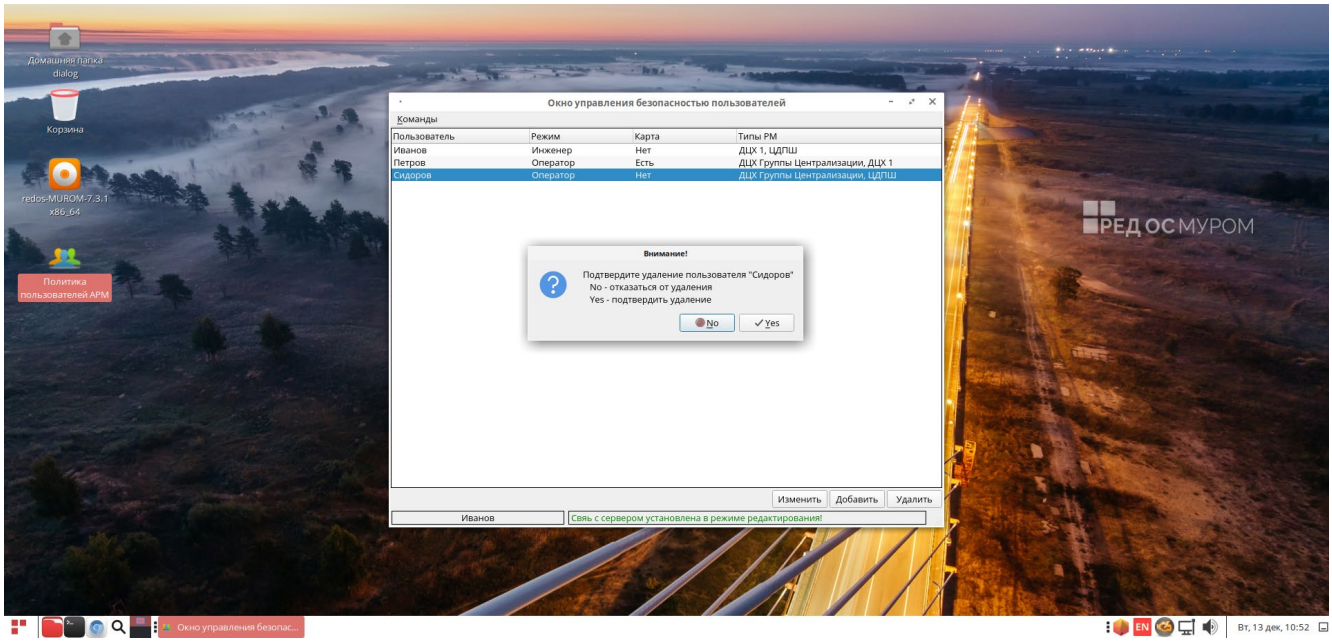


Рис. 5.8.2.

Для удаления нужно нажать на кнопку – Yes, для отмены удаления – No.

При нажатии Yes пользователь удаляется, как показано на Рис. 5.8.3 – строка пользователя Сидоров исчезает из «Окна управления Безопасностью пользователей».

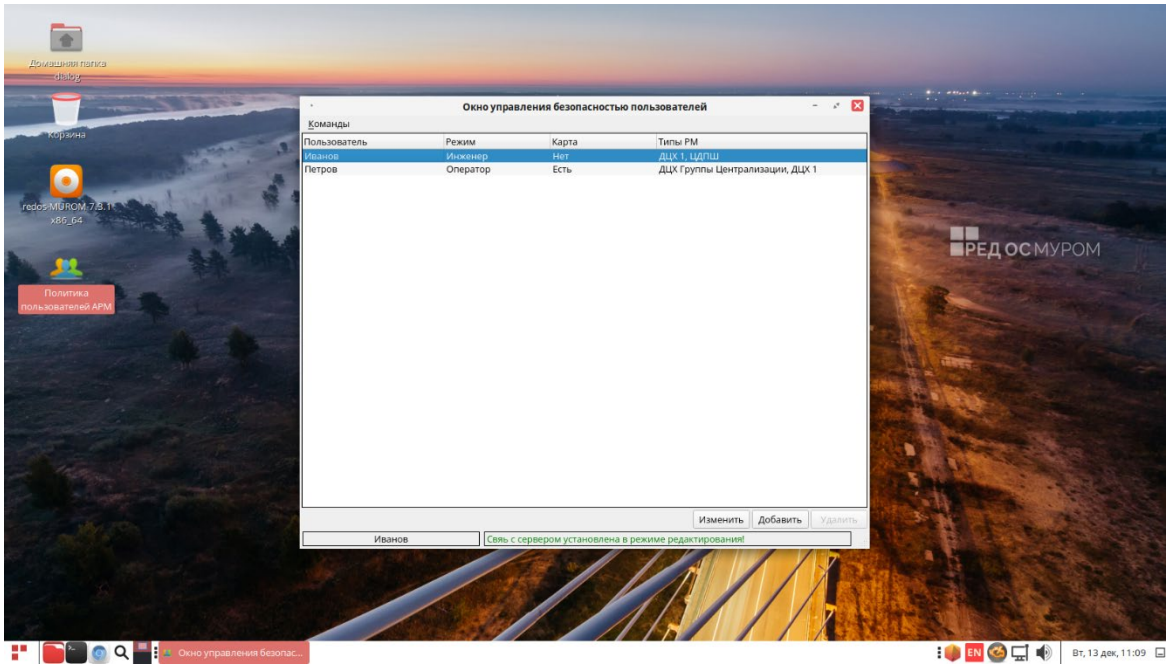


Рис. 5.8.3.

5.9. Редактирование идентификационных данных существующего пользователя

Для редактирования(изменения) идентификационных данных существующего пользователя необходимо войти в режим добавления, удаления пользователей и изменения/просмотра идентификационных данных (см. п.п. 5.4., 5.6.) и при помощи левой кнопки мыши нажать на строку с пользователем, идентификационные данные которого необходимо изменить, строка будет подсвечена синим цветом. Для примера на Рис. 5.9.1. показана ситуация при входе от имени пользователя – Иванов, принадлежит группе – Инженеры, а изменить необходимо идентификационные данные оператора – Сидоров. После этого необходимо нажать кнопку – «Изменить».

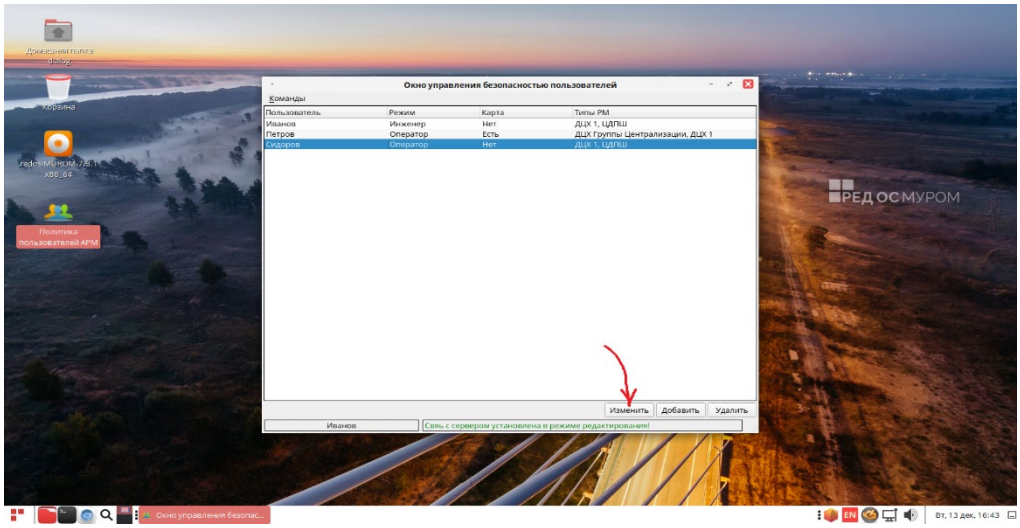


Рис. 5.9.1.

После этого откроется диалоговое окно – Пользователь “Сидоров”, как показано на Рис. 5.9.2 Далее все действия по изменению идентификационных данных пользователя аналогичны действиям по вводу новых значений (см. п.п. 5.7.), при этом кнопка – «Сохранить» становится доступна при изменении или вводе новых значений полей данных.

При этом кнопка «Сохранить» может быть также недоступна в следующих случаях:

- Отсутствует логин пользователя в поле «Пользователь»;
- Пароль не соответствует правилам (12 и более символов и цифр);

- В поле «Подтвердить» введенное значение не соответствует значению поля «Пароль».

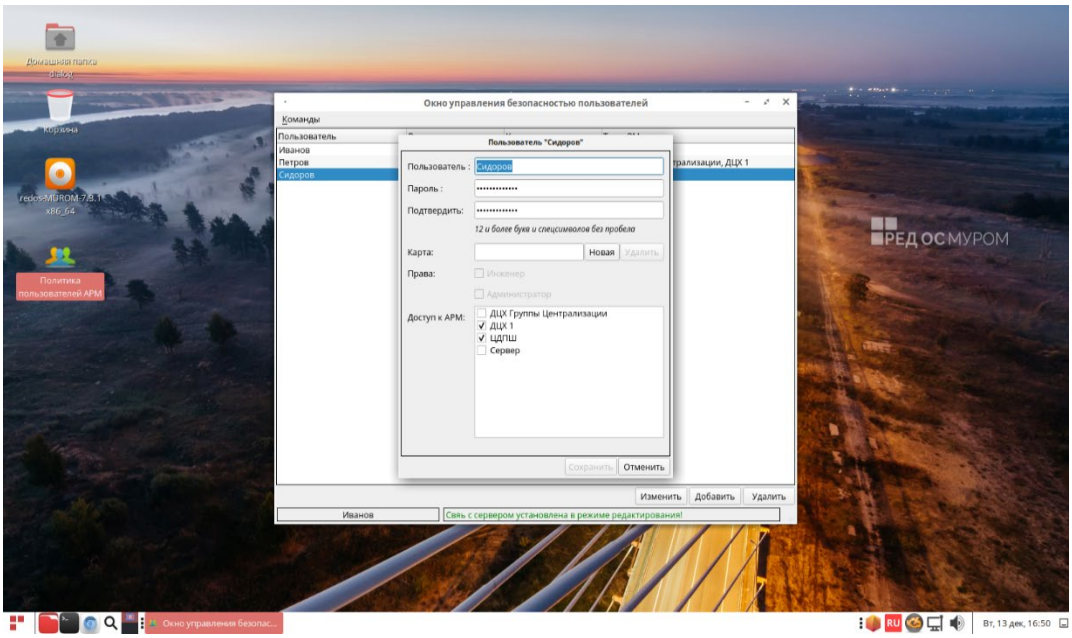


Рис. 5.9.2.

6. СОХРАНЕНИЕ ЗАПИСЕЙ О СОБЫТИЯХ В ЛОГ-ФАЙЛ

В процессе работы с программой информация о действиях пользователя(событиях) сохраняется в виде записей текстовых строк в хронологическом порядке в отдельный файл – так называемый лог-файл (журнал событий). Данный файл имеет фиксированное имя и расположен в определенном каталоге файловой системы - «/var/log/secure». Каждое такое сообщение, в лог-файле, начинается с подстроки «proc.userpolicy», вид лог-файла (журнала событий) в редакторе “nano” изображен на рис. 6.1.

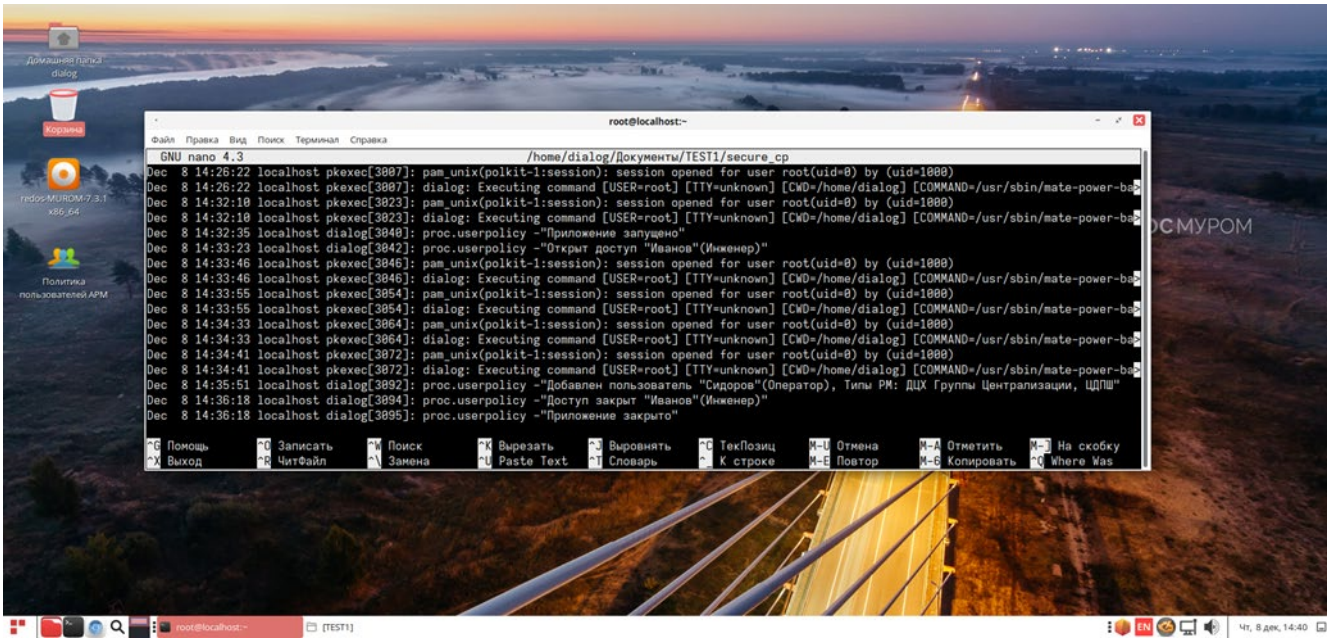


Рис. 6.1.

7. ДЕЙСТВИЯ ПРИ НЕИСПРАВНОСТЯХ ПО

При возникновении неисправностей устройств следует руководствоваться существующими инструкциями.

«Зависание» программы:

Основным признаком того, что программа «зависла» служит статическая картинка основного экрана в течении продолжительного времени. Например, отсутствует реакция программы на попытки выделить курсором мыши отдельные пункты меню программы.

В случае зависания необходимо попытаться штатно закрыть окно программы, если это невозможно, перезапустить стандартным образом операционную систему либо перезагрузить компьютер с помощью кнопки питания.

Если не работает мышь (при перемещении мыши указатель на мониторе не перемещается, при нажатии любой кнопки мыши ничего не изменяется), или *не работает клавиатура* необходимо:

- Проверить отсутствие посторонних предметов на поверхности клавиатуры, наличие разъемов мыши/клавиатуры на своих посадочных местах (в портах системного блока АРМ).
- Проверить надежно ли подсоединены разъемы кабелей подключения мыши/клавиатуры к портам (USB или PS-2) системного блока АРМ. Если работа мыши/клавиатуры не восстановилась, попытаться вынуть разъем кабеля мыши/клавиатуры и подключить в другой свободный порт системного блока.
- Если работа мыши/клавиатуры не восстановилась перезагрузить компьютер с помощью кнопки питания на системном блоке.

Если перезагрузка не помогла, поменять оборудование (мышь или клавиатуру).

Пропало изображение на мониторе:

- Проверить плотность подсоединения сигнальных кабелей в интерфейсных разъемах (HDMI, VGA, D-SUB, Display-port, USB-C) в мониторе и системном блоке.
- Нажать кнопку включения питания на мониторе. Если монитор не включился, проверить плотность подсоединения разъемов питания: монитора АРМ, системного блока (компьютера) АРМ, ИБП АРМ.

Если изображение не появилось либо монитор не включился, заменить монитор.

8. ДЕЙСТВИЯ ПРИ НЕИСПРАВНОСТЯХ ТЕХНИЧЕСКИХ СРЕДСТВ

Нарушениями работы технических средств является:

- выдача заведомо неправильной или полное прекращение выдачи информации на мониторе АРМ;
- длительные прерывистые сигналы блока бесперебойного питания, выдаваемые в течение более 1 мин;
- появление на мониторе АРМ сообщений о неисправностях;

При нарушениях сообщить о неисправности дежурному электромеханику.

Все случаи возникновения нарушений нормальной работы системы регистрируются установленным порядком.

Лист регистрации изменений

	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					