УТВЕРЖДЕН

ЦАУВ.13001-02 34 01-ЛУ

# Серверная операционная система с интегрированными серверными службами МСВСфера 7.3 Сервер

## Руководство пользователя

## ЦАУВ.13001-02 34 01

Версия 1.0

## АННОТАЦИЯ

Настоящее руководство предназначено для пользователей серверной операционной системы с интегрированными серверными службами МСВСфера 7.3 Сервер.

Руководство ориентировано на специалистов, знакомых с операционными системами типа Linux и имеющих минимальный практический опыт работы с ними.

Руководство снабжено иллюстрирующими примерами, сделанными в операционной системе МСВСфера 7.3 Сервер, установленной в полной конфигурации.

## СОДЕРЖАНИЕ

## ВВЕДЕНИЕ

МСВСфера 7.3 Сервер – серверная операционная система на основе ядра Linux с набором интегрированных серверных служб и приложений, включающих: веб-сервер, почтовый сервер, сервер служб сетевой инфраструктуры, серверы файлов и печати, систему резервного копирования и восстановления данных, множество других служб и приложений, а также средства администрирования и защиты информации.

МСВСфера 7.3 Сервер – удобная в использовании операционная система, предназначенная для организации многоцелевых серверов на базе 64-х разрядных аппаратных платформ Intel и AMD. Как правило, она совместима со средствами вычислительной техники, выпущенными в течение последних нескольких лет. Однако, в связи с непрерывным их совершенствованием, в некоторых случаях целесообразно предварительно ознакомиться с соответствующими техническими описаниями и удостоверится в такой совместимости путем пробного тестирования.

В первом разделе настоящего руководства дается описание принципов и правил безопасной работы, возможных ролей пользователей и доступных им средств и интерфейсов, типов регистрируемых событий безопасности, а также действий и режимов работы после сбоев и ошибок. Во втором разделе дается описание процедуры входа в систему, структуры меню, блокировки экрана, завершения сеанса, перезапуска и выключения системы. В третьем разделе описан порядок настройки основных параметров безопасности. В четвертом разделе представлен перечень доступных приложений.

# 1. ОБЩИЕ ПОЛОЖЕНИЯ

## 1.1 Политика информационной безопасности

При реализации технологических процессов обработки данных необходимо руководствоваться принятой политикой информационной безопасности.

Политика информационной безопасности в общем случае должна определять цели, задачи, принципы, правила, а также иные организационные, технологические и процедурные аспекты обеспечения безопасности информации при ее обработке. Она должна являться основой для принятия согласованных управленческих решений и осуществления практических мер, направленных на обеспечение безопасности информации и координации деятельности различных категорий пользователей.

Политика информационной безопасности неразрывно связана с решаемыми задачами и архитектурными особенностями используемых средств и систем автоматизации, должна регламентироваться и обеспечиваться соответствующими положениями, планами, руководствами, инструкциями, методическими указаниями, а также другими организационно-распорядительными и нормативно-методическими документами.

Основной целью обеспечения безопасности информации является предотвращение случайного или преднамеренного несанкционированного вмешательства в процесс функционирования системы или несанкционированного доступа к обрабатываемой в системе информации, что достигается посредством сохранения ее конфиденциальности, доступности, целостности и аутентичности.

Для достижения целей обеспечения безопасности информации необходимо решение целого ряда задач, а именно:

установление организационно-правового режима безопасности, разрешительной системы допуска пользователей к средствам и системам автоматизации;

регламентация процессов обработки информации пользователями, а также действий обслуживающего персонала;

описание пользовательских ролей и доступных им функций и интерфейсов, а также настроек параметров безопасности, типов событий безопасности и действий при наступлении этих событий;

упорядочивание использования параметров идентификации и аутентификации, ограничение сроков действия паролей, определение минимально допустимой длины их значений, состава образующих символов;

разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам, защиту от несанкционированного доступа;

учет информационных ресурсов, регистрацию действий пользователей при использовании информационных ресурсов в специальных журналах и периодический контроль их действий путем анализа содержимого этих журналов;

защита от несанкционированной модификации среды исполнения программ и ее восстановление в случае нарушения;

резервное копирование и восстановление информационных массивов и носителей информации после случайных или преднамеренных воздействий;

контроль целостности используемых программных средств, защиту от вредоносного программного обеспечения;

защита информации, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного доступа или искажения;

контроль функционирования средств и систем защиты информации;

допуск к работе только лиц, прошедших соответствующую подготовку и ознакомленных с должностными инструкциями и эксплуатационной документацией, назначение ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации;

проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработка и реализация предложений по их совершенствованию.

### 1.2 Принципы и правила безопасной работы

Общими принципами организации безопасной работы являются:

принцип ограничения доступа, заключающийся в том, что каждому пользователю предоставляется доступ к информации в соответствии с его функциональными обязанностями;

принцип минимальных полномочий, заключающийся в выделении пользователям наименьших прав доступа к минимуму необходимых информационных ресурсов и функциональных возможностей, которые необходимы для выполнения их функциональных обязанностей;

принцип персональной ответственности, заключающийся в разделении прав между пользователями исходя из их персональной ответственности за совершаемые действия;

принципу непрерывного контроля состояния информационной безопасности и всех событий на нее влияющих;

а также принципы адекватности защитных мер моделям угроз с учетом затрат на реализацию и возможных потерь от осуществления угроз, согласованного комплексного применения различных методов и средств защиты информации для построения целостной системы защиты, эффективности реализации принятых защитных мер, осведомлённости пользователей в вопросах обеспечения информационной безопасности.

Решению вышеперечисленных задач обеспечения безопасности информации может способствовать реализация правил безопасной работы, к которым относятся:

использование механизмов однозначной идентификации пользователей по присвоенным им уникальным идентификаторам;

осуществление управления идентификаторами пользователей: присвоение, блокирование, разблокирование, ограничение срока действия;

использование механизмов однозначной аутентификации пользователей по предоставленным им уникальным параметрам аутентификации;

осуществление управления параметрами аутентификации пользователей: генерация, присвоение, изменение, верификация качества, ограничение срока действия, ограничение количества неуспешных попыток аутентификации;

ассоциация атрибутов безопасности пользователей с процессами, действующими от имени этих пользователей;

использование механизмов идентификации объектов файловых систем при реализации в системе правил управления доступом, контроля целостности, резервного копирования и регистрации событий безопасности, связанных с этими объектами;

использование механизмов управления доступом пользовательских процессов к объектам файловых систем, осуществление возможности задания правил управления доступом, разрешающих или запрещающих доступ субъектов доступа к объектам доступа, а также определяющих разрешенные типы доступа, такие, как создание, модификация и удаление объектов, добавление данных в объекты, удаление данных из объектов, чтение данных из объектов, запуск исполняемых объектов;

использование механизмов ограничения числа параллельных сеансов и контроля доступа в систему с учетом параметров, связанных со временем доступа пользователей в систему, а также своевременного завершения сеанса взаимодействия пользователя с системой по истечении определенного времени бездействия;

использование механизмов очистки остаточной информации в памяти средств вычислительной техники при ее освобождении или блокирование доступа субъектов к

остаточной информации, механизмов изоляции процессов одних субъектов доступа от процессов других субъектов доступа;

использование механизмов резервного копирования объектов файловой системы и компонентов системы, восстановления функциональных возможностей безопасности и настроек параметров системы после сбоев и отказов, сохранения штатного режима функционирования и корректное восстановление штатного режима функционирования при сбоях и ошибках;

использование механизмов контроля целостности программных компонентов системы, а также иных объектов файловой системы, содержащих значения ее параметров, проверка правильности выполнения функций безопасности;

использование механизмов регистрации событий, относящихся к возможным нарушениям безопасности, предупреждения и сигнализации о таких событиях;

использование механизмов контроля установки и запуска компонентов программного обеспечения, ограничения на установку программного обеспечения из недоверенных источников или незадействованного в технологическом процессе обработки информации;

использование механизмов обеспечения доступности информации и сервисов, выделения для них вычислительных ресурсов в соответствии с приоритетами;

использование мер и средств, предотвращающих действия, направленные на нарушение физической целостности средств вычислительной техники, на которых функционирует система.

**1.3 Роли пользователей и доступные им средства и интерфейсы**

Пользователи должны использовать предоставляемые системой возможности в соответствии с возложенными на них функциональными обязанностями. Права пользователей для получения доступа и выполнения обработки информации в системе присваиваются им в соответствии с выполняемыми ролями, отражающими производственные функции и обязанности. Определение ролей позволяет использовать четкие и понятные для пользователей правила разграничения доступа. Каждый пользователь может выполнять одну или несколько ролей, а каждая роль может обладать несколькими полномочиями, разрешенными в рамках этой роли.

Для каждого пользователя должна быть определена сфера его полномочий: программы, которые он может запускать, данные, которые он имеет право просматривать, изменять и удалять. В этом смысле все пользователи системы могут быть условно разделены на две категории: обычные пользователи, выполняющие стандартные пользовательские роли, и администраторы, выполняющие так называемые административные роли.

Обычные пользователи выполняют определенный набор функциональных задач, связанных с обработкой данных и, возможно, контролем работы своих подчиненных, имеют право создавать новые объекты данных, владельцами которых они становятся, и определять порядок доступа к ним других пользователей.

Администраторы, помимо выполнения перечисленных выше задач, выполняют задачи по установке и настройке системы, а также поддержанию ее в работоспособном состоянии, в том числе:

администрирование пользователей, настройка окружения пользователей, управление (создание, редактирование, удаление) пользовательскими учетными записями, их идентификаторами и параметрами аутентификации, управление группами и бюджетами пользователей, управление сеансами доступа пользователей к системе;

администрирование файловых систем, создание монтирование и удаление объектов файловых систем, управление выделяемыми квотами, распределение памяти, управление доступом пользователей к объектам файловых систем, проверка целостности, резервное копирование, архивное хранение и аварийное восстановление объектов файловых систем;

администрирование сервисов, планирование выполнения процессов, мониторинг выполнения процессов, регистрация и аудит событий безопасности.

Для выполнения обозначенных выше задач пользователям и администраторам системы предоставляются соответствующие средства, часть из которых описана в руководстве администратора, а часть в настоящем руководстве пользователя. При попытке с помощью какого-либо средства сделать что-то, выходящее за рамки его полномочий, пользователь может сначала получить запрос подтверждения полномочий, необходимых для выполнения запрошенного действия, а затем сообщение об ошибке или отказе в доступе при невозможности такого подтверждения.

Пользовательский интерфейс некоторых предоставляемых системой средств является графическим, интуитивно понятным, использующим окна, меню, списки выбора, поля ввода, кнопки, ориентированным на взаимодействие с помощью клавиатуры и мыши. Пользовательский интерфейс других средств является так называемым консольным, ориентированным на взаимодействие в терминальном режиме с помощью командной строки, задающей команды и дополнительные параметры, результаты выполнения которых выводятся в виде текстовых сообщений.

### 1.4 Типы регистрируемых событий безопасности

В системе реализована регистрация событий, касающихся обеспечения безопасности, в том числе:

событий и результатов идентификации и аутентификации пользователей, начала и завершения сеансов их работы в системе;

событий, связанных с истечением установленных сроков действия идентификаторов и параметров аутентификации пользователей;

событий, связанных с попытками и результатами получения доступа к объектам файловых систем;

событий, связанных с успешным или неуспешным запуском пользовательских процессов и их завершением;

событий, связанных с созданием, модификацией и удалением объектов файловых систем;

событий контроля и нарушения целостности программной среды и обрабатываемых данных:

событий, связанных с фильтрации информационных потоков;

событий, связанных с запуском и завершением выполнения функции регистрации событий безопасности, других событий.

Для всех регистрируемых событий безопасности генерируются соответствующие записи, помещаемые в специальный журнал регистрации событий безопасности (журнал аудита), в которых фиксируются:

дата и время события;

тип и результат события;

идентификатор пользователя, с которым связано событие;

другие параметры, зависящие от типа события.

Для удобной работы с журналом аудита в системе имеются средства, позволяющие осуществлять поиск, просмотр, фильтрацию и упорядочение записей регистрации событий безопасности, а также периодическое или по запросу формирование необходимых отчетов.

Средства регистрации событий безопасности обеспечивают возможность включения и исключения событий в совокупность событий, подлежащих регистрации, защиты хранимых записей регистрации событий безопасности от несанкционированного удаления и модификации; возможность выполнения действий, направленных на сохранение данных журнала регистрации и обеспечивающих непрерывность процесса регистрации при превышении журналом регистрации определенного размера.

### 1.5 Действия и режимы работы после сбоев и ошибок

В процессе эксплуатации системой ведутся журналы регистрации сбоев и ошибок, возникающих при запуске и выполнении программ.

В них фиксируются случаи обнаружения отсутствия объектов файловой системы при попытках доступа к ним по идентификаторам, случаи сброса (отказа) в соединении при попытке обращения к сервису, который не запущен или недоступен, случаи обнаружения ошибок в синтаксисе или параметрах выполняемых команд, а также события, связанные с другими сбоями и ошибками.

При возникновении сбоев и ошибок во время эксплуатации системы необходимо принять меры к устранению их причин на основе информации, содержащейся в системных журналах регистрации сбоев и ошибок. Если это не даст положительный результату, рекомендуется осуществить принудительный перезапуск системы. Если и принудительный перезапуск не поможет устранить сбой и сохранить работоспособность системы, то следует обратиться к администратору, который может предпринять попытки запуска системы в режиме восстановления или в аварийном режиме.

Режим восстановления может оказаться полезным в ситуациях, когда система не может нормально загрузиться, а также, когда необходимо выполнить действия по восстановлению важных данных. Режим восстановления позволяет загрузить минимальное окружение системы с имеющегося (приобретенного ранее) инсталляционного носителя. В режиме восстановления все локальные файловые системы будут примонтированы и некоторые основные службы будут запущены. Это может обеспечить доступ к находящимся на жестком диске объектам файловой системы с целью их копирования или внесения корректирующих изменений.

В аварийном режиме система загружается с минимальным окружением и монтирует корневую файловую систему только для чтения, при этом она не монтирует другие локальные файловые системы и не активирует сетевые интерфейсы.

# 2 ВХОД, ПЕРЕЗАПУСК И ВЫКЛЮЧЕНИЕ СИСТЕМЫ

## 2.1 Вход в систему

Вход пользователя в систему начинается с идентификации и аутентификации, в ходе которых он выбирает свое имя из предлагаемого системой списка имен зарегистрированных пользователей и предъявляет пароль.

При предъявлении пользователем пароля вместо вводимых с клавиатуры значений на экране будут отображаться маскирующие символы. Если пользователь введет неверный пароль, то ему будет выдано на экране соответствующее сообщение и потребуется повторить аутентификацию.

## 2.2 Структура меню

В случае ввода правильного значения пароля, вход пользователю будет разрешен и на экране появится изображение так называемого рабочего стола, включающего следующие элементы графического интерфейса:

меню Приложения, предоставляющее возможность запуска интегрированных в систему приложений (см. Снимок экрана 1);

меню Места, предоставляющее возможность доступа к папкам и файлам системы, просмотра ресурсов компьютера и обзора сети (см. Снимок экрана 2);

меню выбора раскладки клавиатуры (см. Снимок экрана 3);

меню настройки даты и времени (см. Снимок экрана 4);

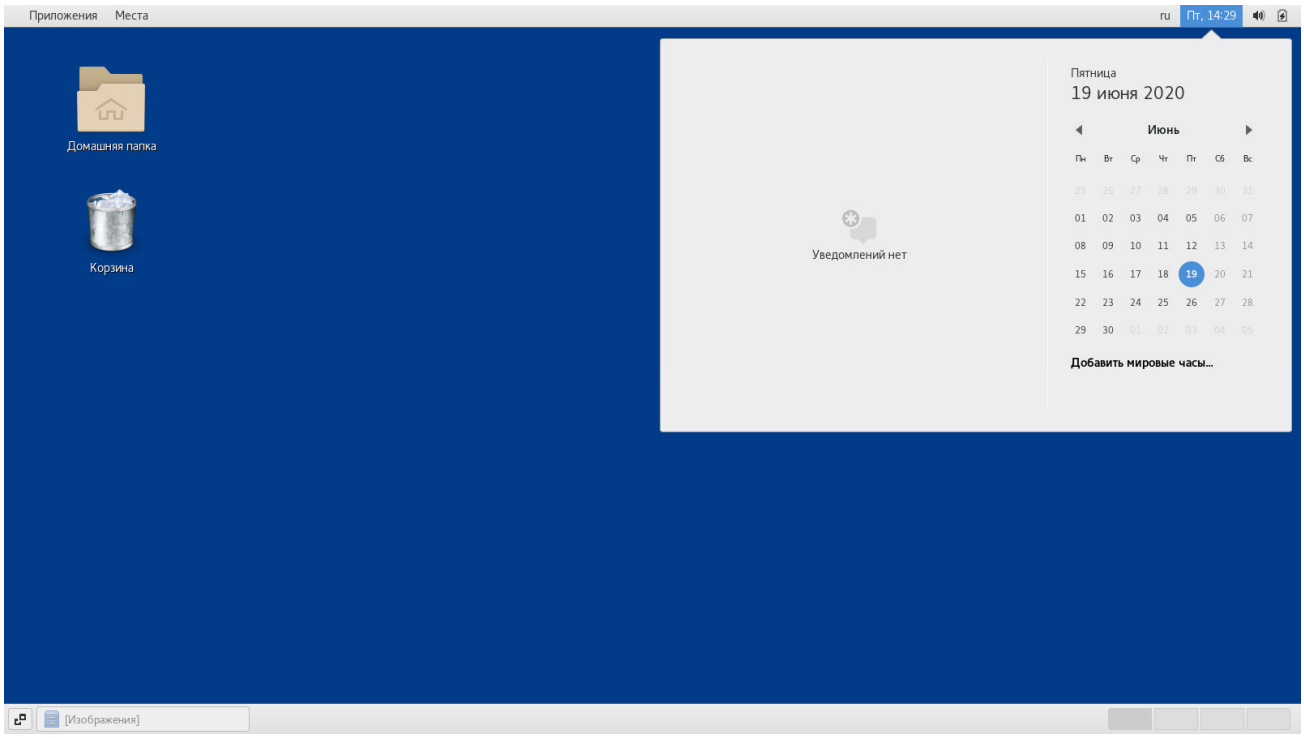
системное меню, предоставляющее возможность настройки некоторых системных параметров, а также возможность завершения сеанса, блокировки экрана, перезапуска и выключения системы (см. Снимок экрана 5).

Подробнее о составе и функциональных возможностях вышеперечисленных меню изложено в следующих разделах и во встроенной в систему документации.


Снимок экрана 1 – Меню Приложения


Снимок экрана 2 – Меню Места


Снимок экрана 3 - Меню выбора раскладки клавиатуры




Снимок экрана 4 – Меню календаря, даты и времени


Снимок экрана 5 – Системное меню

### 2.3 Блокировка экрана

Блокировка экрана осуществляется нажатием в системном меню круглой кнопки с изображением замка (путем наведения на нее курсора и нажатия кнопки манипулятора мышь, см. Снимок экрана 6) и сопровождается появлением так называемого экрана блокировки (см. Снимок экрана 7). Для разблокировки экрана необходимо будет нажать на клавиатуре клавишу Ввод и снова предъявить свой пароль (см. Снимок экрана 8)..

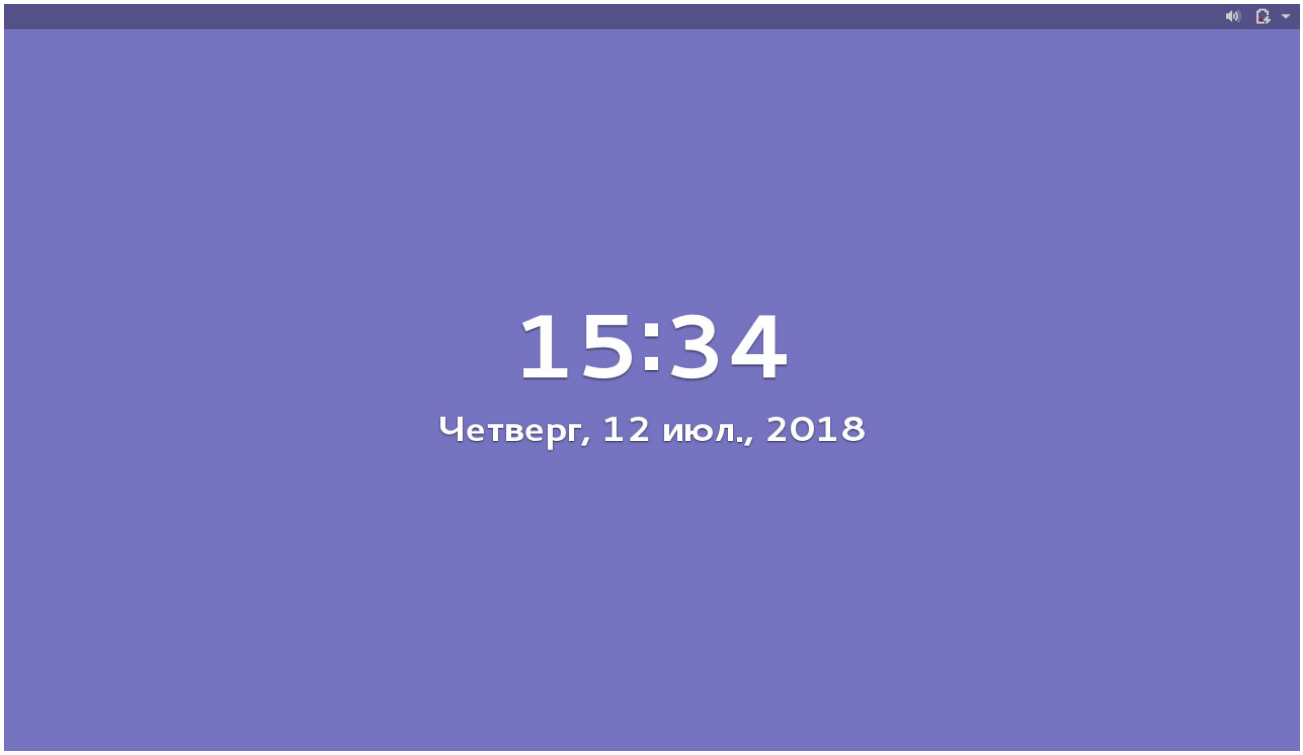
### 2.4 Завершение сеанса

Завершение сеанса работы пользователя с системой осуществляется нажатием в системном меню на имя пользователя с последующим выбором расположенного ниже меню завершения сеанса (см. Снимок экрана 9) и подтверждением данного выбора (см. Снимок экрана 10). Завершение сеанса сопровождается завершением работы всех запущенных пользователем приложений.

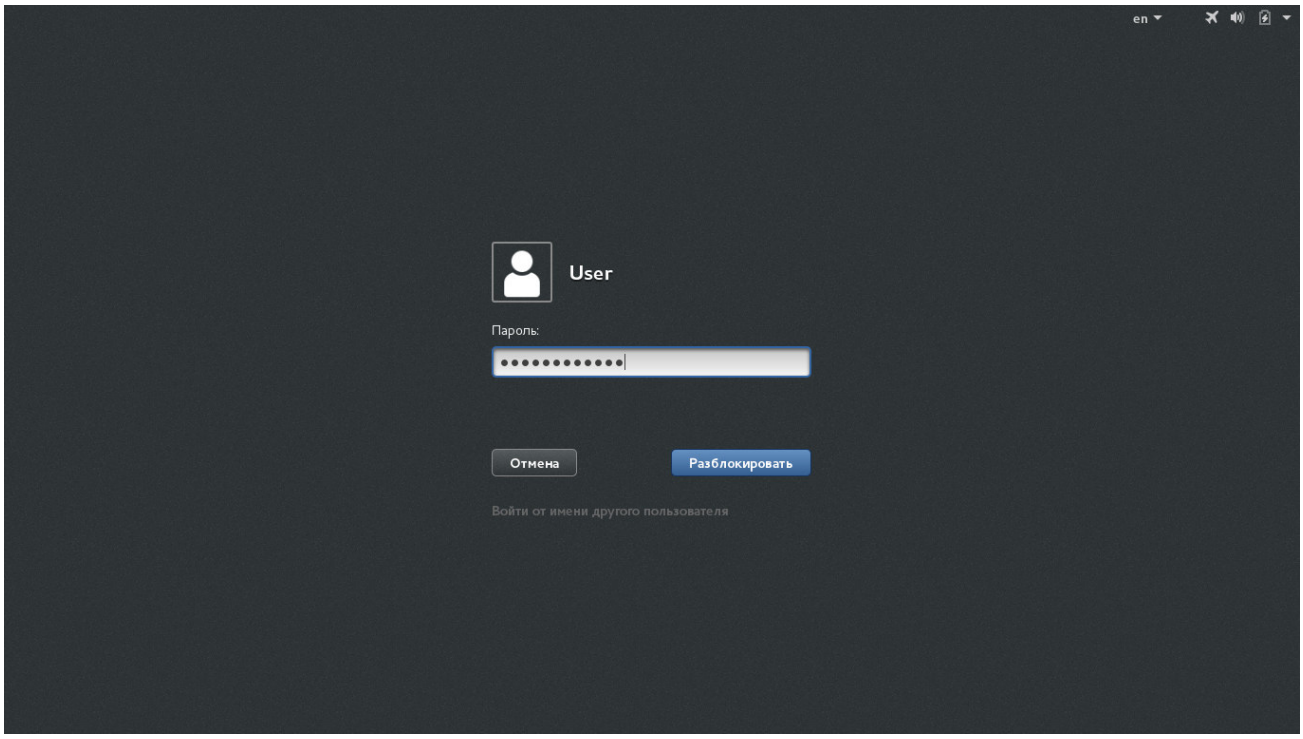
### 2.5 Перезапуск и выключение системы

Перезапуск и выключение системы осуществляются нажатием в системном меню круглой кнопки с изображением выключателя электропитания (см. Снимок экрана 11) и последующим нажатием кнопки Перезапуск или кнопки Выключение (см. Снимок экрана 12).


Снимок экрана 6 – Кнопка блокировки экрана

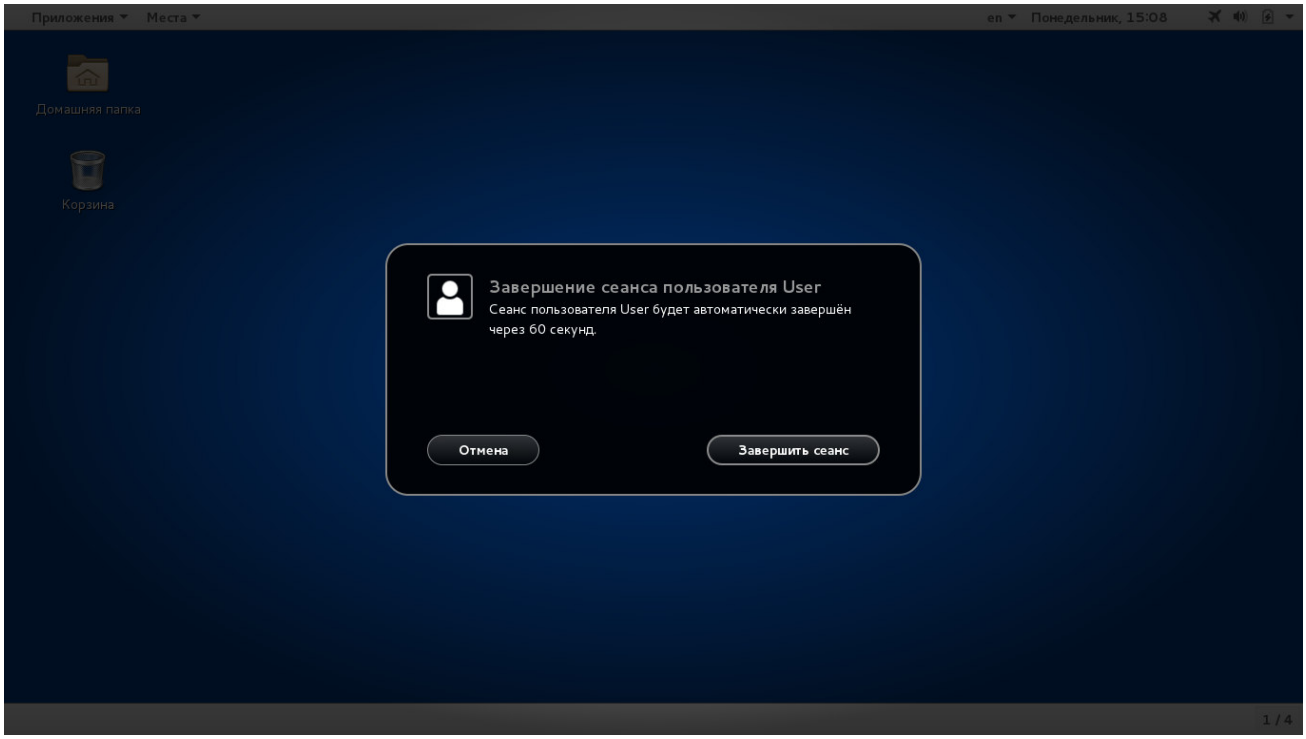



Снимок экрана 7 – Экран блокировки

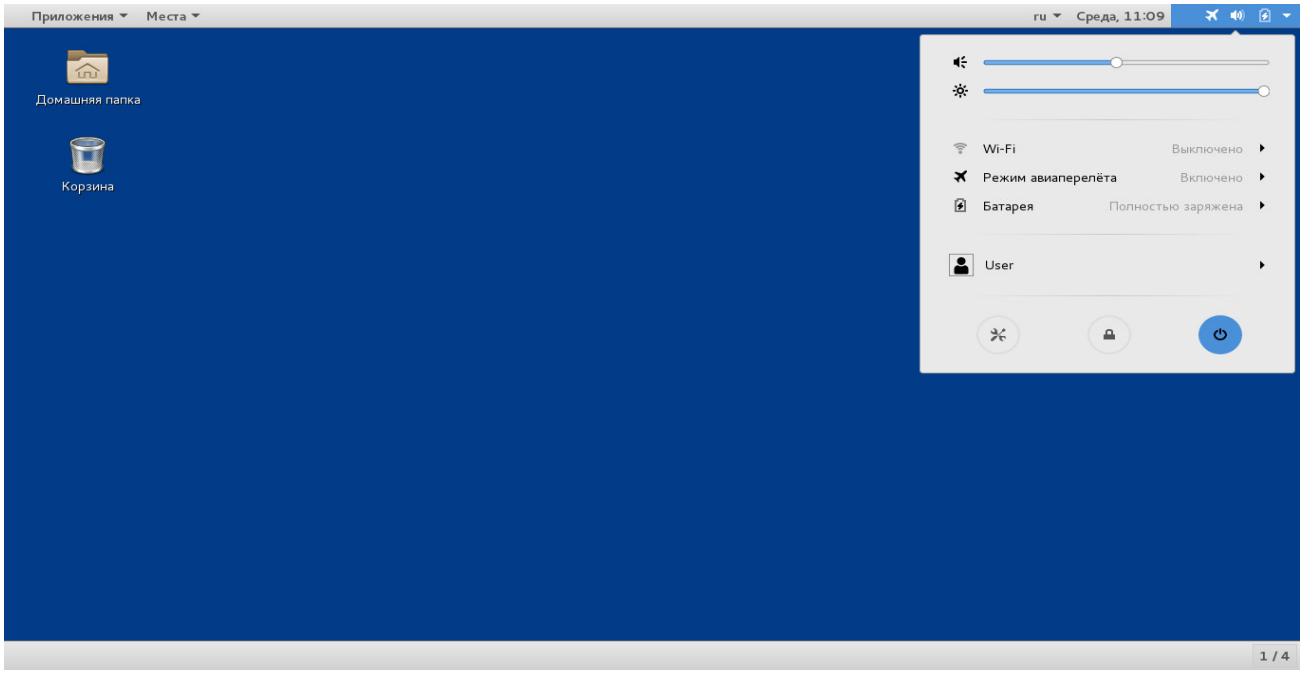



Снимок экрана 8 - Разблокировка экрана

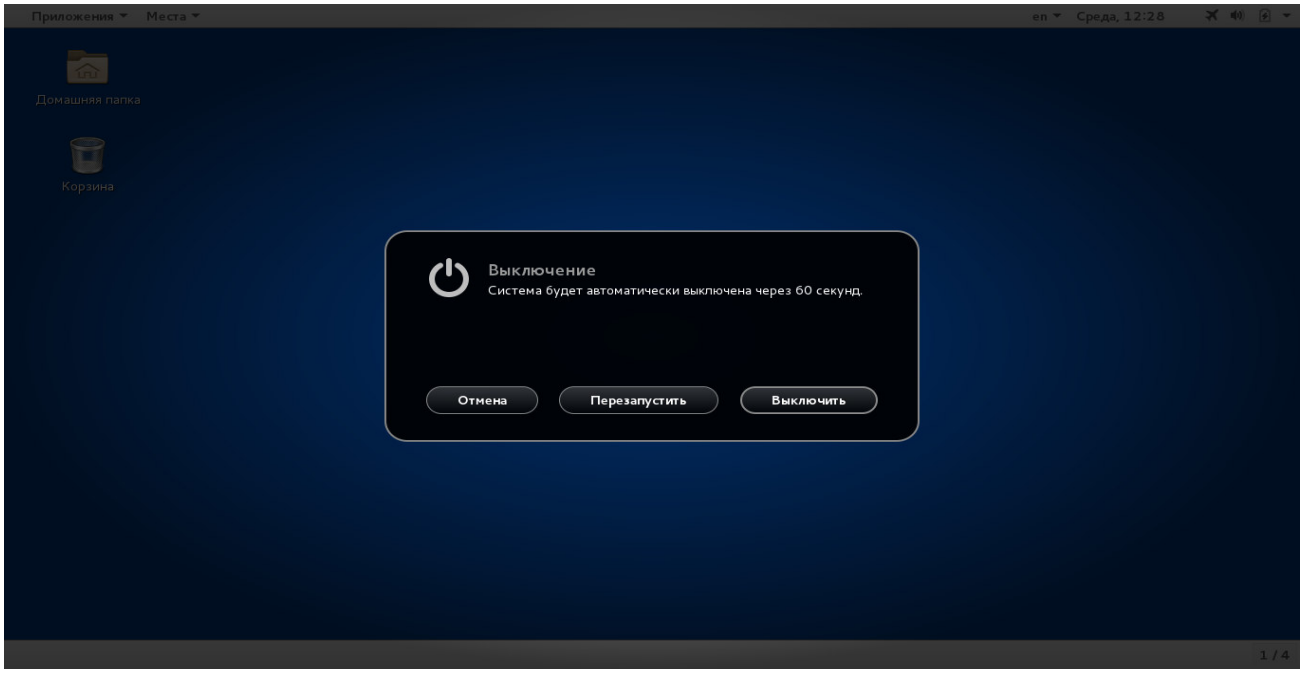

Снимок экрана 9 – Завершить сеанс




Снимок экрана 10 – Подтверждение завершения сеанса




Снимок экрана 11 – Кнопка перезапуска или выключения системы




Снимок экрана 12 – Подтверждение перезапуска или выключения системы

# 3 НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ

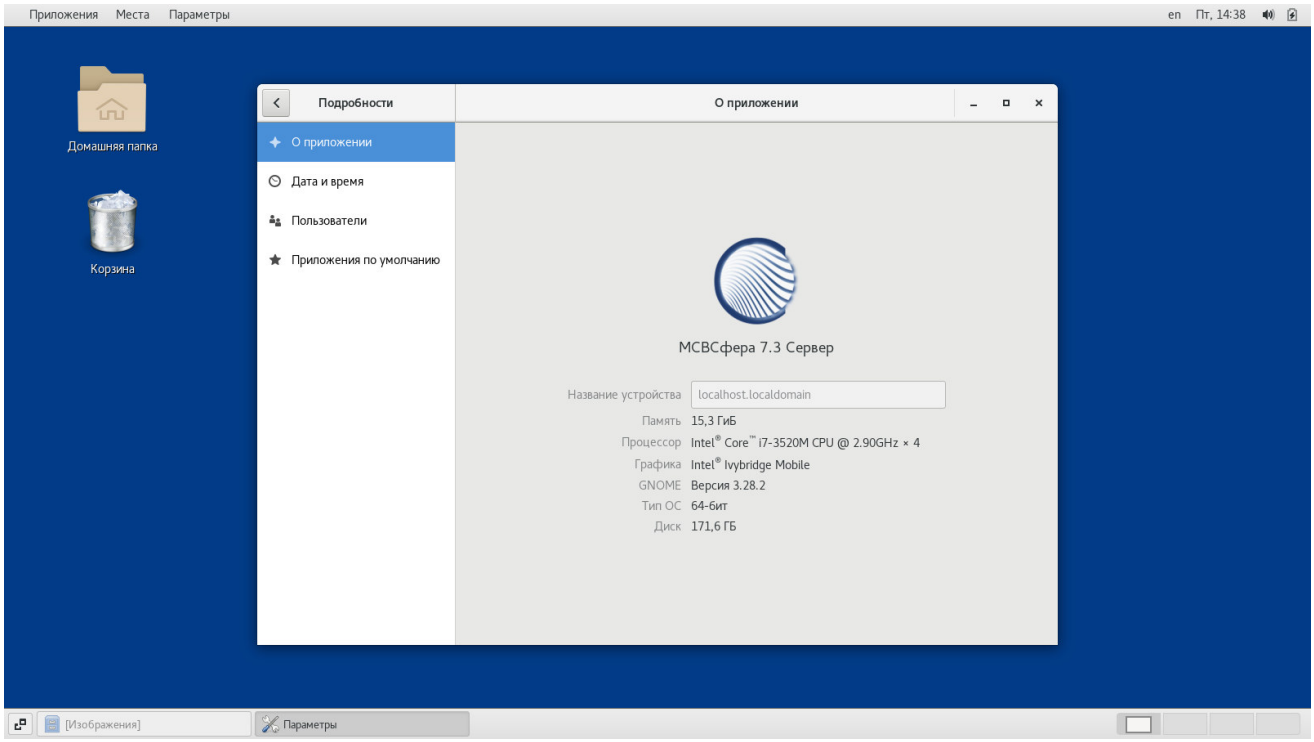
Просмотр и изменение значений системных параметров, в том числе параметров безопасности, осуществляется нажатием в системном меню круглой кнопки Параметры с изображением инструментов (см. Снимок экрана 13) с последующим выбором из появившегося на экране списка параметров тех из них, которые необходимо просмотреть и/или изменить.

## 3.1 Имя и пароль пользователя

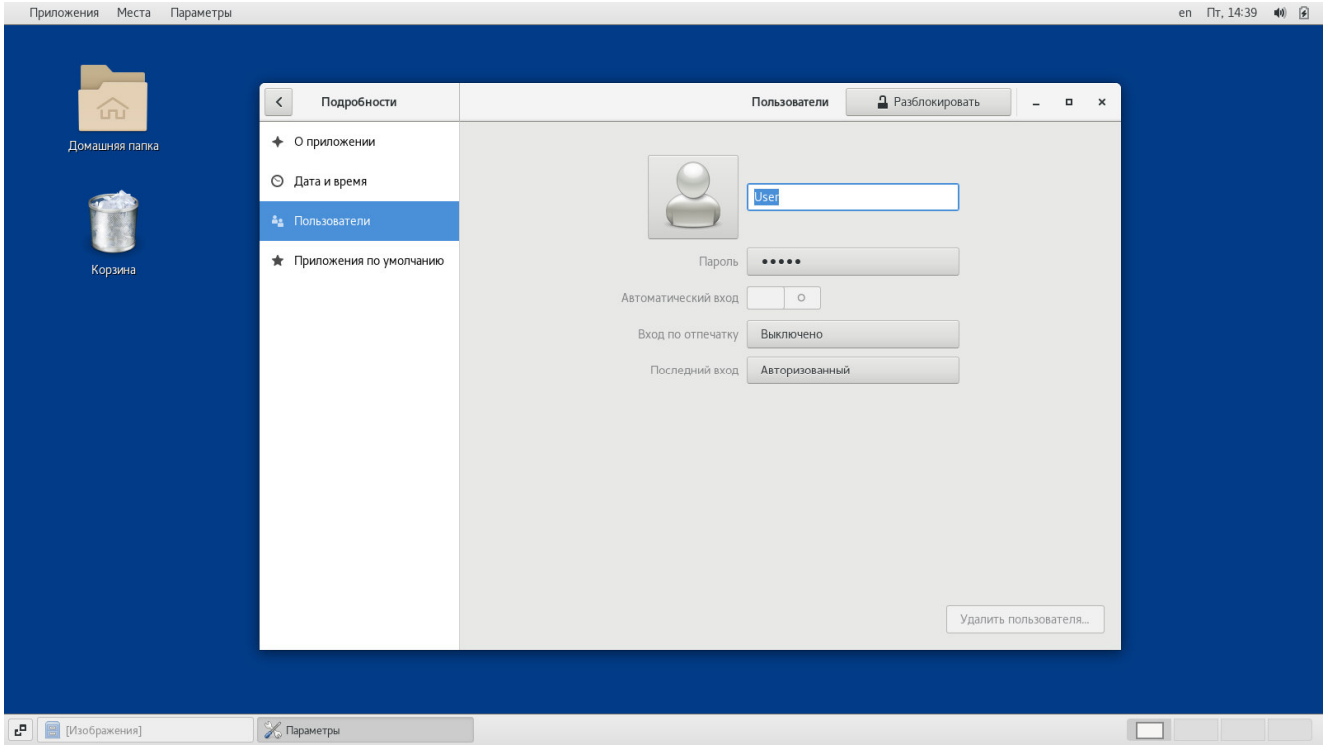
Для изменения значений своего имени или пароля необходимо выбрать и запустить приложение Пользователи, после чего задать новое значение своего имени пользователя (см. Снимок экрана 15) или задать и подтвердить новое значение своего пароля, продемонстрировав предварительно знание текущего значения пароля (см. Снимки экрана 16, 17).

При изменении пароля следует помнить, что его новое значение не должно быть тривиальным, т.е. легким для подбора или угадывания. Для выработки качественного значения пароля можно воспользоваться кнопкой с изображением шестеренок, активизирующей так называемый генератор паролей.

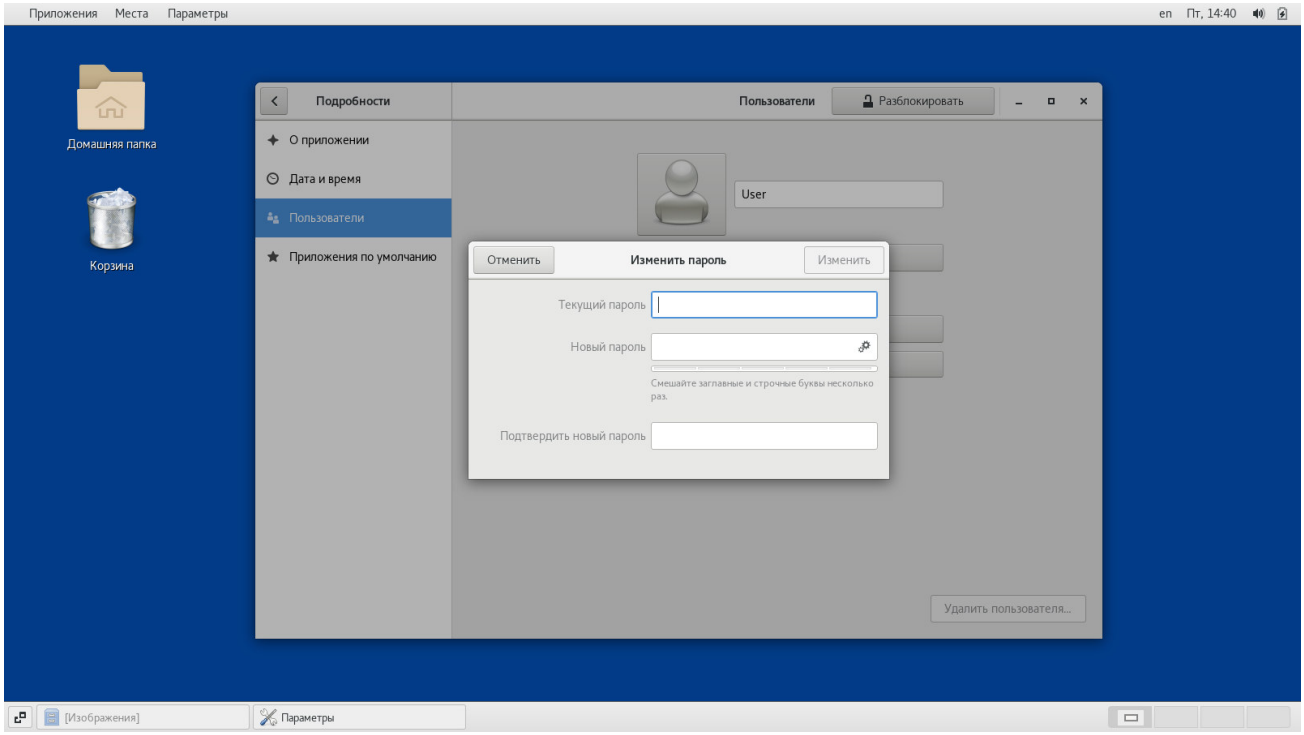

Снимок экрана 13 - Кнопка Параметры



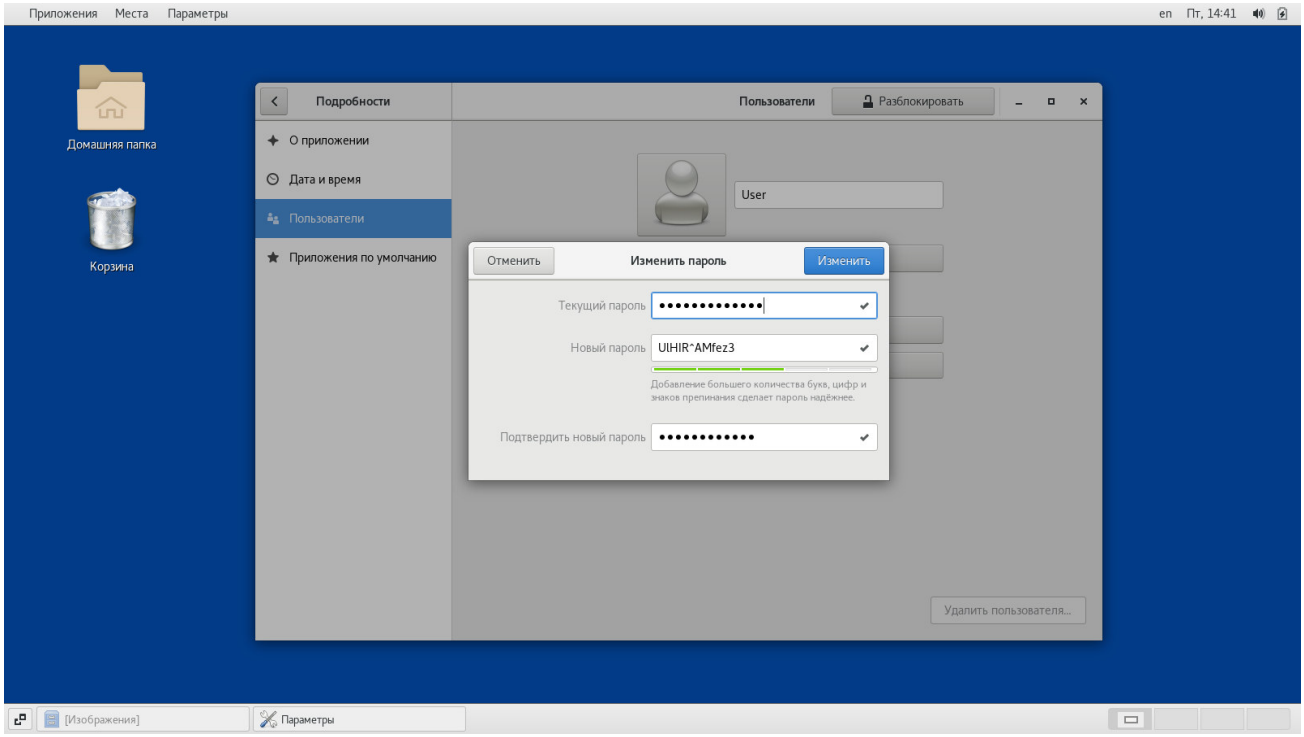

Снимок экрана 14 - О приложении




Снимок экрана 15 - Пользователи - Имя

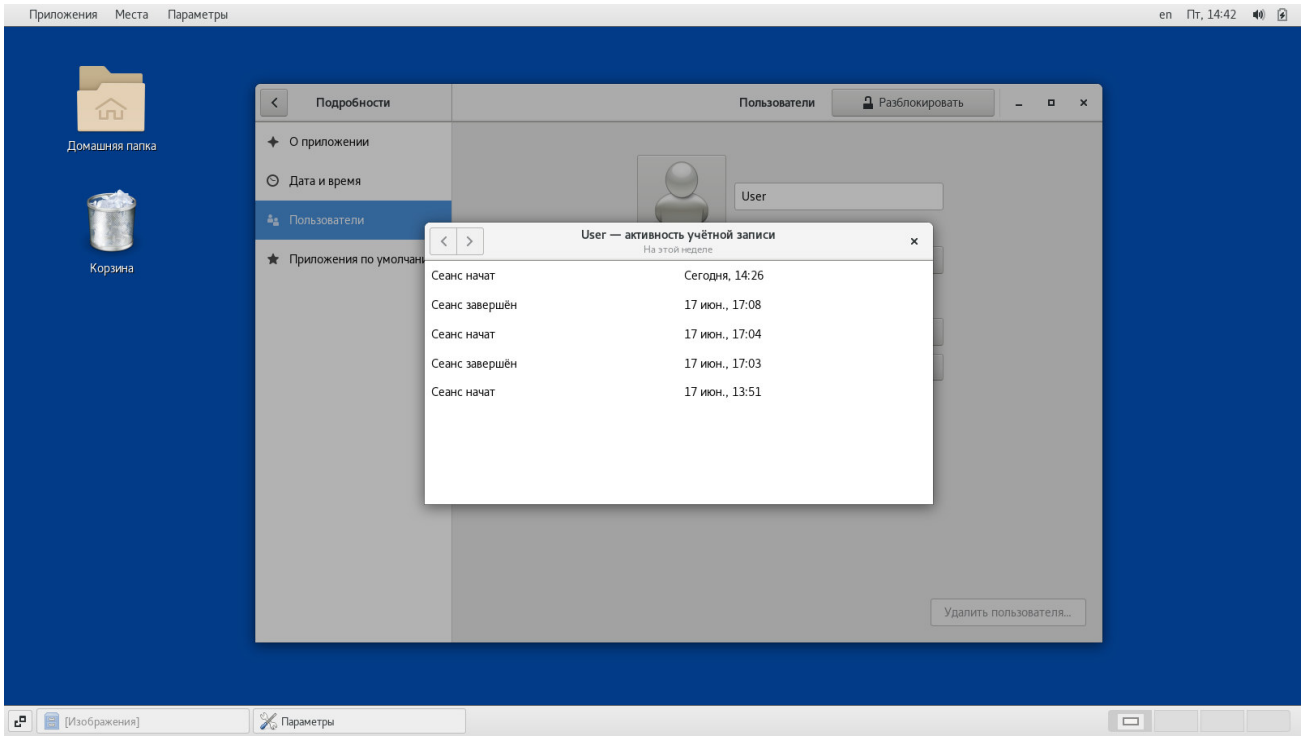



Снимок экрана 16 - Изменить пароль




Снимок экрана 17 - Изменение значения пароля

Для просмотра истории входа в систему и выхода из нее можно в окне Пользователи нажать кнопку Последний вход. Появится так называемый журнал входа в систему с информацией о датах и времени начала и завершения сеансов работы.




Снимок экрана 18 - Журнал входа в систему

### 3.2 Блокировка экрана

Настройка параметров блокировки экрана осуществляется с помощью меню Блокировка экрана (см. Снимок экрана 20) приложения Конфиденциальность (см. Снимок экрана 19).

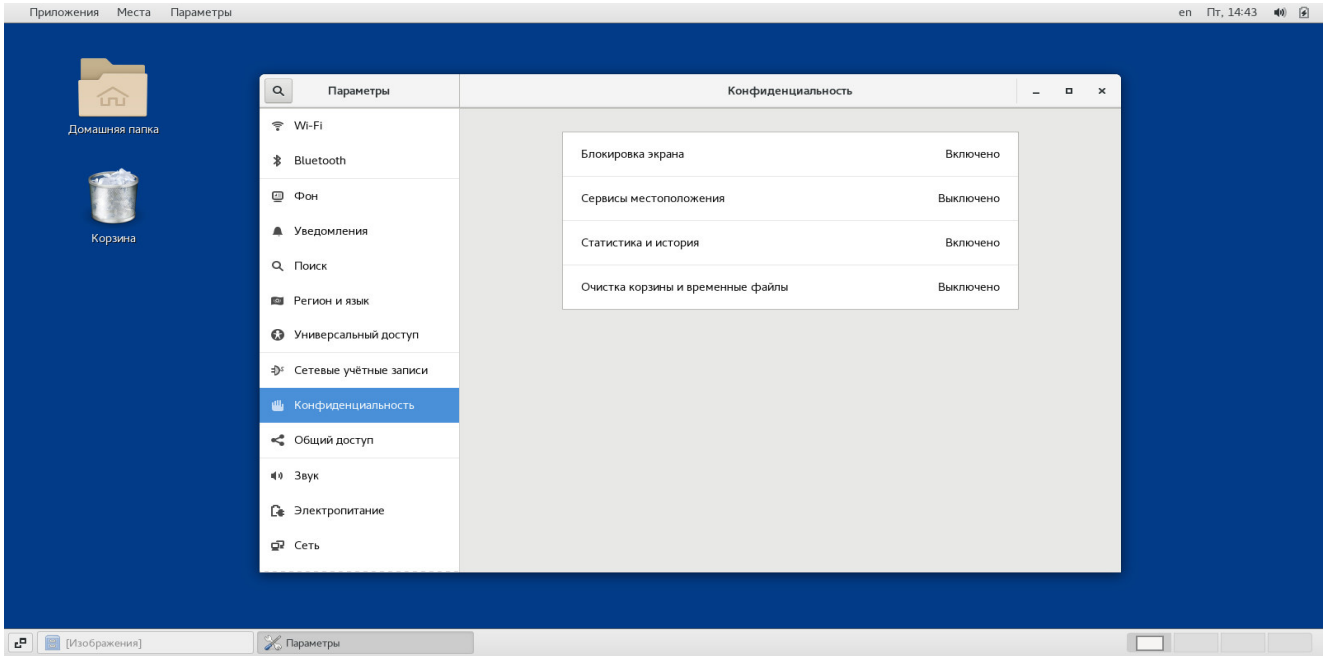
Блокировка экрана будет выполняться после истечения установленного промежутка времени, которое, в свою очередь, будет отсчитываться от момента выключения экрана, настраиваемого с помощью приложения меню Параметры – Электропитание – Выключение экрана.

### 3.3 Статистика и история

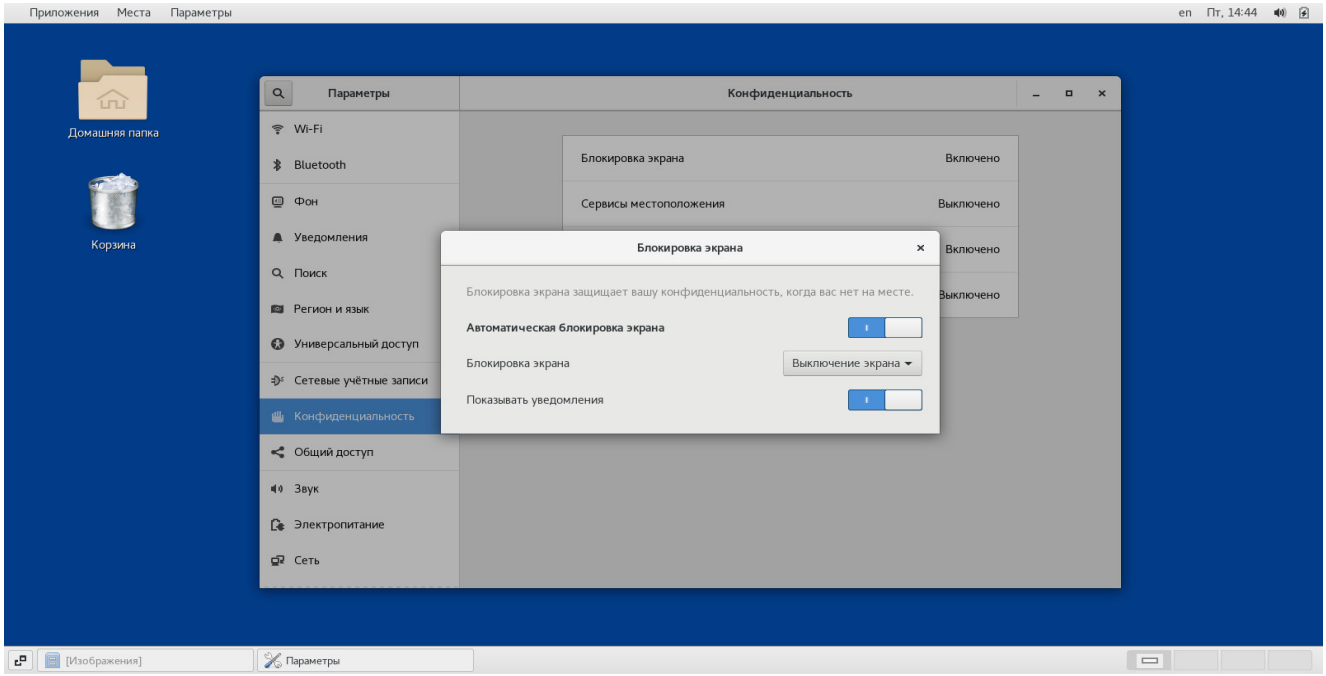
Настройка параметров ведения и хранения статистики и истории осуществляется с помощью меню Статистика и история (см. Снимок экрана 21) приложения Конфиденциальность.

### 3.4 Очистка корзины и временные файлы

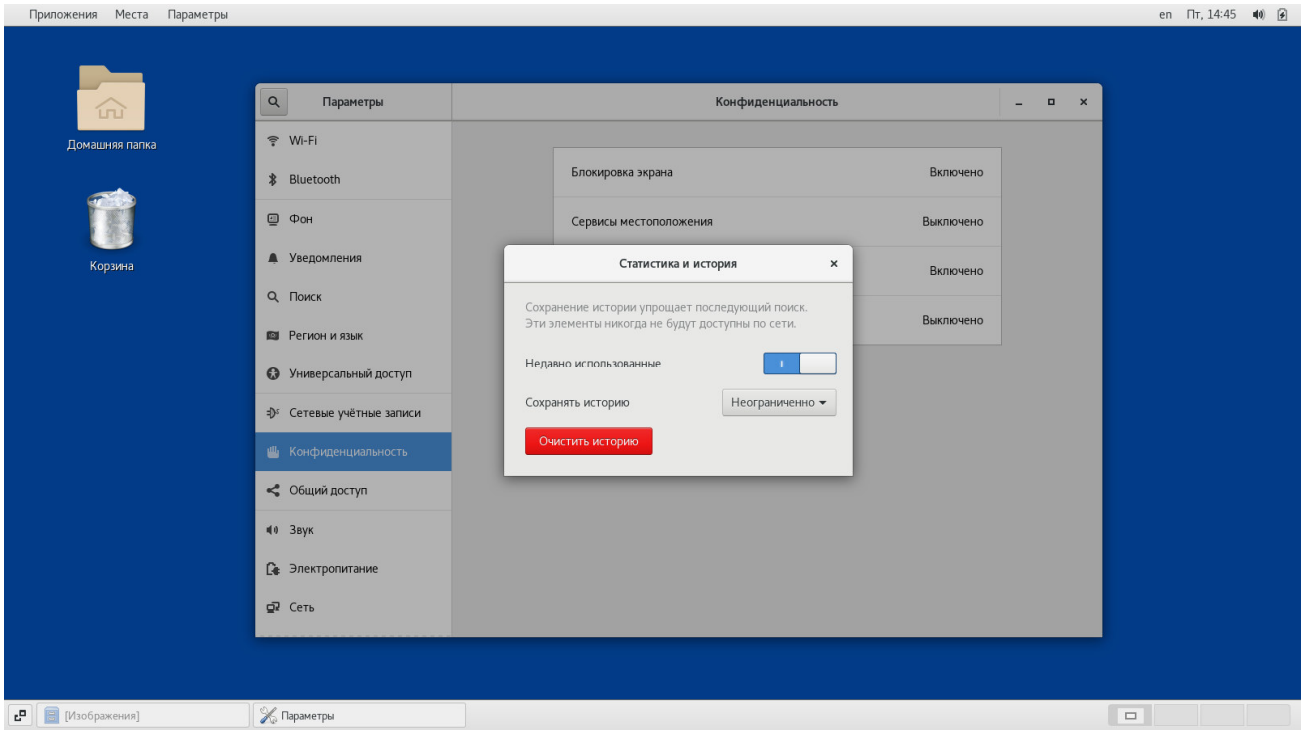
Настройка параметров автоматической очистки корзины и удаления временных файлов осуществляется с помощью меню Очистка корзины и временные файлы (см. Снимок экрана 22) приложения Конфиденциальность.



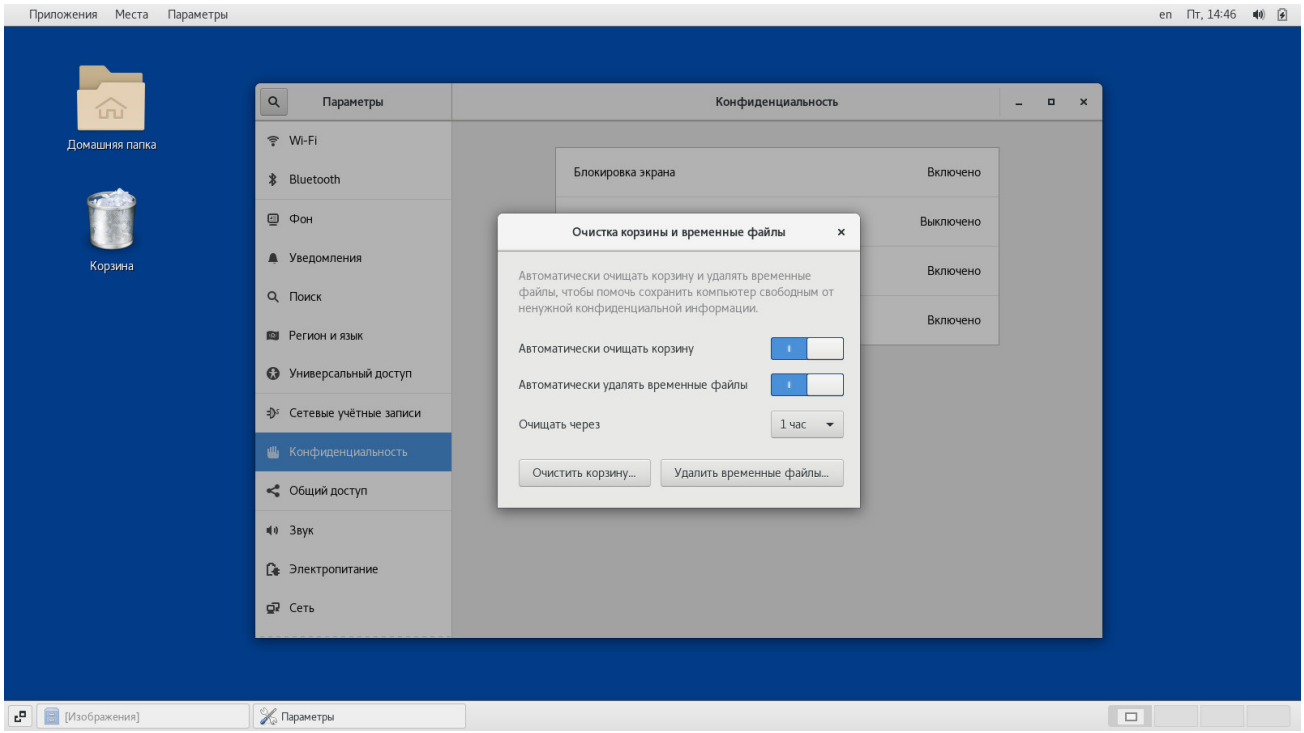

Снимок экрана 19 – Конфиденциальность




Снимок экрана 20 – Блокировка экрана




Снимок экрана 21 – Статистика и история




Снимок экрана 22 – Очистка корзины и временные файлы

Как известно, все удаляемые в ходе работы с системой файлы перемещаются в специальную папку, называемую корзиной, из которой их потом можно восстановить.

Для безвозвратного удаления файла, находящегося в корзине, его надо выделить курсором, нажать правую кнопку мыши и в открывшемся списке выбрать соответствующее действие, после чего подтвердить его.

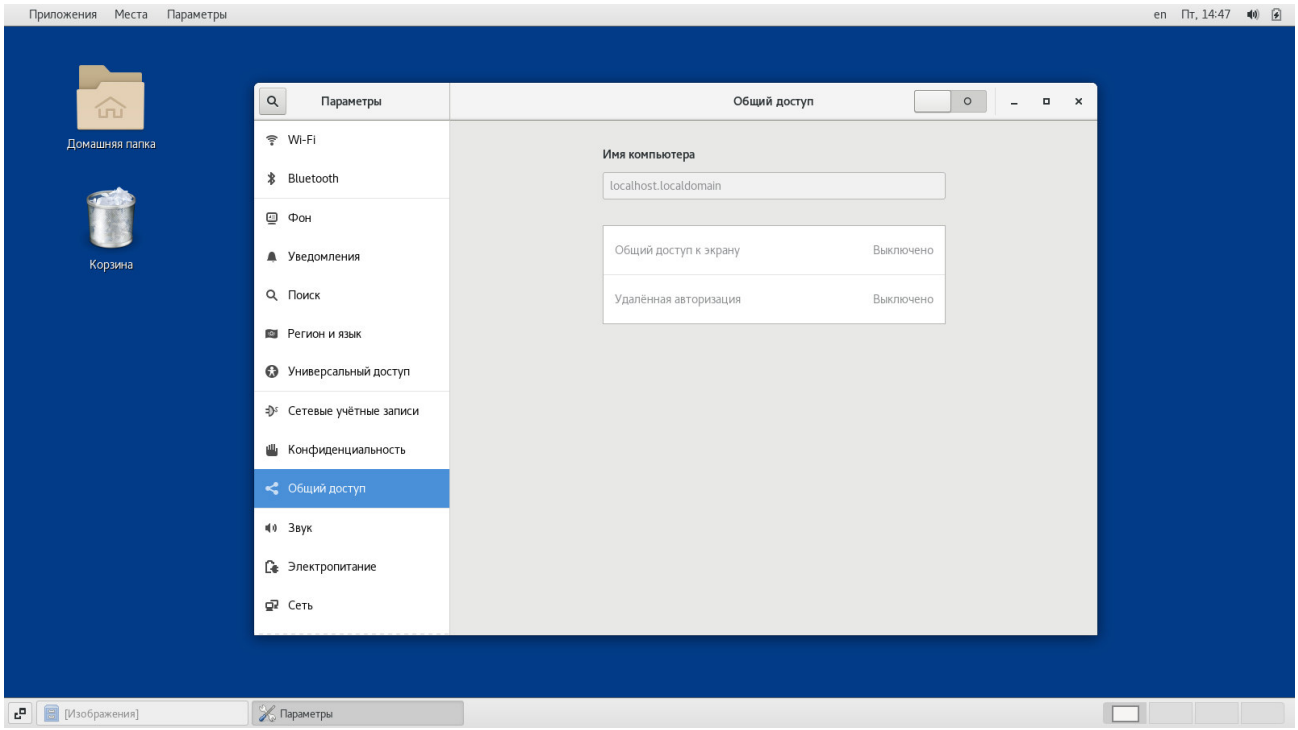
Для безвозвратного удаления сразу всех находящихся в корзине файлов необходимо нажать кнопку Очистить и подтвердить очистку корзины.

### 3.5 Общий доступ к экрану

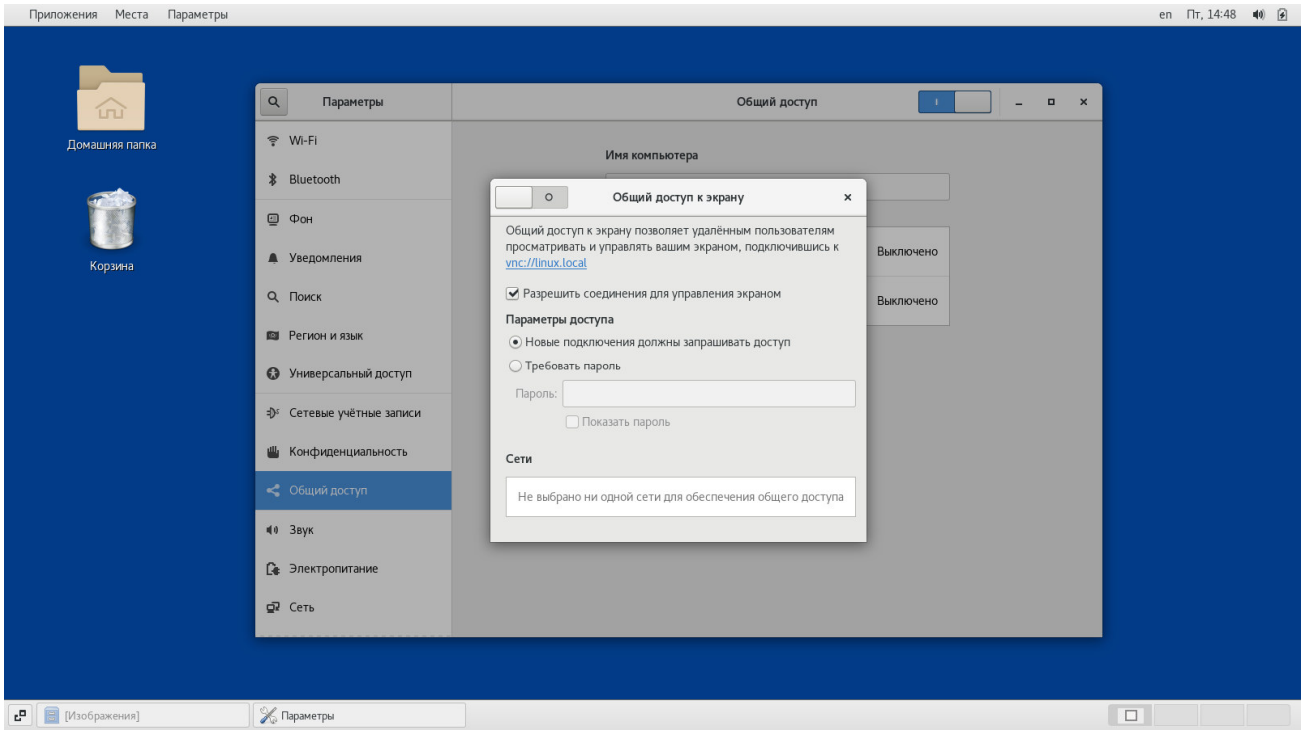
Общий доступ к экрану предоставляет возможность удаленного управления системой с использованием графического интерфейса пользователя. Настройка параметров общего доступа к экрану осуществляется с помощью меню Общий доступ к экрану (см. Снимок экрана 24) приложения Общий доступ (см. Снимок экрана 23).

### 3.6 Удаленная авторизация

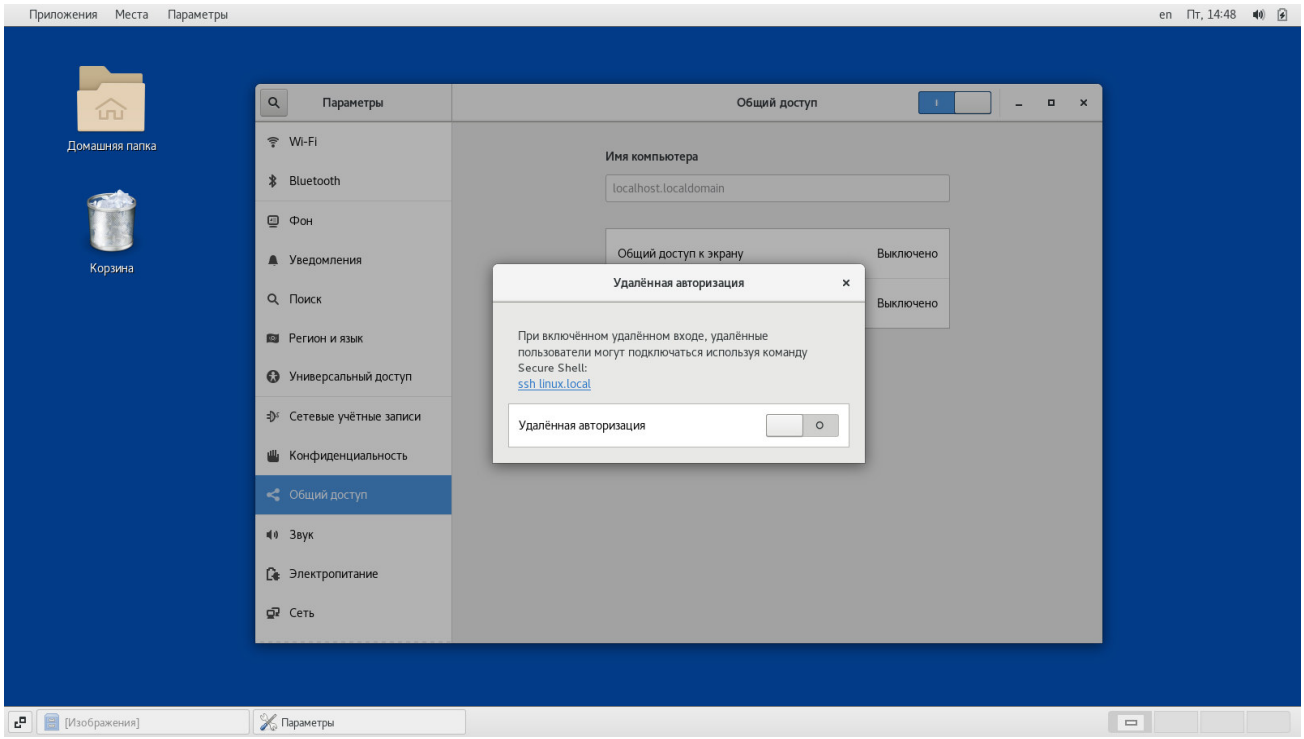
Удаленная авторизация предоставляет возможность удаленным пользователям подключаться к системе при помощи SSH-соединения через терминал. Настройка параметров удаленной авторизации осуществляется с помощью меню Удаленная авторизация (см. Снимок экрана 25) приложения Общий доступ.




Снимок экрана 23 – Общий доступ



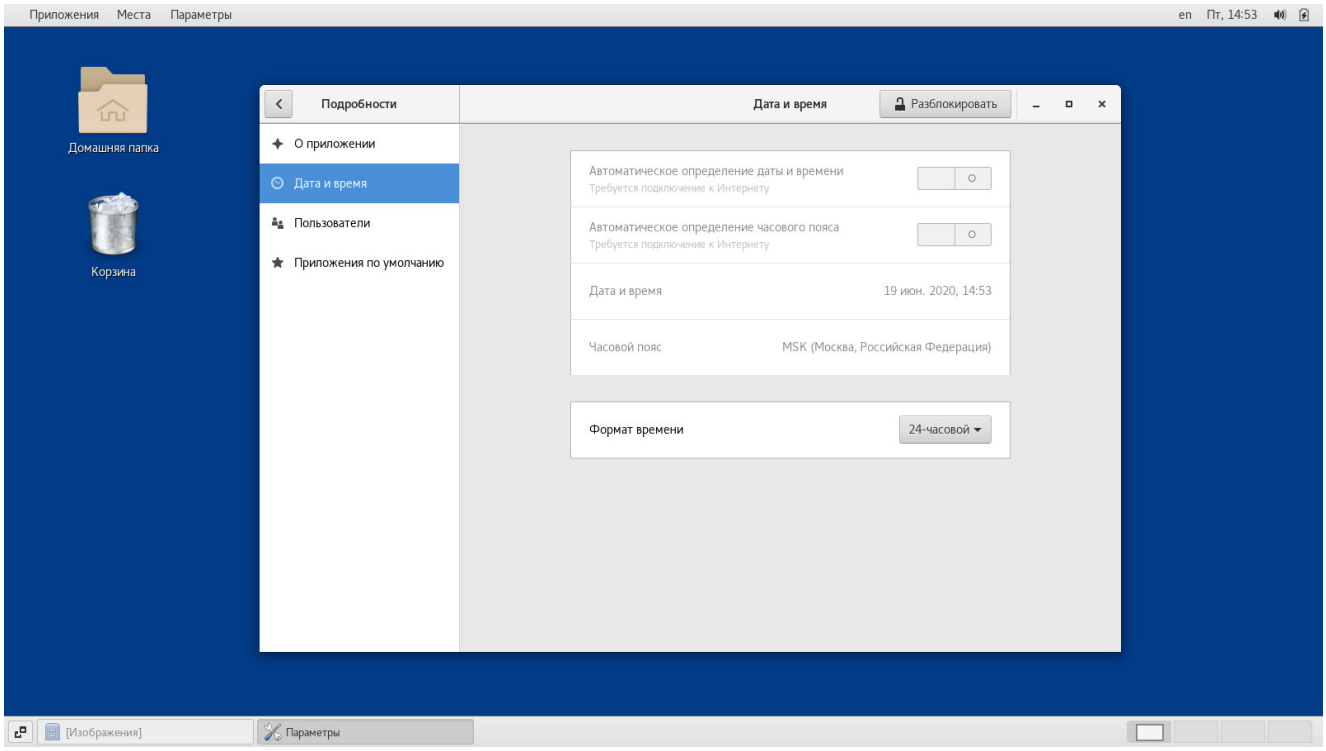

Снимок экрана 24 – Общий доступ к экрану




Снимок экрана 25 – Удаленная авторизация

### 3.7 Дата и время

Настройка даты и времени осуществляется с помощью приложения Дата и время.




Снимок экрана 26 – Дата и время

### 3.8 Права доступа к папкам и файлам

Для просмотра и определения свойств папки и прав доступа к ней необходимо ее выбрать, нажать правую кнопку мыши и в появившемся списке выбрать меню Свойства, затем открыть вкладку Права (см. Снимок экрана 27), после чего можно определять права доступа для владельца, группы и других пользователей, выбирая их из следующего списка:

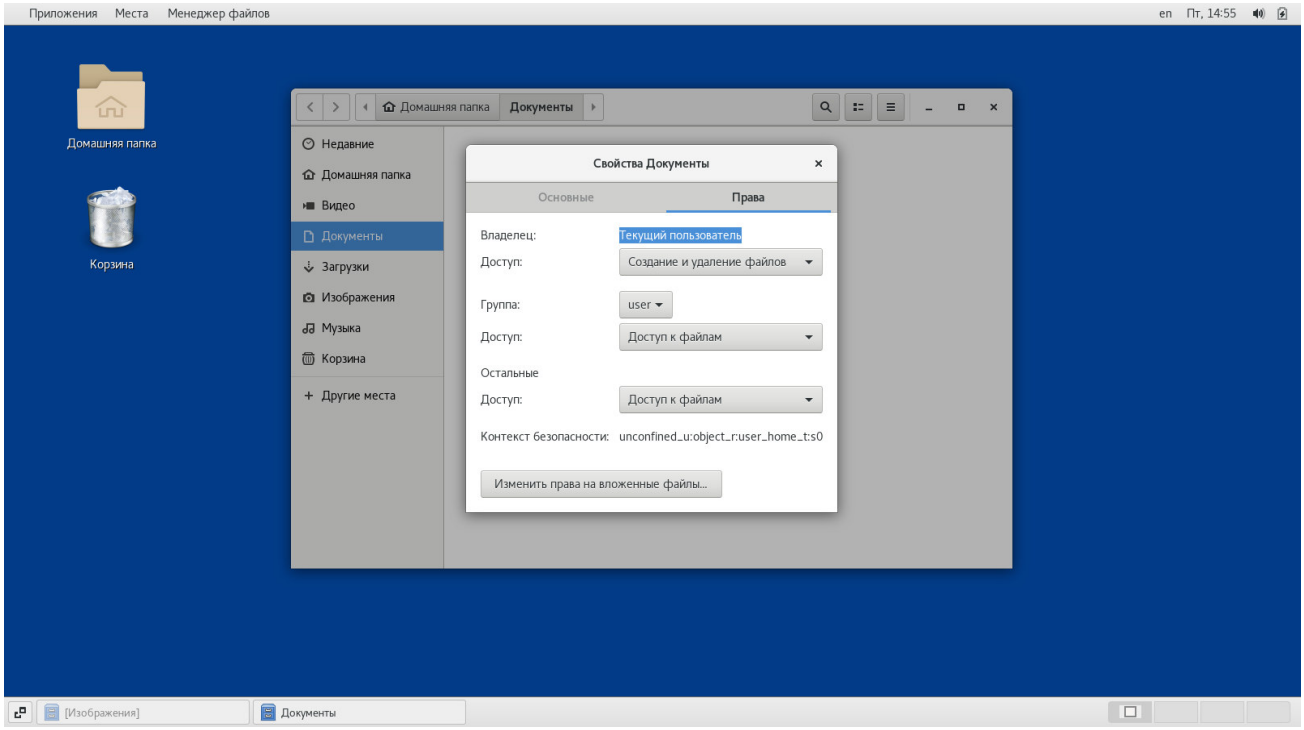
Нет – пользователь даже не сможет увидеть, какие файлы содержатся в папке;

Только перечисление файлов – пользователь сможет увидеть, какие файлы содержатся в папке, но не сможет открывать, создавать или удалять их;

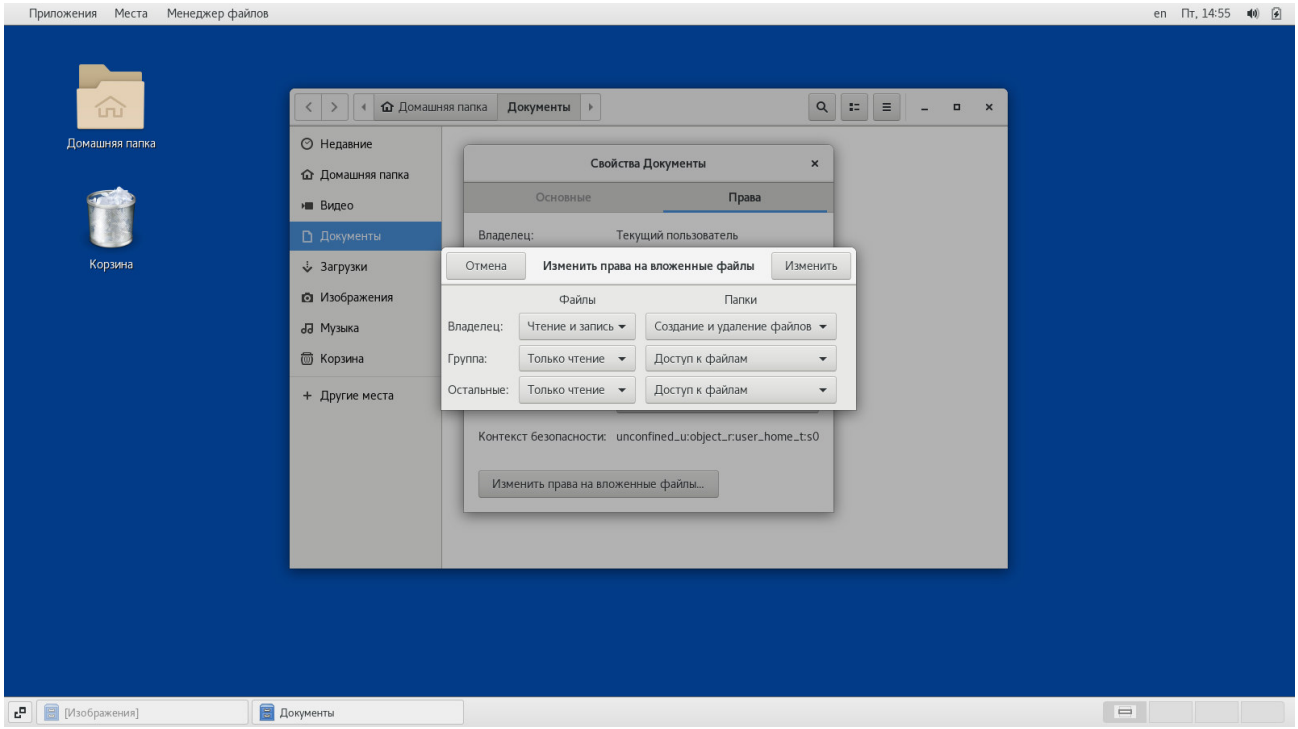
Доступ к файлам – пользователь сможет открывать файлы в папке, если это позволяют права доступа к данному конкретному файлу, но не сможет удалять файлы или создавать новые файлы;

Создание и удаление файлов – пользователь будет иметь полный доступ к папке, включая открытие, создание и удаление файлов.

Для быстрого определения одинаковых прав доступа для всех файлов в папке можно воспользоваться кнопкой  Изменить права на вложенные файлы.



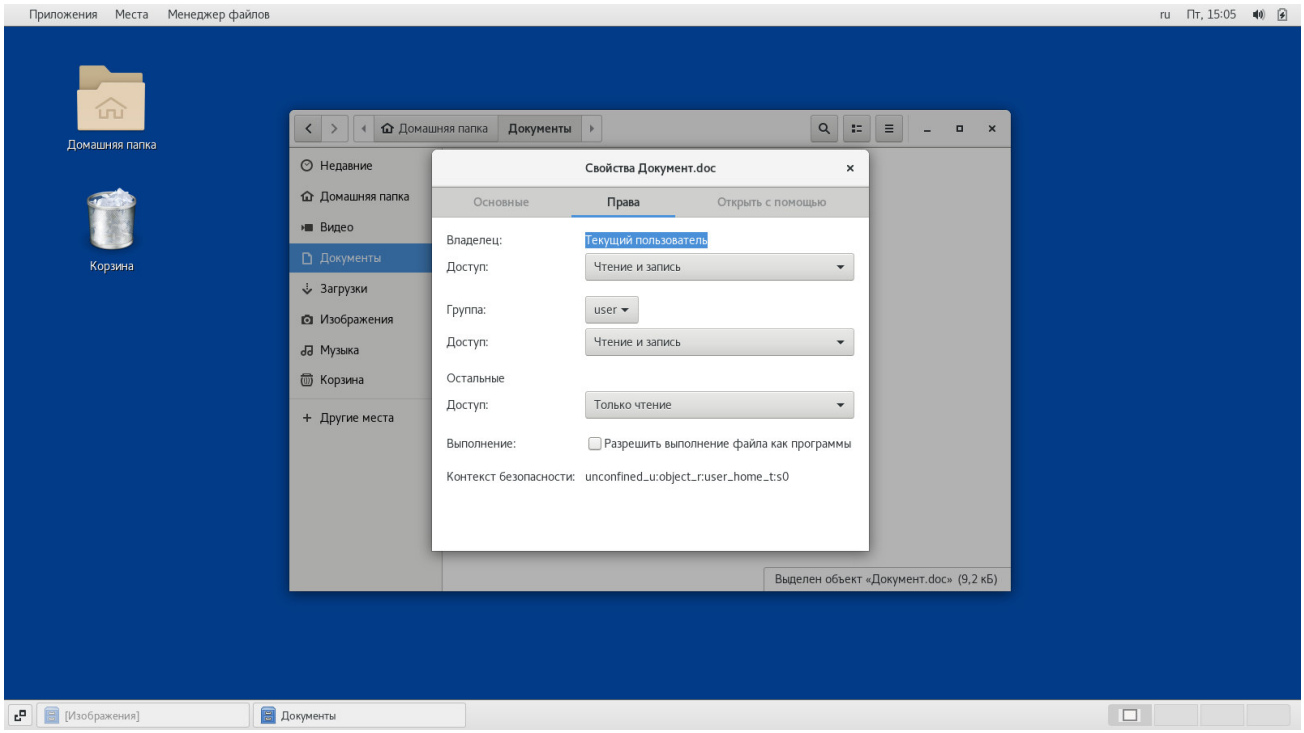

Снимок экрана 27 - Права доступа к папке




Снимок экрана 28 - Изменение прав на вложенные файлы

Права доступа к файлам устанавливаются аналогичным образом - выбирается файл, осуществляется переход к его Свойствам, выбирается вкладка Права, затем определяются права

доступа к файлу, предоставляющие возможность открывать, изменять, удалять или запускать его, как программу.




Снимок экрана 29 - Права доступа к файлу

# 4. ПЕРЕЧЕНЬ ДОСТУПНЫХ ПРИЛОЖЕНИЙ

## 4.1 Избранное

С помощью меню Избранное пользователь может запускать следующие приложения (см. Снимок экрана 30 ):

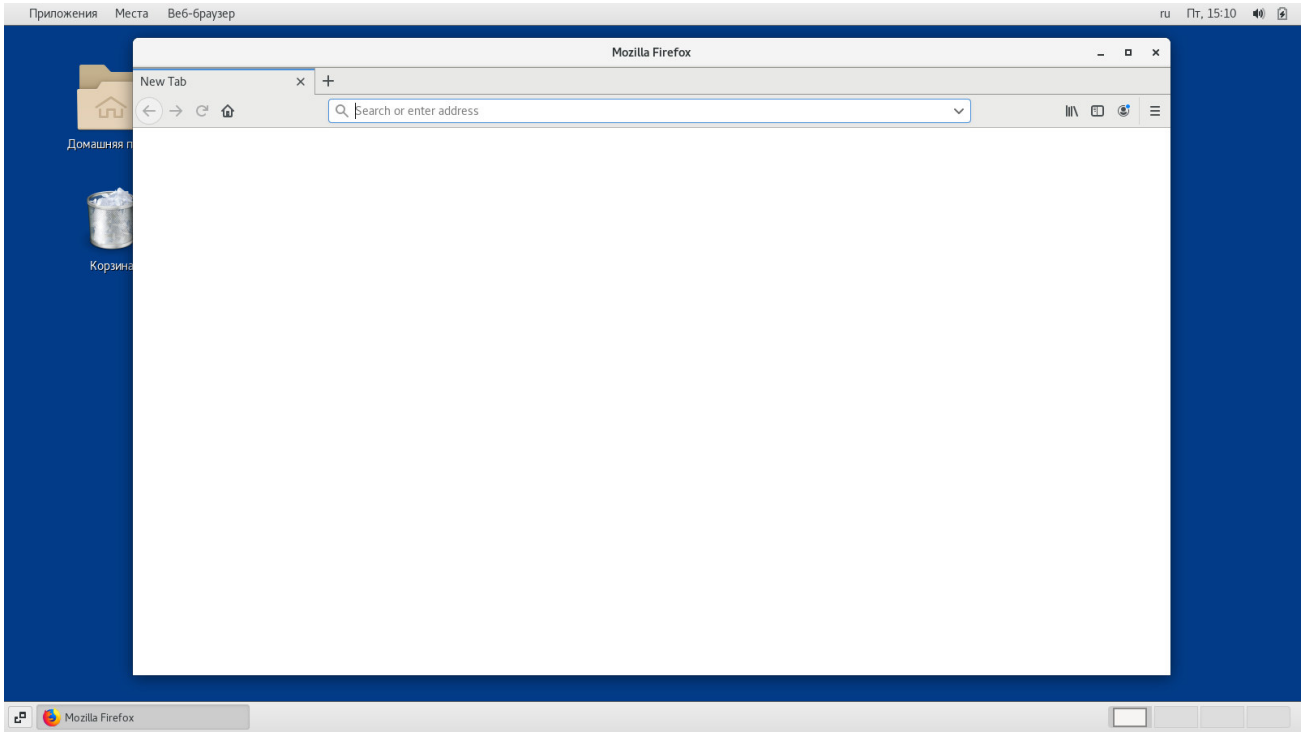
браузер Mozilla Firefox, отличающийся интуитивно понятным интерфейсом и высокой скоростью работы, поддерживающий все современные интернет-технологии и имеющий множество дополнительных опций и функциональных возможностей (см. Снимок экрана 31);

файловый менеджер Nautilus, обеспечивающий простой доступ к папкам и файлам и поддерживающий различные представления в виде иконок или списков (см. Снимок экрана 32);

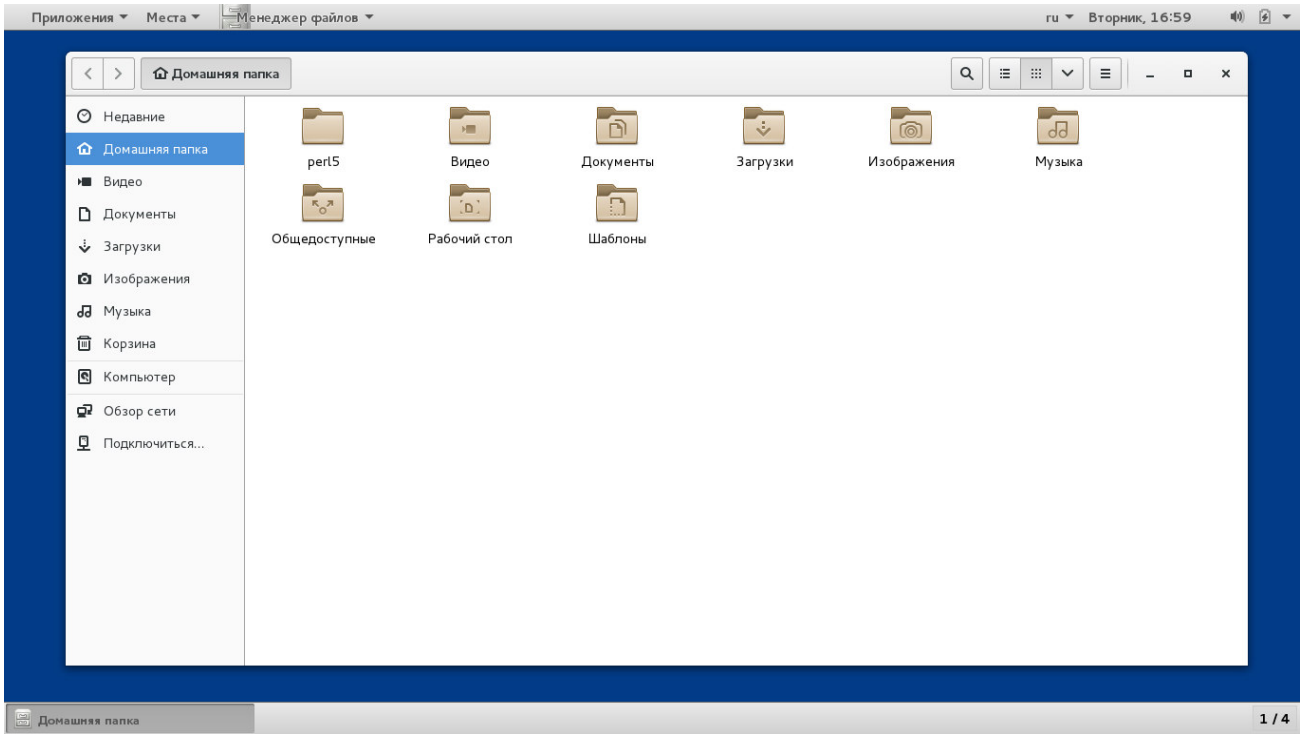
справку с подробным описанием функционала, реализуемого графической средой GNOME (см. Снимок экрана 33);

эмулятор терминала для доступа из графического интерфейса в окружение командного интерпретатора системы (см. Снимок экрана 34).

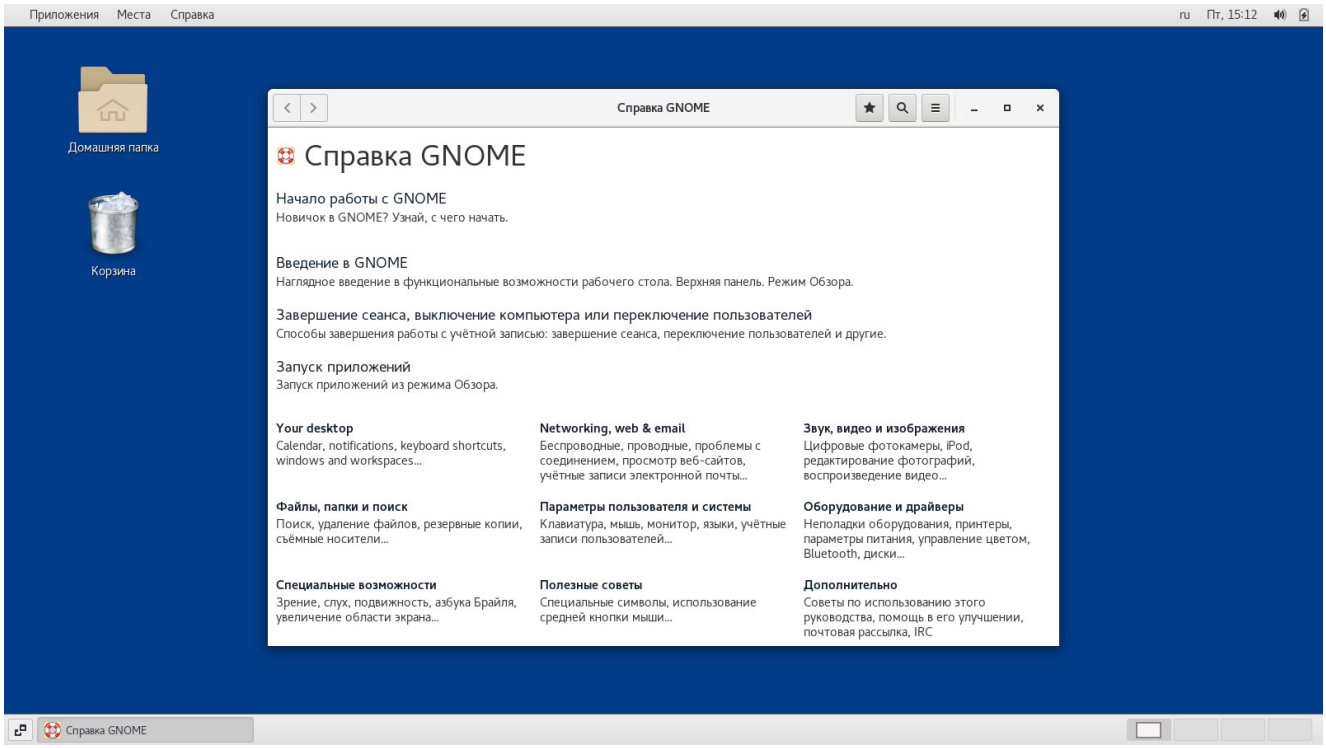

Снимок экрана 30 - Приложения - Избранное



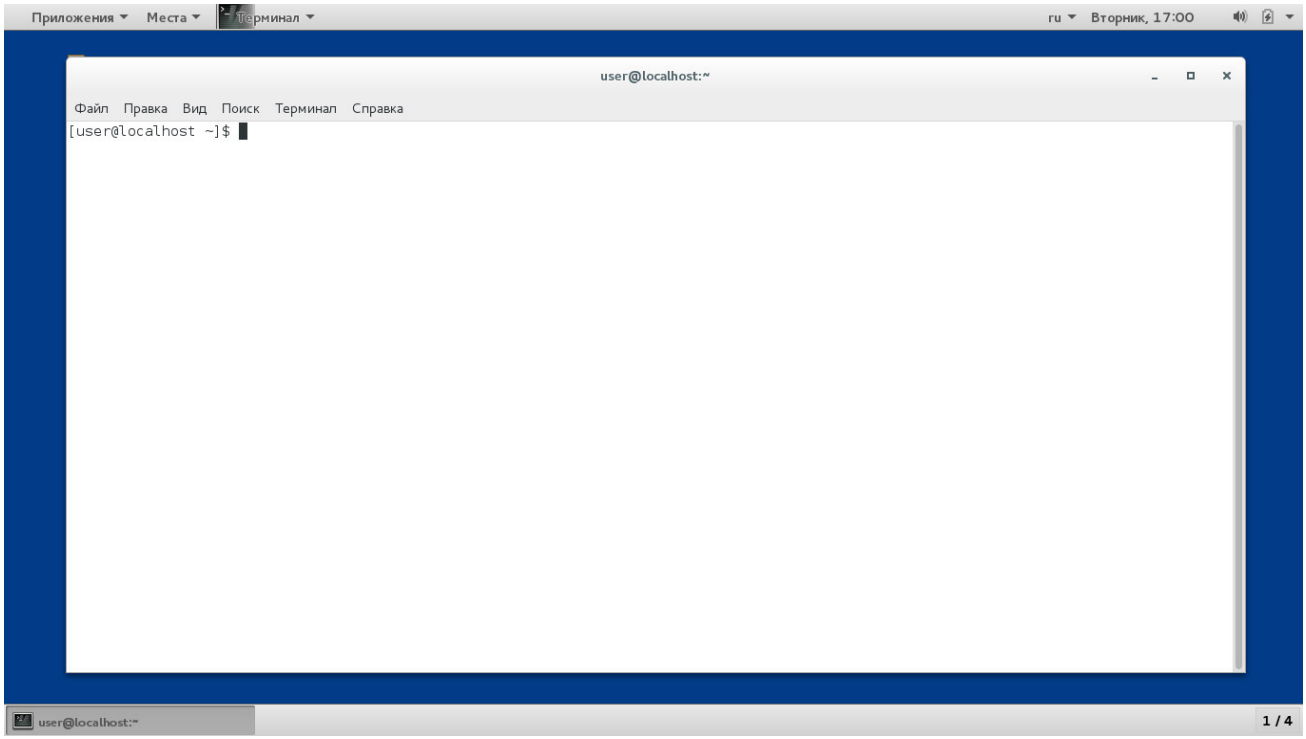

Снимок экрана 31 - Веб-браузер Mozilla Firefox




Снимок экрана 32 - Менеджер файлов Nautilus




Снимок экрана 33 - Справка GNOME




Снимок экрана 34 - Терминал

### 4.2 Офис

С помощью меню Офис пользователь может запускать следующие приложения (см. Снимок экрана 35):

редактор документов LibreOffice Writer, позволяющий создавать и редактировать документы, содержащие изображения, таблицы и графики, допускающий выбор шрифта, цвета, курсива, подчеркивания, определение стилей и автоформатирование, обеспечивающий макетирование страниц, работу с шаблонами и составными документами, выполнение функций слияния, создание оглавлений, встроенных иллюстраций, библиографий и диаграмм (см. Снимок экрана 36);

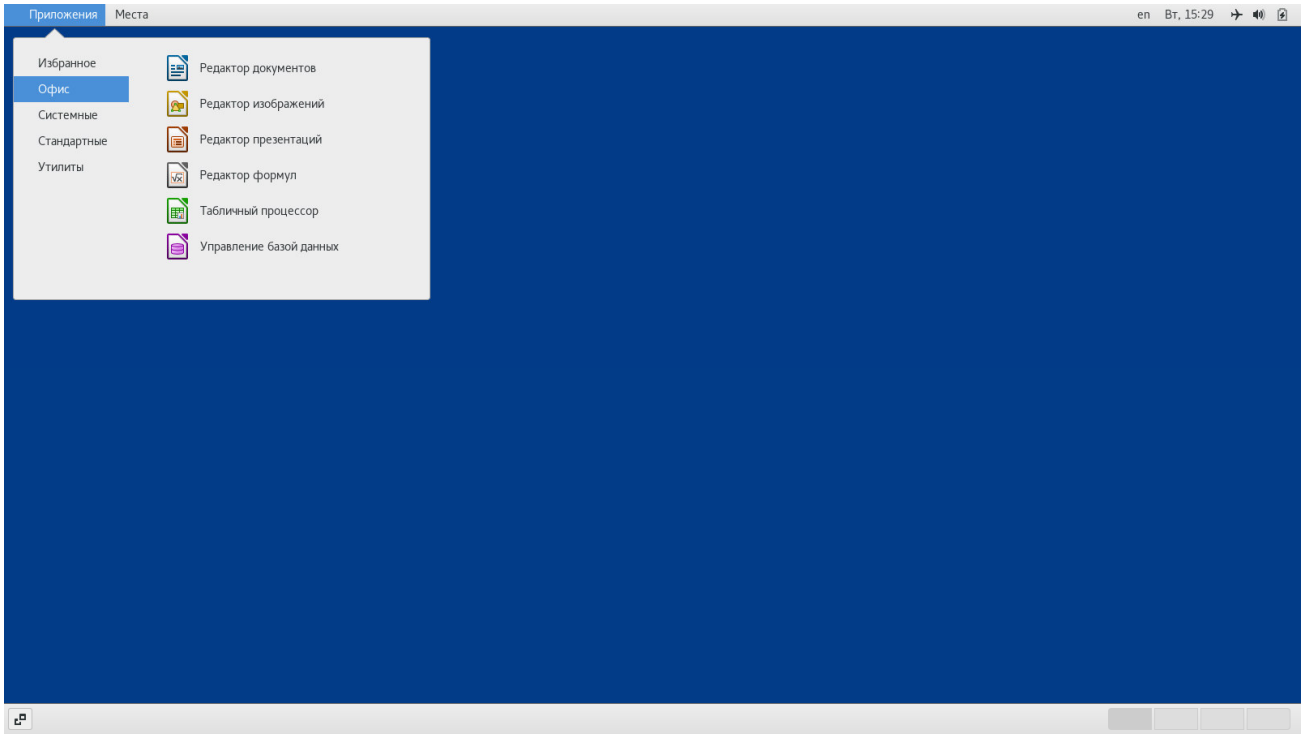
редактор изображений LibreOffice Draw, обеспечивающий работу с рисунками, фотореалистичными изображениями и динамическими иллюстрациями со спецэффектами, позволяющий создавать объемные объекты и задавать их освещение, выстраивать связные блок-схемы и сетевые диаграммы (см. Снимок экрана 37);

редактор презентаций LibreOffice Impress, позволяющий создавать и демонстрировать презентации, включающие текст, изображения, рисунки, фигуры, анимации и различные динамические спецэффекты (см. Снимок экрана 38);

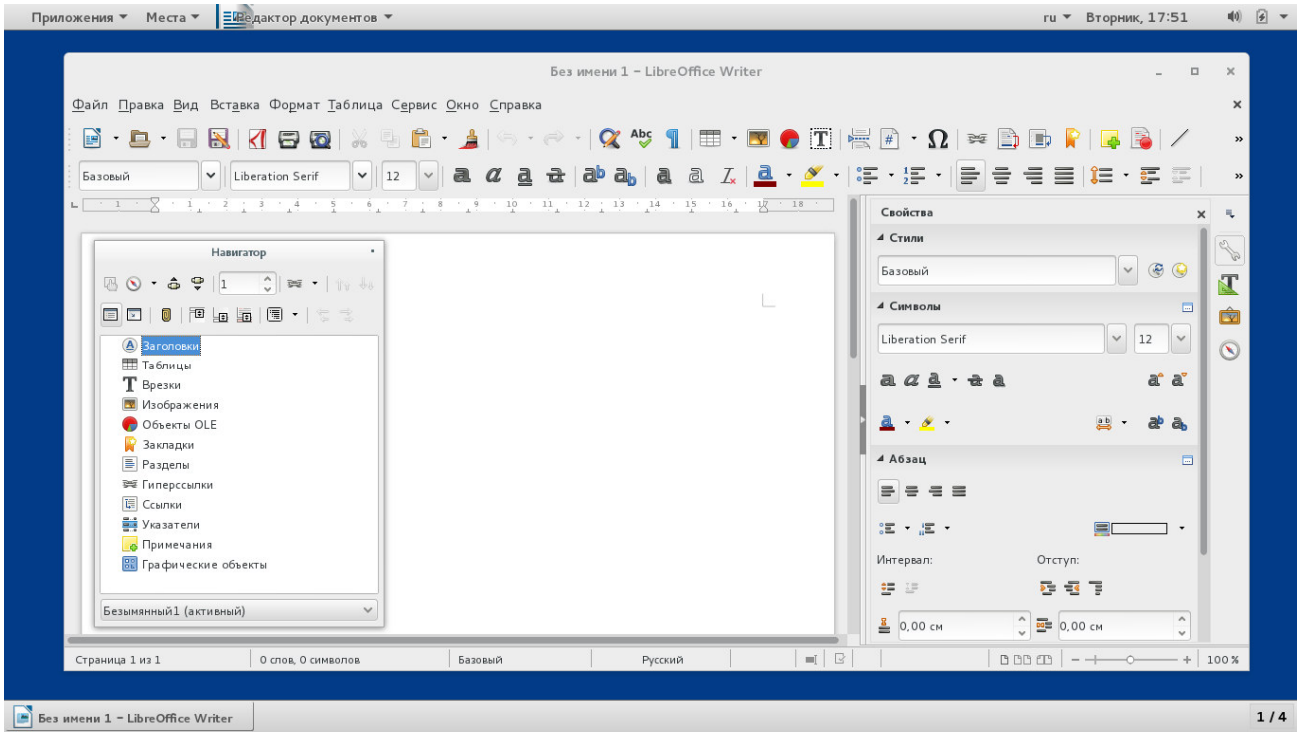
редактор формул LibreOffice Math, являющийся средством для создания и редактирования математических формул и уравнений, а также встраивания их в любые документы;

табличный процессор LibreOffice Calc, являющийся многофункциональным средством работы с таблицами и базами данных, с помощью которого можно создавать сложные формулы и динамические диаграммы, производить упорядочивание, выполнять расчеты и анализировать данные, подводить промежуточные и общие итоги (см. Снимок экрана 39);

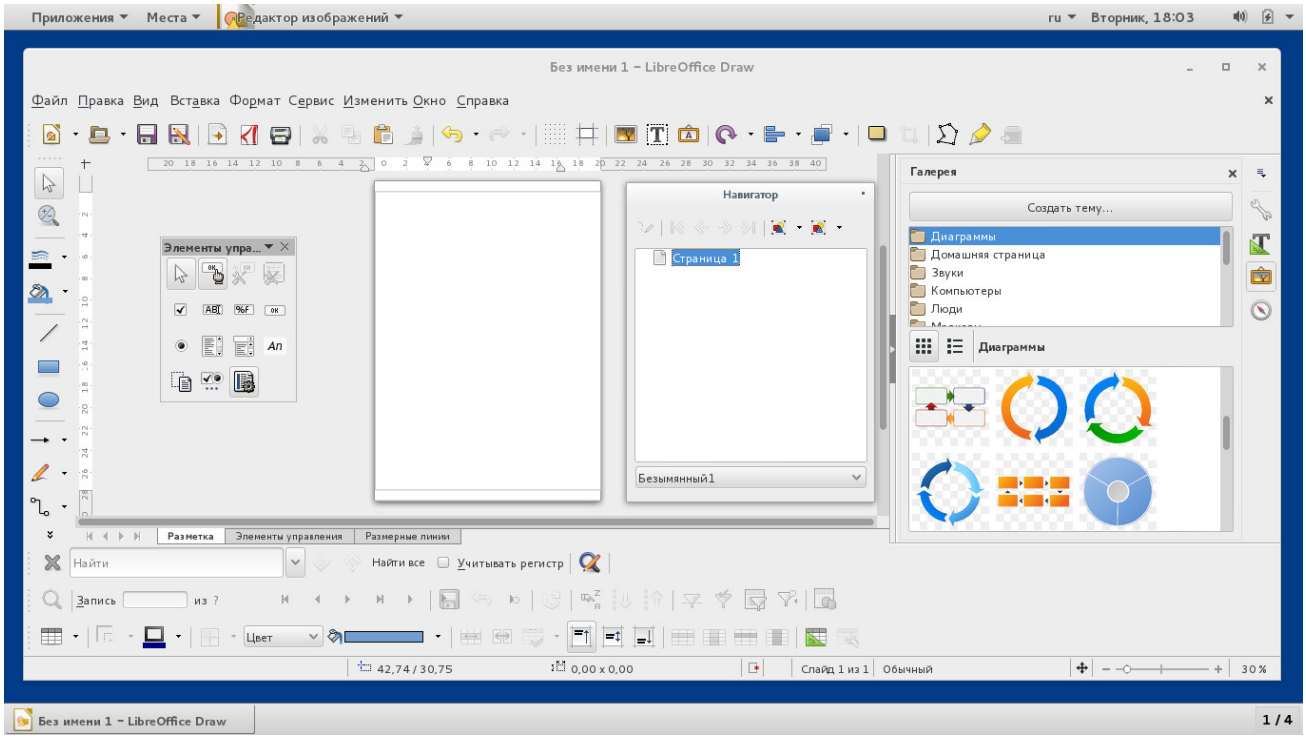
средство для работы с базой данных LibreOffice Base, обеспечивающее подключение к внешним источникам и базам данных для выполнения запросов, построения форм, отчетов и других представлений (см. Снимок экрана 40).



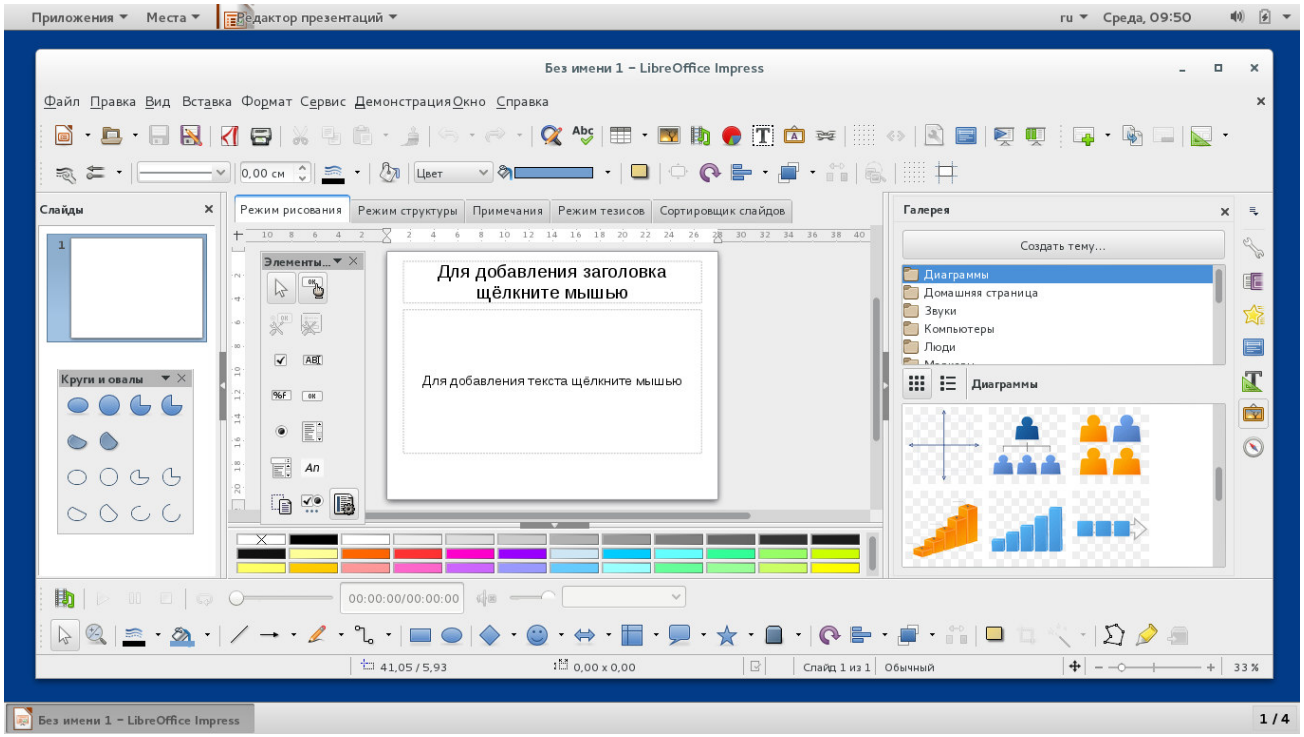

Снимок экрана 35 - Приложения - Офис



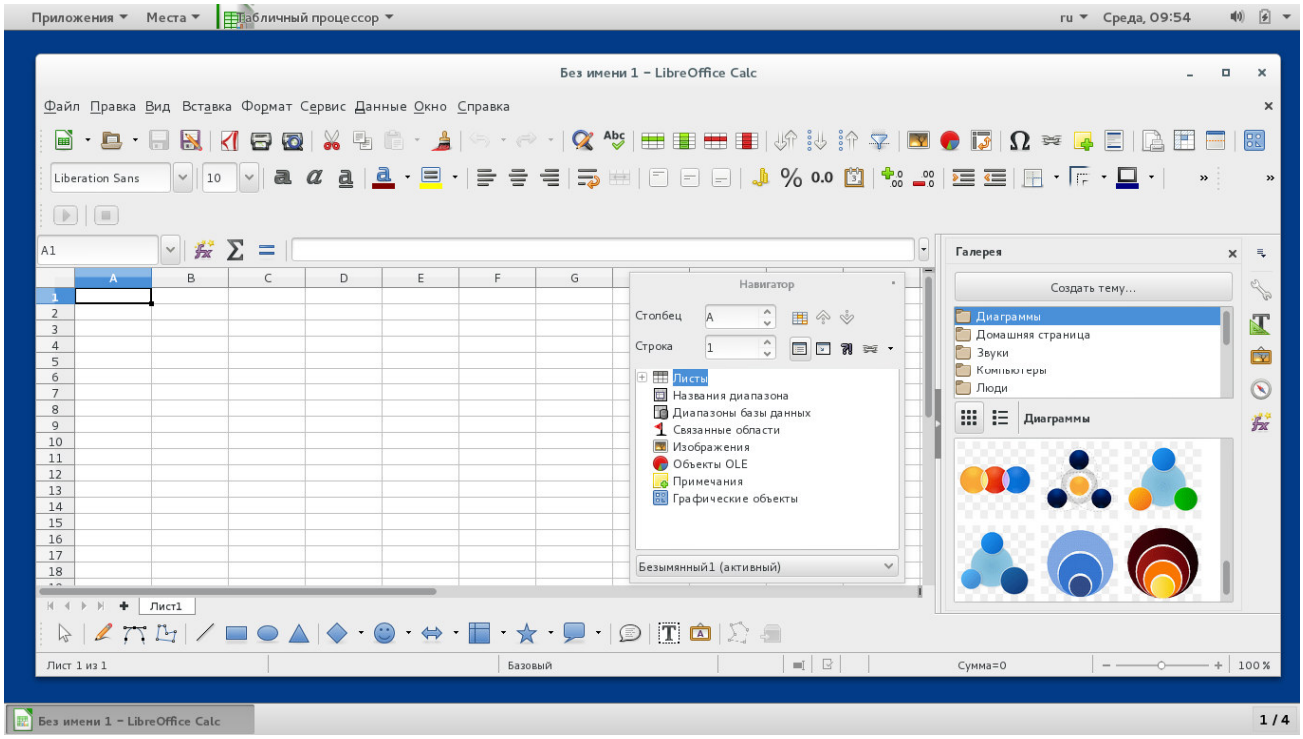

Снимок экрана 36 - Редактор документов LibreOffice Writer



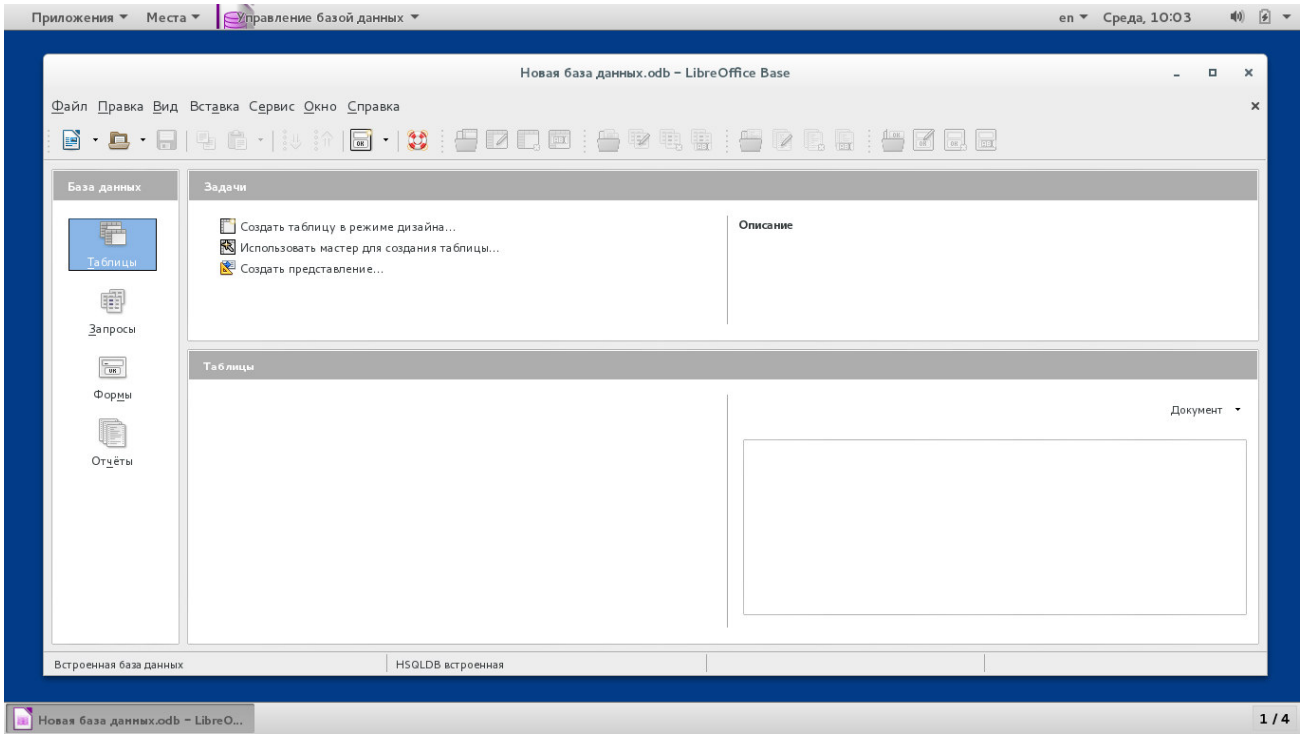

Снимок экрана 37 - Редактор изображений LibreOffice Draw




Снимок экрана 38 - Редактор презентаций LibreOffice Impress




Снимок экрана 39 - Табличный процессор LibreOffice Calc

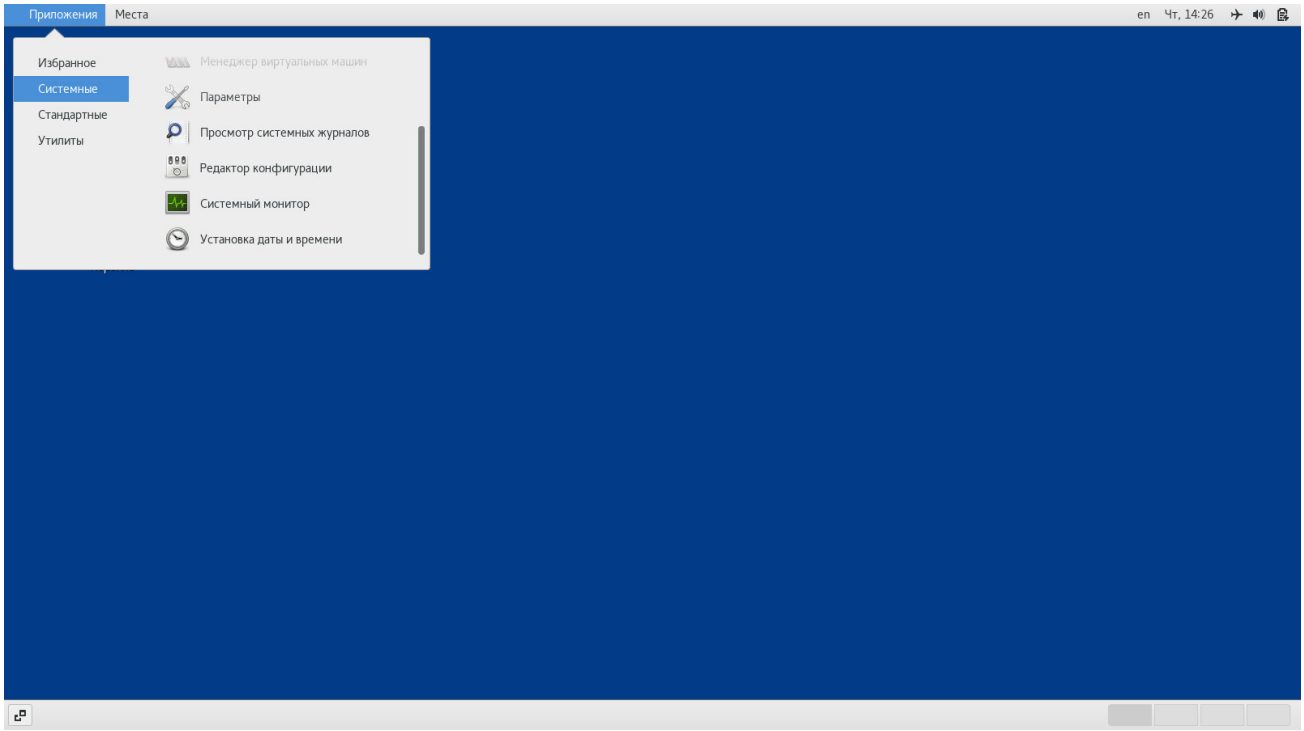



Снимок экрана 40 - Средство для работы с базой данных LibreOffice Base

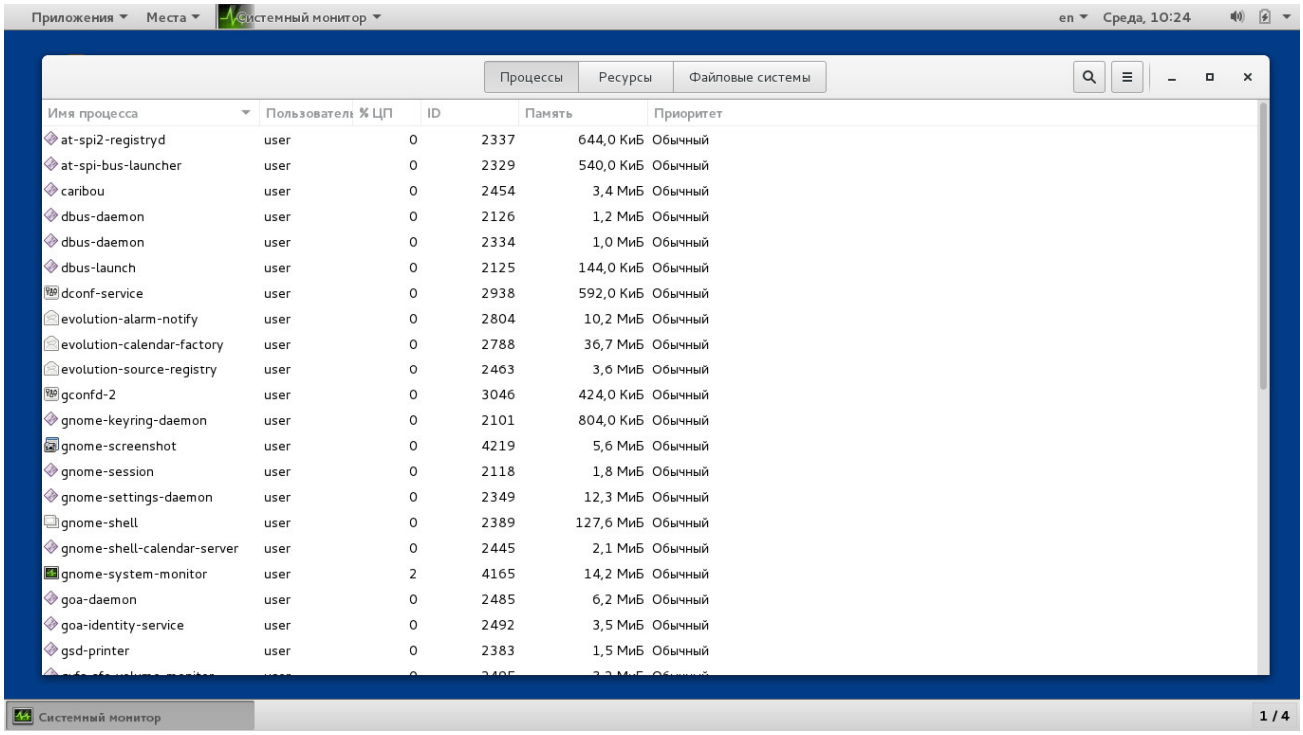
### 4.3 Системные

С помощью меню Системные пользователь может запускать следующие приложения (см. Снимки экрана 41, 42): приложение Boxes для доступа к удаленным и виртуальным машинам, приложение для определения и настройки автоматически запускаемых при старте системы программ, приложение Firewall-config для настройки межсетевого экрана, менеджер виртуальных машин Virtual Machine Manager, приложение для настройки системных параметров, приложение для просмотра системных журналов, редактор конфигурации пользовательских и системных настроек Gconf, системный монитор System Monitor для просмотра состояний текущих процессов (см. Снимок экрана 42) и ресурсов системы (см. Снимок экрана 43), приложение System-Config-Date для установки даты и времени.

Для настройки межсетевого экрана, управления виртуальными машинами, просмотра системных журналов и установки даты и времени требуются полномочия администратора.




Снимок экрана 41 - Приложения - Системные

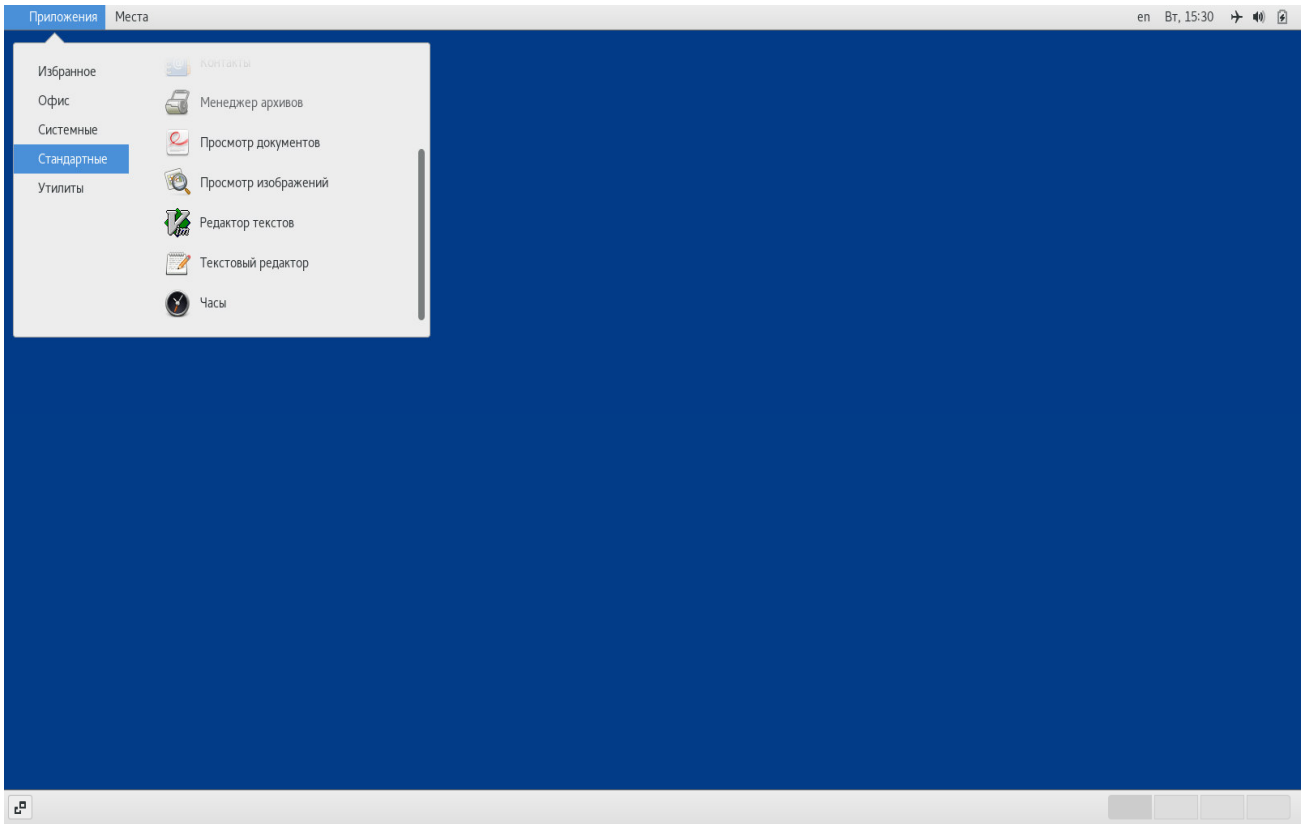



Снимок экрана 42 - Системный монитор процессов

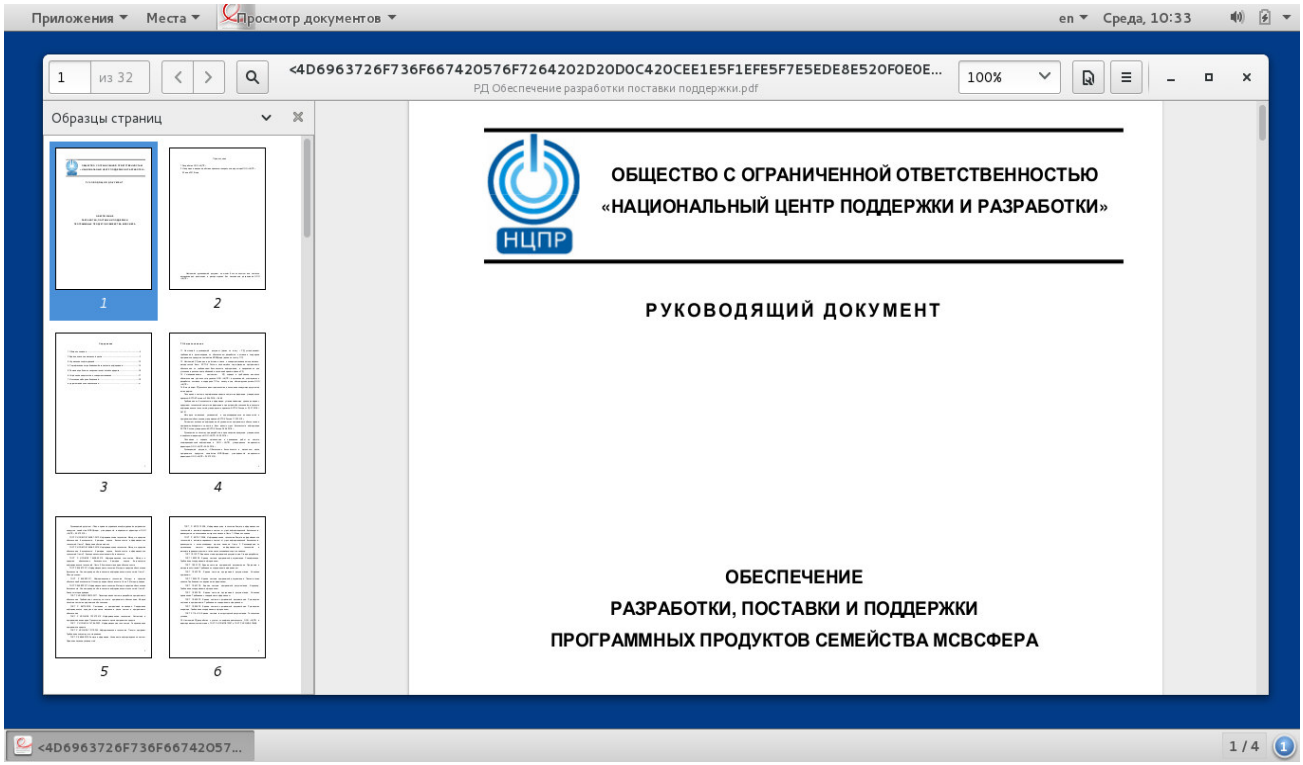

Снимок экрана 43 - Системный монитор ресурсов

### 4.4 Стандартные

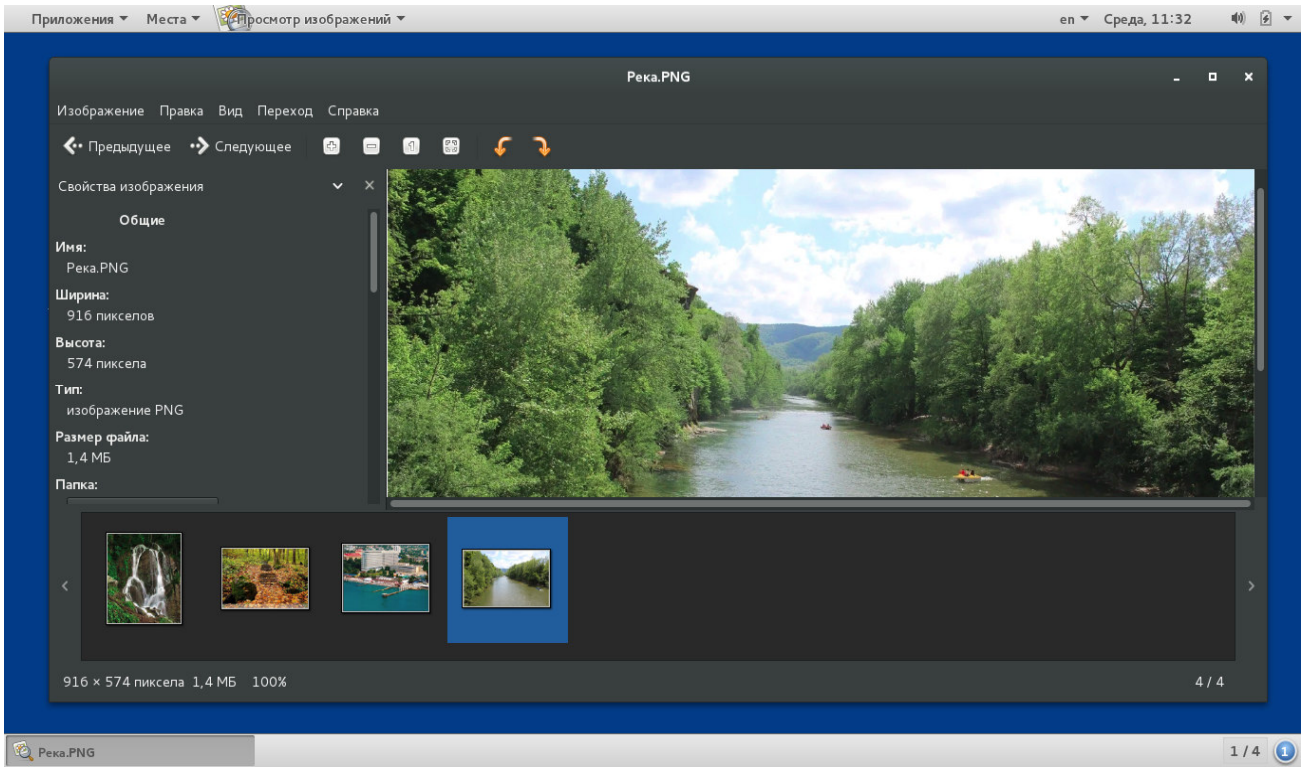
С помощью меню Стандартные пользователь может запускать следующие приложения (см. Снимок экрана 44): приложение Gnote для ведения заметок, приложение Brasero для записи оптических дисков, калькулятор, приложение для ведения контактов, менеджер архивов, приложение Evince для просмотра документов (см. Снимок экрана 45), приложение Eye для просмотра изображений (см. Снимок экрана 46), улучшенный редактор текстов Vi, текстовый редактор Gedit, часы для организации времени (см. Снимок экрана 47).



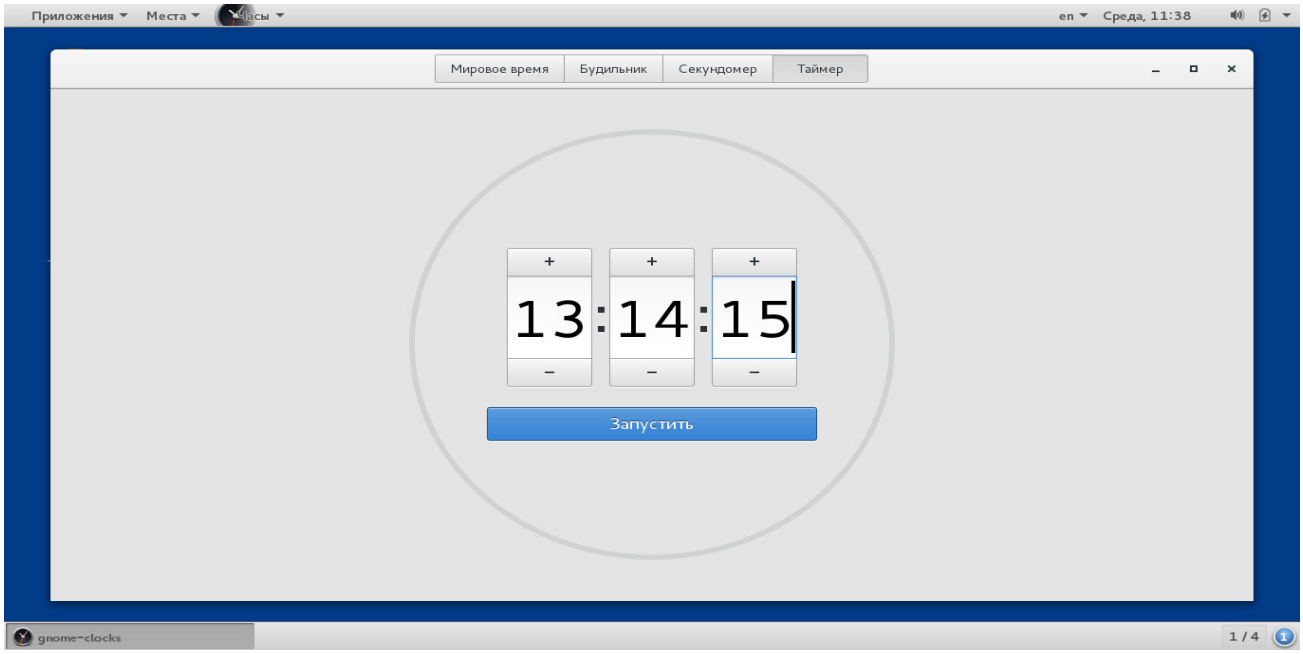

Снимок экрана 44 – Приложения – Стандартные




Снимок экрана 45 - Просмотр документов




Снимок экрана 46 - Просмотр изображений

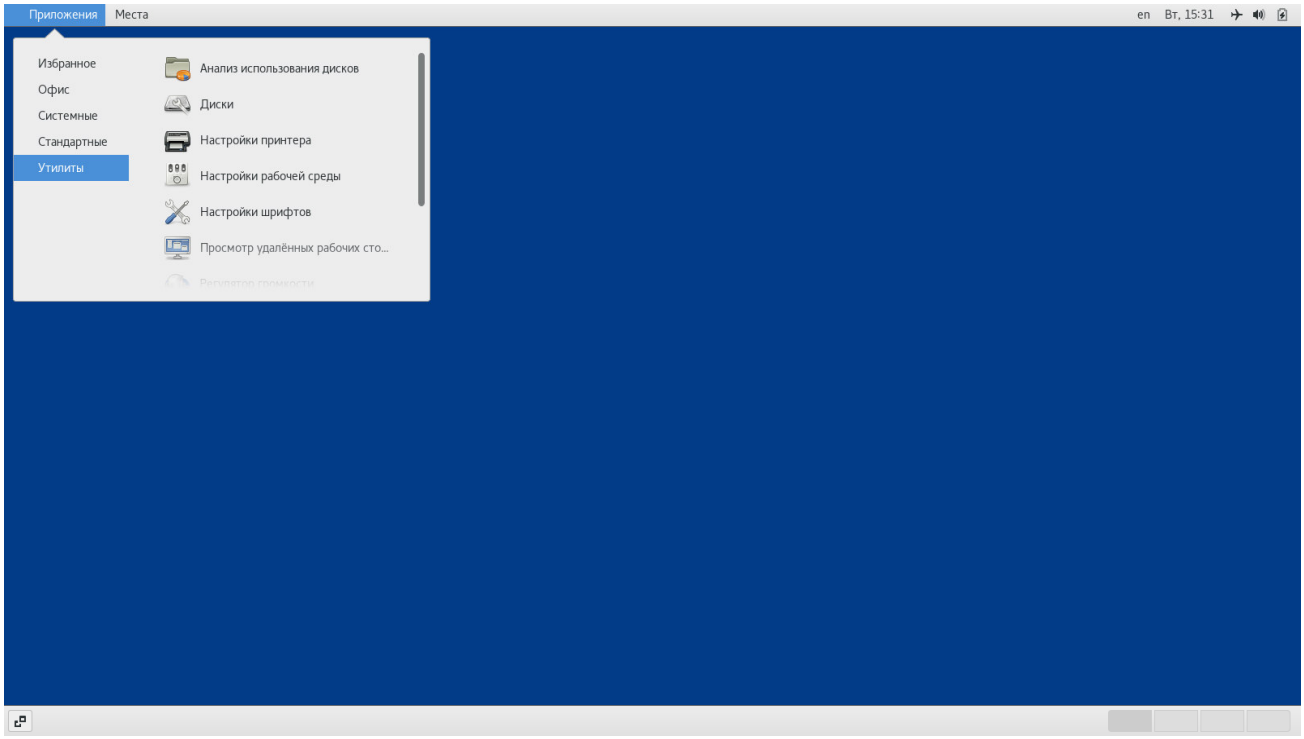



Снимок экрана 47 - Часы – Таймер

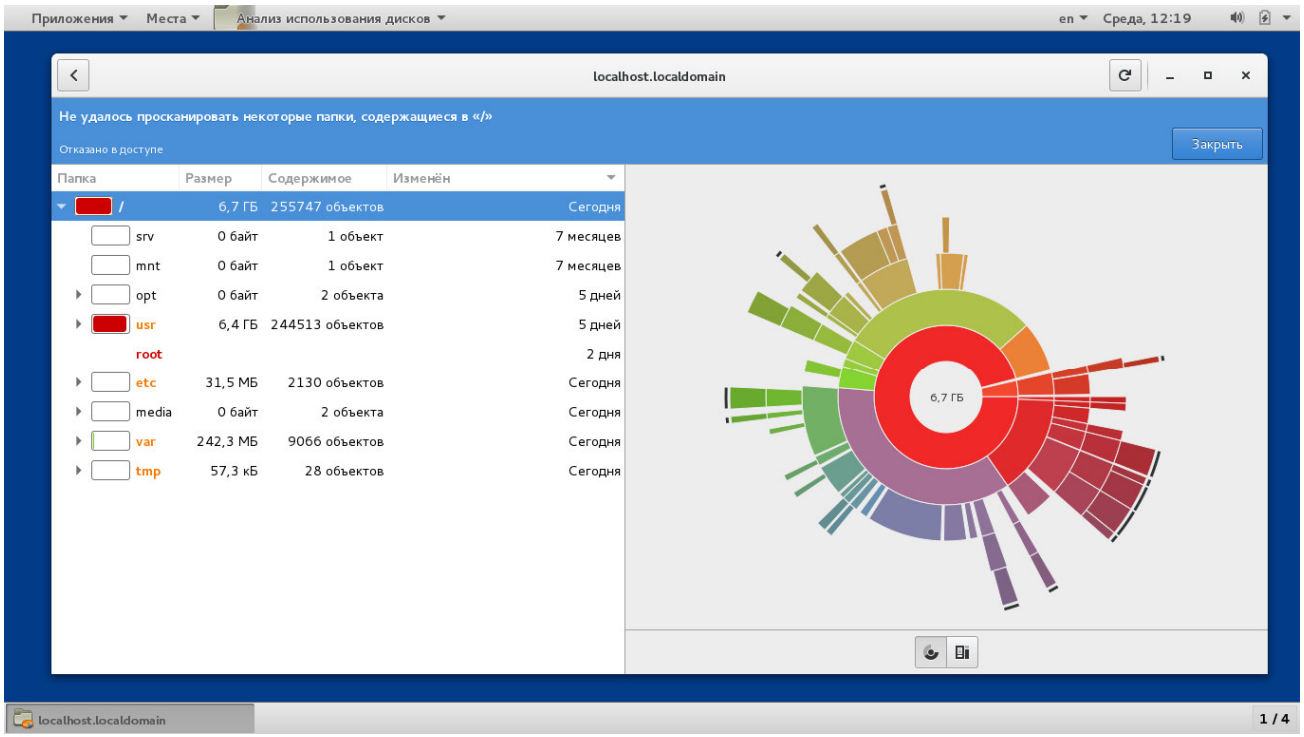
### 4.5 Утилиты

С помощью меню Утилиты пользователь может запускать следующие приложения (см. Снимок экрана 48): приложения Baobab и Disks для анализа использования дисков (см. Снимок экрана 49), приложение для настройки принтера, приложение для настройки параметров рабочей среды, приложение Vinagre для просмотра удаленных рабочих столов, приложение для регулирования громкости, приложение для получения снимков (скриншотов) и видео (скринкастов) с экрана, таблица символов, шрифты.

.




Снимок экрана 48 - Приложения - Утилиты




Снимок экрана 49 - Анализ использования дисков

| Лист регистрации изменений | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Номера листов (страниц) | | | | | Всего листов (страниц) в докум. | № документа | Входящий № сопроводи-тельного докум. и дата | Подп. | Дата |
| Изм | измененных | замененных | новых | аннулиро-ванных | | | | | |
| | | | | | | | | | |