

УТВЕРЖДЕН

**МСВСфера 8 Сервер**  
**Руководство пользователя**

Инов. № подп.	Подпись и дата	Взам. инв №	Инов. № дубл.	Подпись и дата

# Оглавление

<b>Аннотация</b>	<b>3</b>
<b>Общие сведения</b>	<b>4</b>
Назначение и область применения . . . . .	4
Политика информационной безопасности . . . . .	4
Принципы и правила безопасной работы . . . . .	5
Роли пользователей и доступные им средства и интерфейсы . . . . .	7
Типы регистрируемых событий безопасности . . . . .	9
Действия и режимы работы после сбоев и ошибок . . . . .	10
<b>Вход, перезапуск и выключение системы</b>	<b>11</b>
Вход в систему . . . . .	11
Структура меню . . . . .	11
<b>Пользовательские настройки</b>	<b>18</b>
<b>Решение задач пользователей</b>	<b>36</b>
Специальные возможности графического окружения рабочего стола . . . . .	36
Технология единого входа (SSO) браузеров . . . . .	42
<b>Приложения</b>	<b>45</b>
<b>Центр приложений</b>	<b>48</b>

## Аннотация

Настоящее руководство ориентировано на специалистов, знакомых с операционными системами и имеющих минимальный практический опыт работы с ними.

Руководство предназначено для пользователей серверной операционной системы с интегрированными серверными службами МСВСфера 8 Сервер. Руководство снабжено примерами, сделанными в операционной системе МСВСфера 8 Сервер, установленной в базовой конфигурации.

# Общие сведения

## Назначение и область применения

**МСВСфера 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.

Операционная система МСВСфера предназначена для организации многоцелевых серверов на базе 64-х разрядных аппаратных платформ Intel и AMD, а также платформ ARM архитектуры aarch64 (начиная с версии 9). 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 удостовериться в такой совместимости путем пробного тестирования.

## 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 её 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 её 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 её 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.

## **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 её 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 её 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.

## **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;
- 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 её 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 консольным, ориентированным на взаимодействие в терминальном режиме с помощью командной строки, задающей команды и дополнительные параметры, результаты выполнения которых выводятся в виде текстовых сообщений.

## 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.

## **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 результат, 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.

# Вход, перезапуск и выключение системы

## Вход в систему

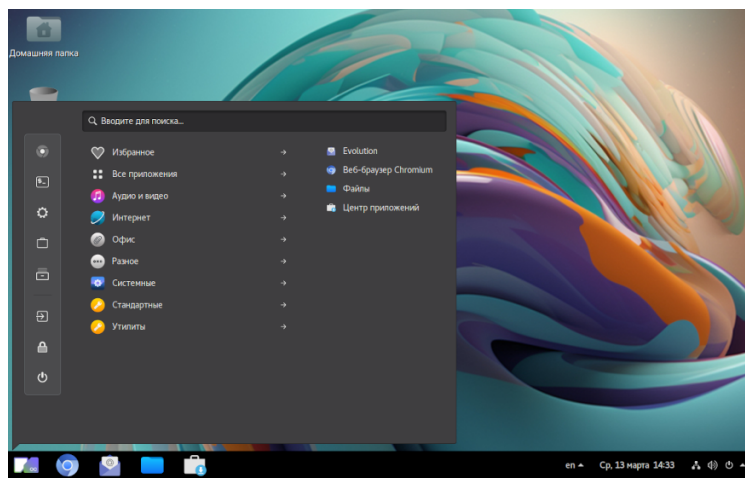
Вход пользователя в систему начинается с идентификации и аутентификации, в ходе которых он выбирает свое имя из предлагаемого системой списка имен зарегистрированных пользователей и предъявляет пароль.

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.

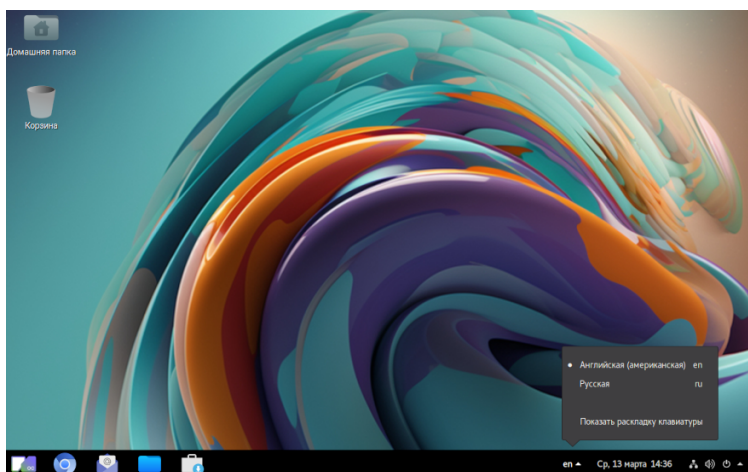
## Структура меню

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

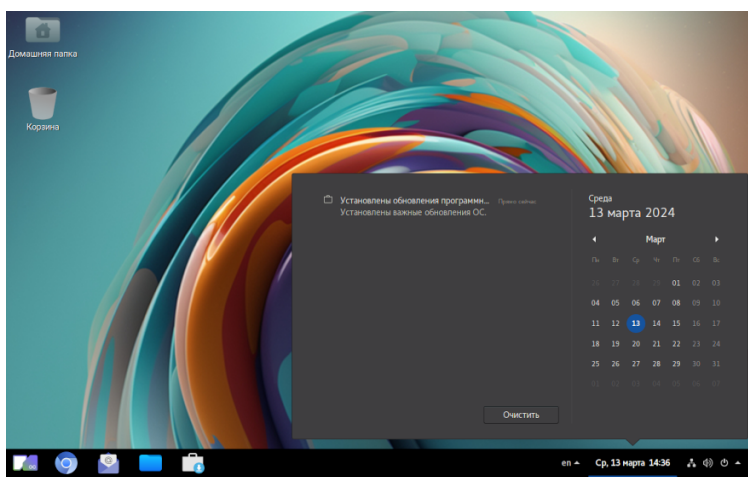
Меню «Приложения», предоставляющее возможность запуска интегрированных в систему приложений:



Меню выбора языка ввода:



Меню настройки даты и времени:

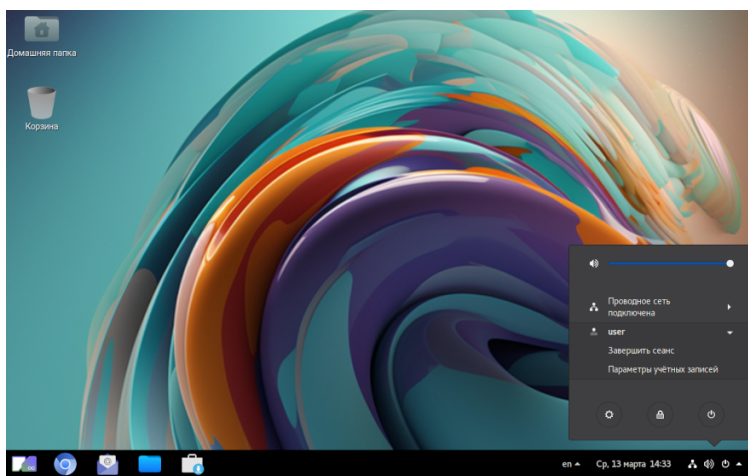


Здесь также можно увидеть последние уведомления системы и включить/выключить режим «Не беспокоить».

Системное меню, предоставляющее возможность настройки некоторых системных параметров, а также возможность завершения сеанса, блокировки экрана, перезапуска и выключения системы.

Системное меню.

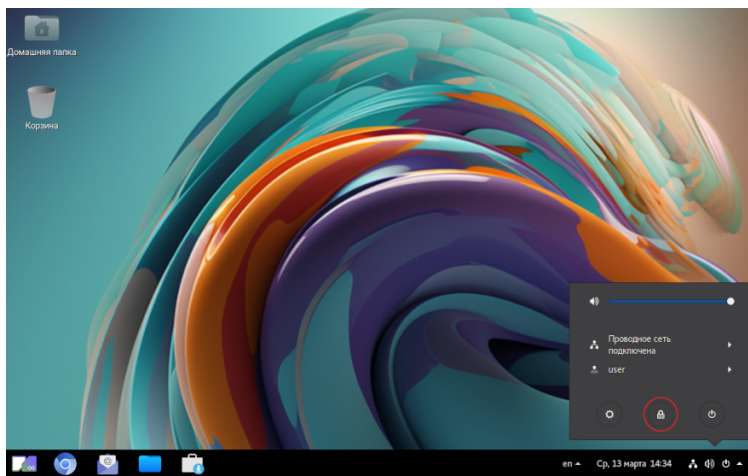




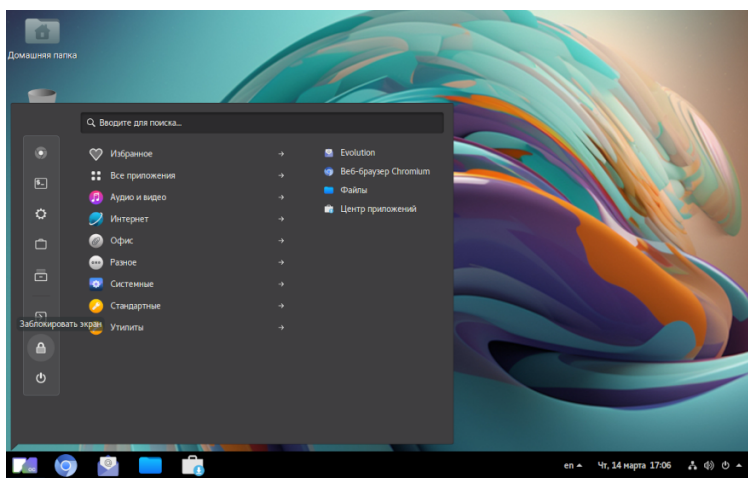
Подробнее о составе и функциональных возможностях вышеперечисленных меню изложено ниже.

### Блокировка экрана

Блокировка экрана осуществляется нажатием в системном меню «Заблокировать» (путем наведения на нее курсора и нажатия кнопки мыши):



Либо из меню «Приложения».

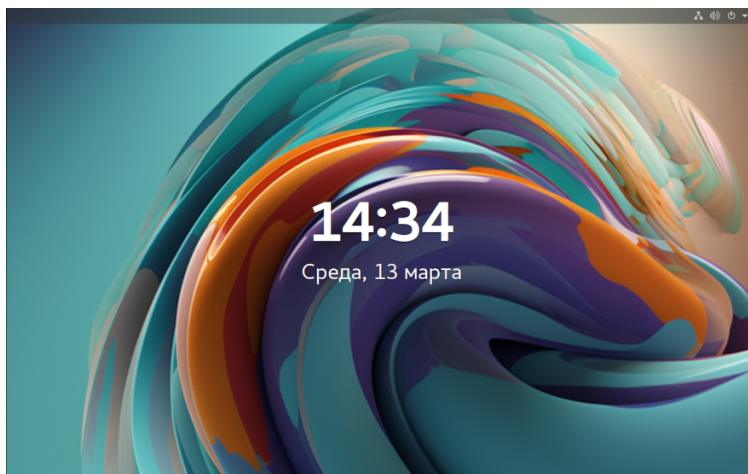


Также вы можете выполнить блокировку экрана нажатием клавиш **Super** + **L**.

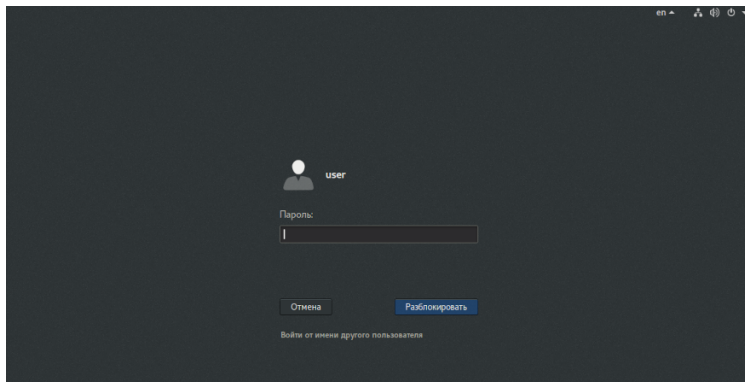
### Важно

Клавиша «Super» располагается, как правило, в левом нижнем углу клавиатуры рядом с клавишей **Alt**. На многих клавиатурах на клавише «Super» изображён логотип Windows. Иногда её называют клавишей Windows или системной клавишей.

Блокировка сопровождается появлением экрана блокировки:

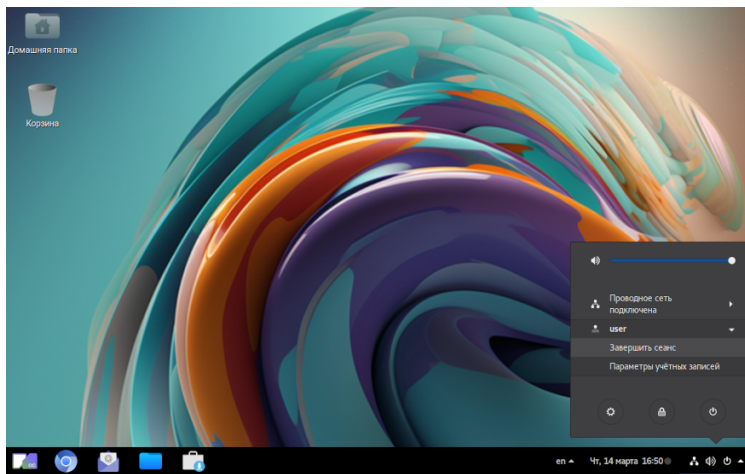


Для разблокировки экрана необходимо нажать на клавиатуре или мыши любую клавишу и снова предъявить свой пароль:

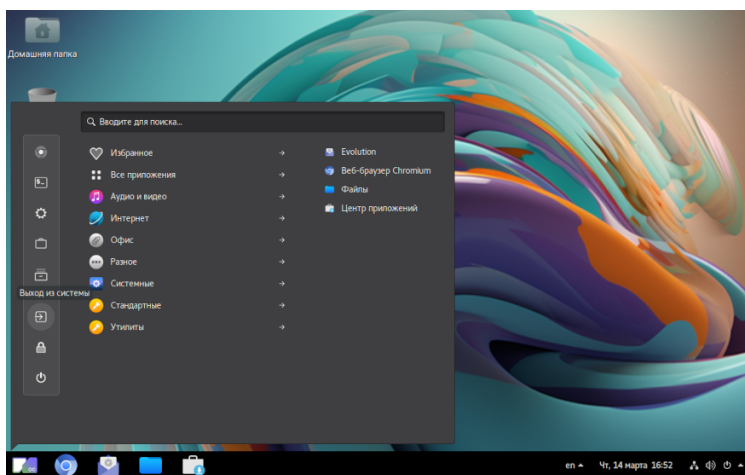


## Завершение сеанса

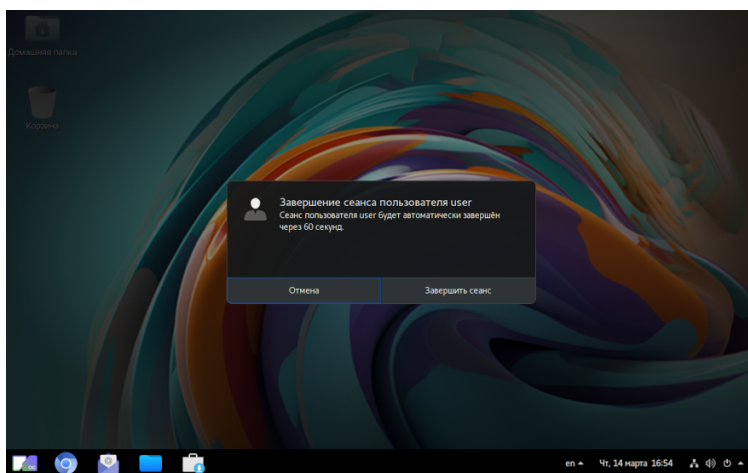
Завершение сеанса работы пользователя с системой осуществляется нажатием в системном меню на имя пользователя и выбором «Завершить сеанс»:



Или в меню «Приложения» нажатием на значок выхода из системы.



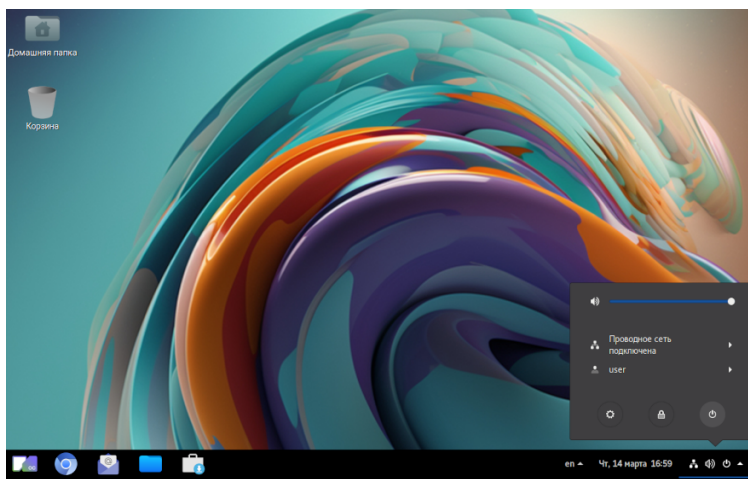
И подтверждением данного выбора:



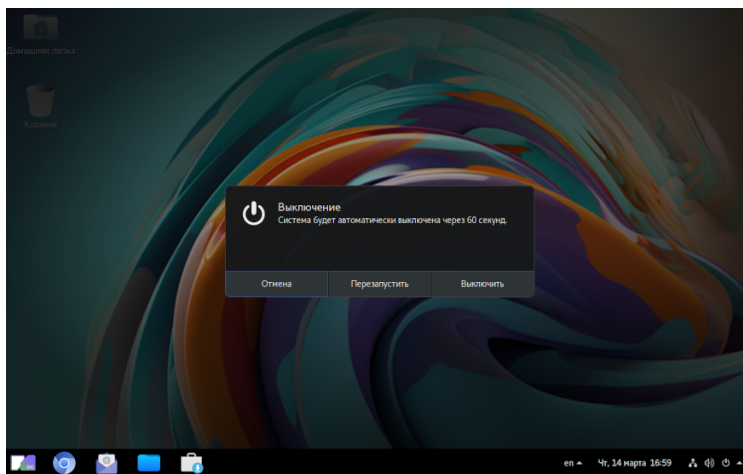
Завершение сеанса сопровождается завершением работы всех запущенных пользователем приложений.

## Перезапуск и выключение

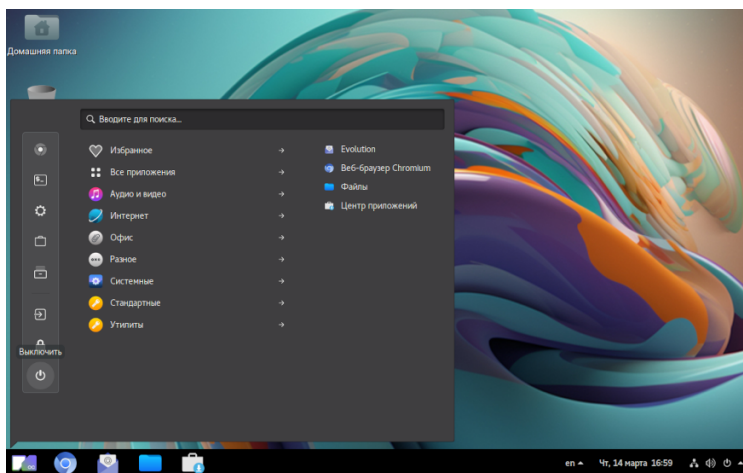
Перезапуск и выключение системы осуществляются нажатием в системном меню на «Выключить»:



И последующим нажатием на «Перезапустить» или «Выключить»:



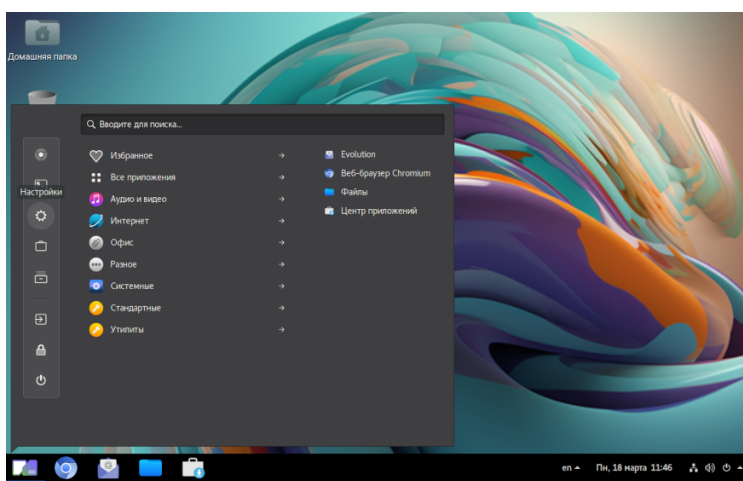
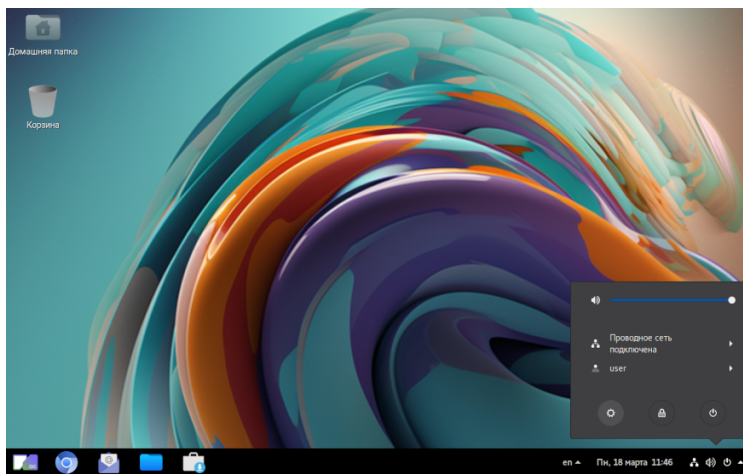
Или в меню «Приложения» нажатием на значок выключения и последующим нажатием на «Перезапустить» или «Выключить».





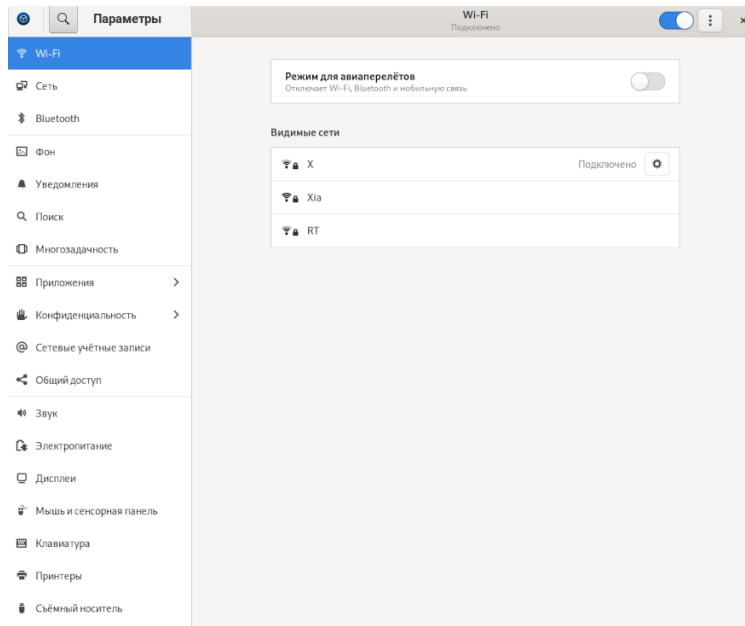
# Пользовательские настройки

Просмотр и изменение пользовательских настроек осуществляется нажатием в системном меню «Настройки» или нажатием на значок шестерёнки в меню «Приложения». С последующим выбором из появившегося на экране списка параметров тех из них, которые необходимо просмотреть и/или изменить.

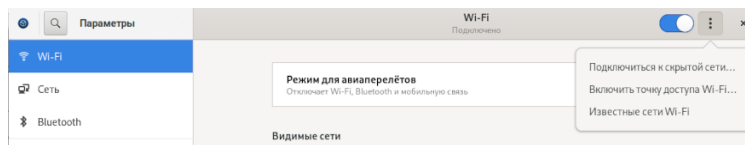


## Wi-Fi

Для настройки и просмотра параметров Wi-Fi перейдите в «**Настройки**» → «**Wi-Fi**». Здесь вы можете включить авиарежим и просмотреть список видимых сетей.



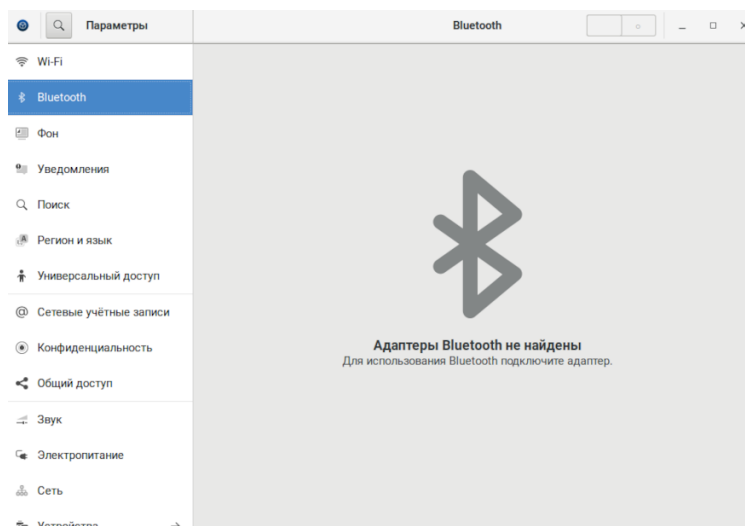
Нажмите на значок «три точки», чтобы включить дополнительные возможности Wi-Fi.



Нажмите на значок шестерёнки напротив подключённой сети, чтобы просмотреть подробную информацию о сети и пароль или забыть соединение.

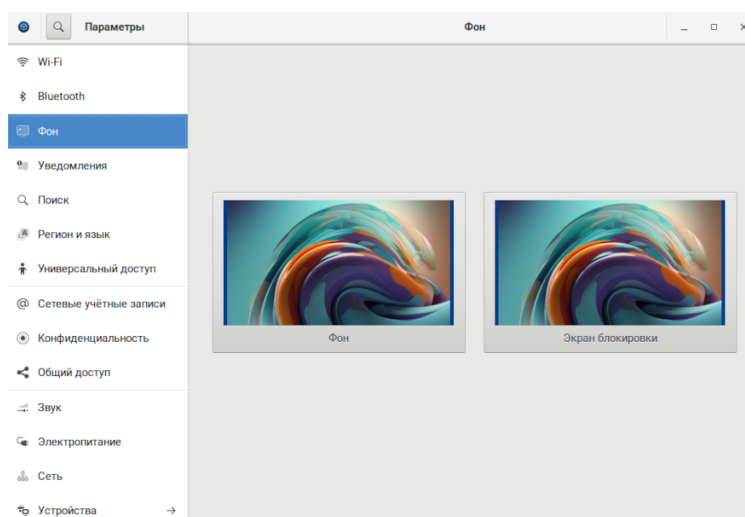
## Bluetooth

Для настройки и просмотра параметров Bluetooth перейдите в «**Настройки**» → «**Bluetooth**». Для подключения устройства выберите его из списка.



## Фон

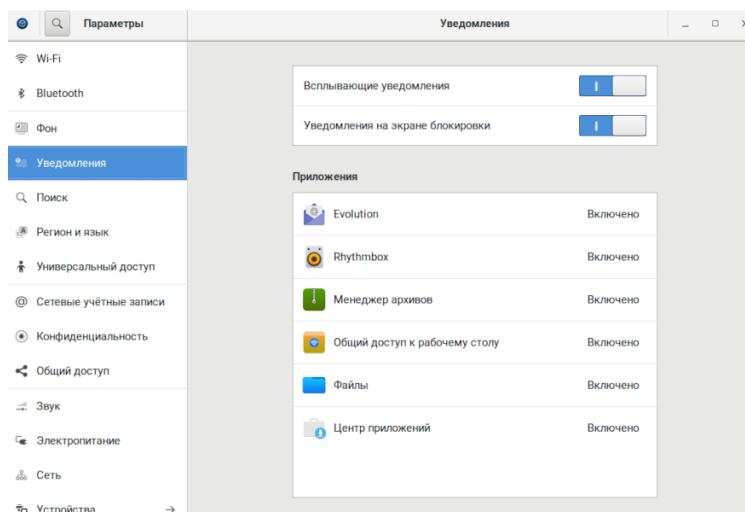
Перейдите в «**Настройки**» → «**Фон**» для выбора и добавления изображения рабочего стола.



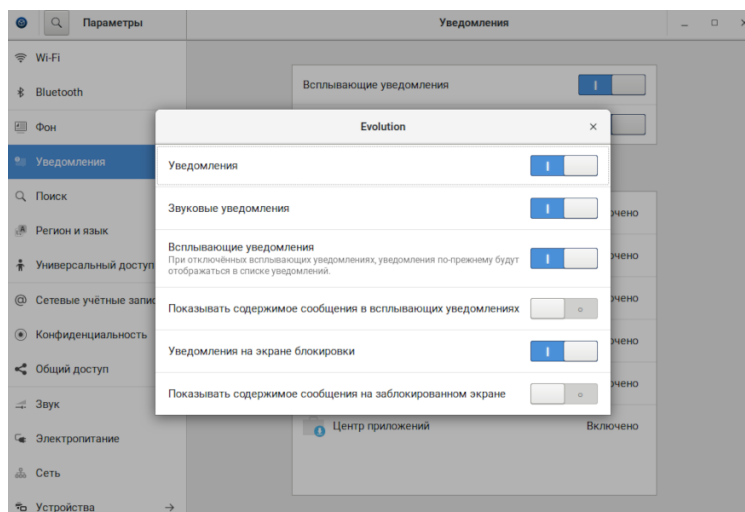
## Уведомления

Перейдите в «**Настройки**» → «**Уведомления**» для настройки уведомлений приложений или включения/выключения режима «**Не беспокоить**».





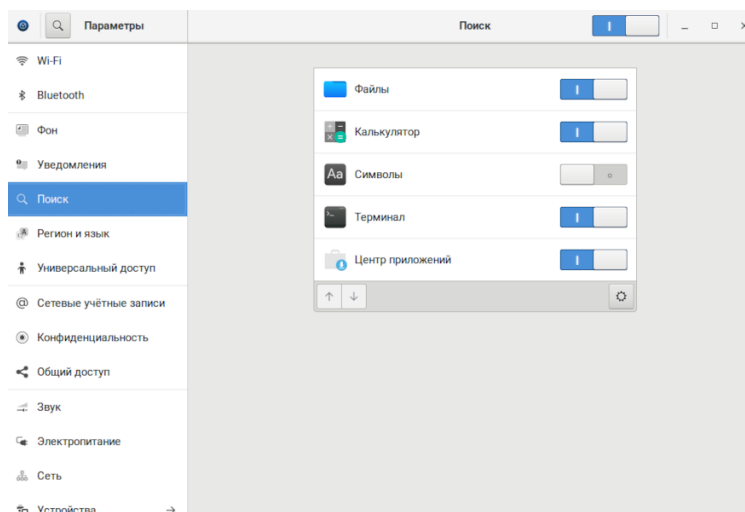
Нажмите на приложение для настройки уведомлений отдельно для него.



## Поиск

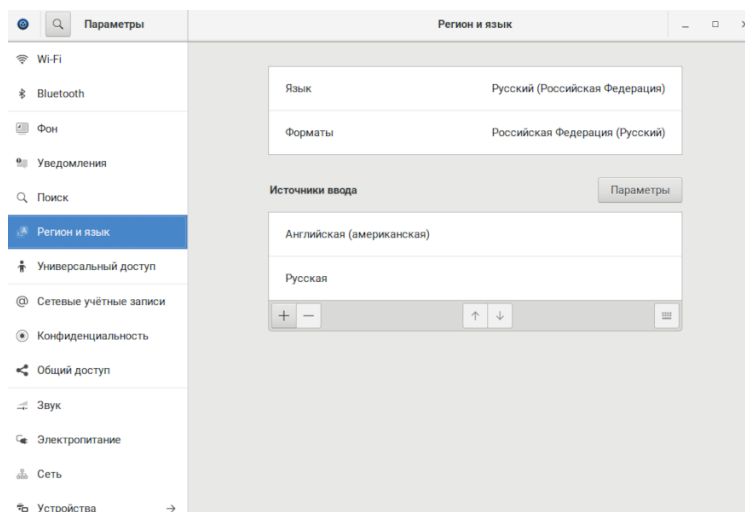
Перейдите в «**Настройки**» → «**Поиск**» для настройки вывода результатов поиска. Порядок результатов поиска можно изменить, перемещая строки в списке с помощью стрелок.

Выполнить дополнительные настройки вы можете, нажав на значок шестерёнки.



## Регион и язык

Для просмотра и настройки языка и формата отображения дат/чисел/валют перейдите в «**Настройки**» → «**Регион и язык**».

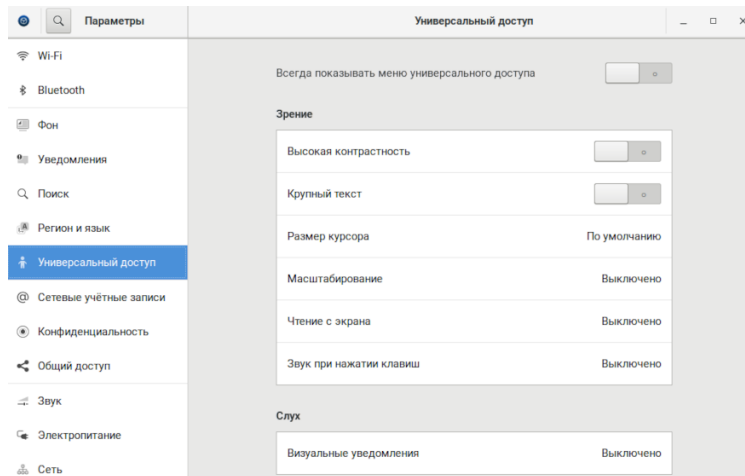


Для настройки соответствующих параметров нажмите на «**Язык**» или «**Форматы**».

Для настройки параметров источников ввода нажмите на «**Параметры**».

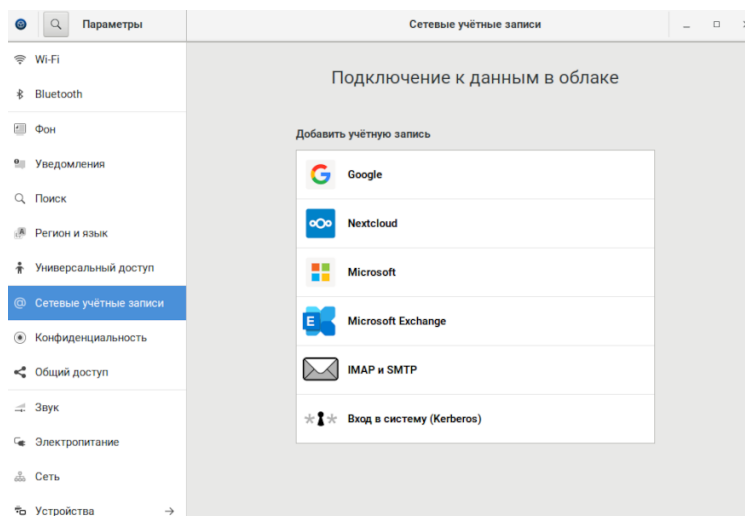
## Универсальный доступ

Для включения специальных возможностей универсального доступа перейдите в «**Настройки**» → «**Универсальный доступ**».



## Сетевые учётные записи

Для подключения вашей сетевой учётной записи в одной из систем облачного хранения данных перейдите в «Настройки» → «Сетевые учётные записи».



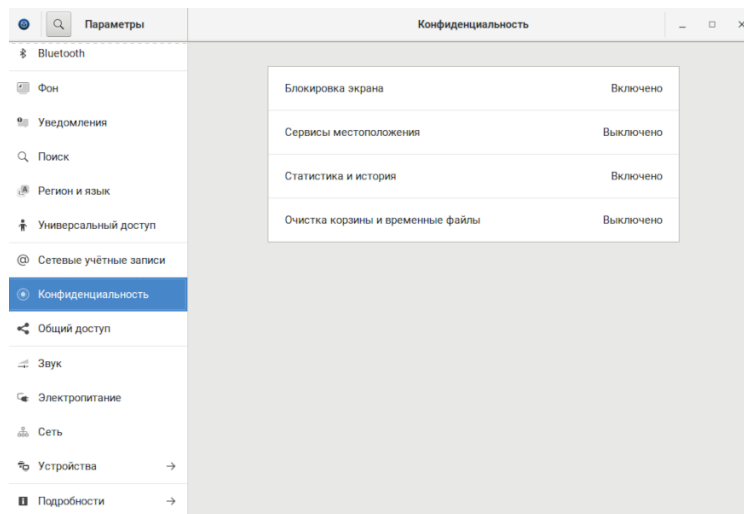
## Конфиденциальность

Здесь вы можете настроить следующие параметры:

- **Блокировка экрана.** Блокировка экрана будет выполняться после истечения установленного промежутка времени, которое, в свою очередь, будет отсчитываться от момента выключения экрана, настраиваемого с помощью приложения меню «Настройки» → «Электропитание» → «Выключение экрана».
- **Сервисы местоположения.** Включение сервисов местоположения позволяет автоматически изменять часовые пояса и синхронизировать текущее время.
- **Статистика и история.**

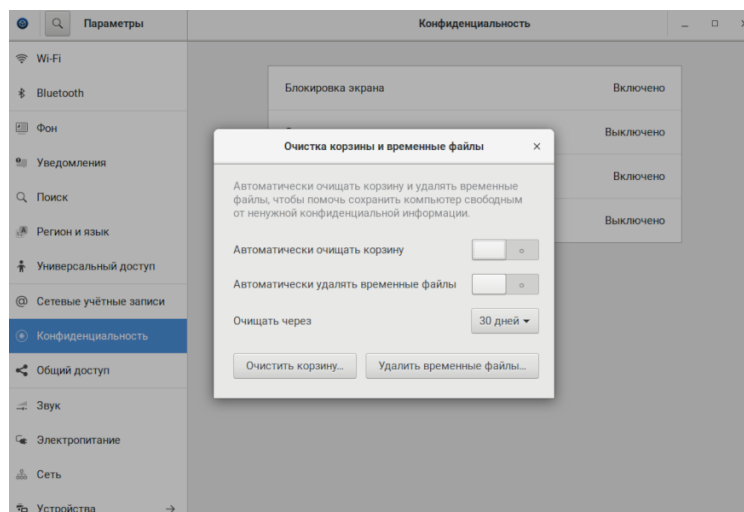
- Очистка корзины и временные файлы.

При нажатии на параметр, откроется диалоговое окно, в котором вы можете выполнить необходимые действия по настройке.



## Очистка корзины и временные файлы

Для настройки параметров автоматической очистки корзины и удаления временных файлов перейдите в «**Настройки**» → «**Конфиденциальность**» → «**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

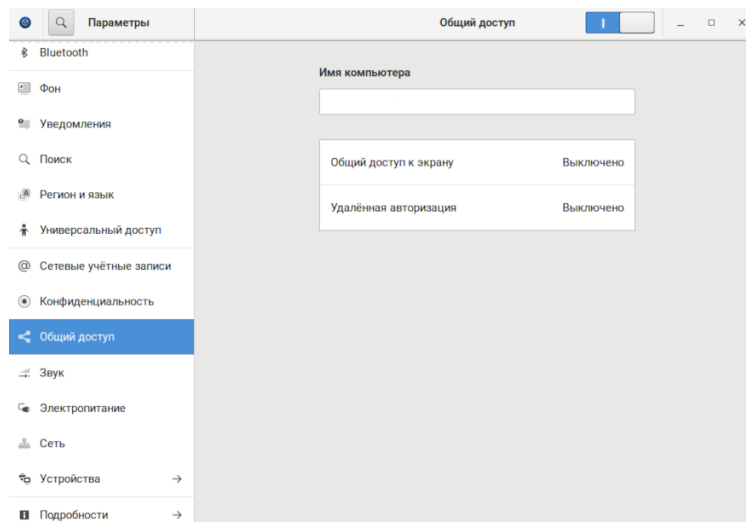
соответствующее действие, после чего подтвердить его.

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

Для безвозвратного удаления сразу всех временных файлов необходимо нажать кнопку «**Удалить временные файлы**» и подтвердить действие.

## Общий доступ

Общий доступ к экрану предоставляет возможность удалённого управления системой с использованием графического интерфейса пользователя.



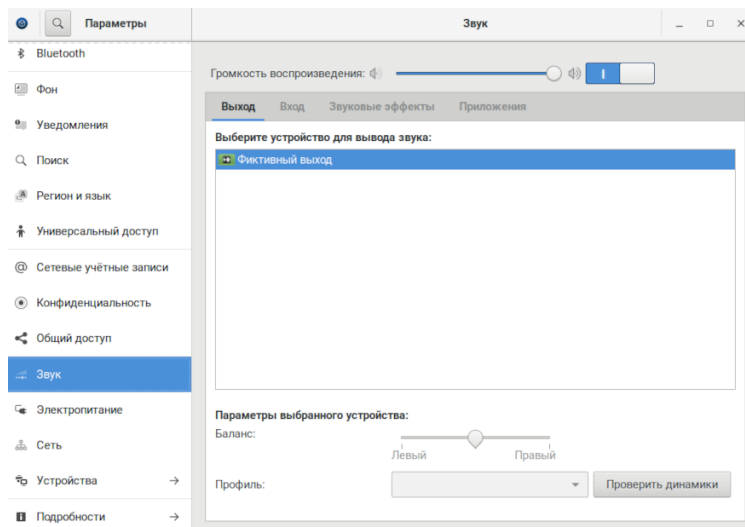
Для настройки параметров общего доступа к экрану перейдите в «**Настройки**» → «**Общий доступ**» и переведите переключатель в правом верхнем углу во включённое положение, затем нажмите на «**Общий доступ к экрану**».

Удаленная авторизация предоставляет возможность удаленным пользователям подключаться к системе при помощи SSH-соединения через терминал.

Для настройки параметров удалённой авторизации перейдите в «**Настройки**» → «**Общий доступ**» и переведите переключатель в правом верхнем углу во включённое положение, затем нажмите на «**Удалённая авторизация**».

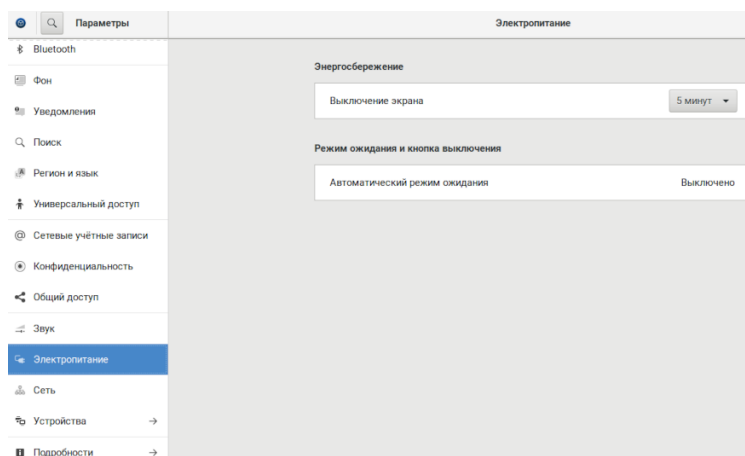
## Звук

Для просмотра и управления настройками звука перейдите в «**Настройки**» → «**Звук**».



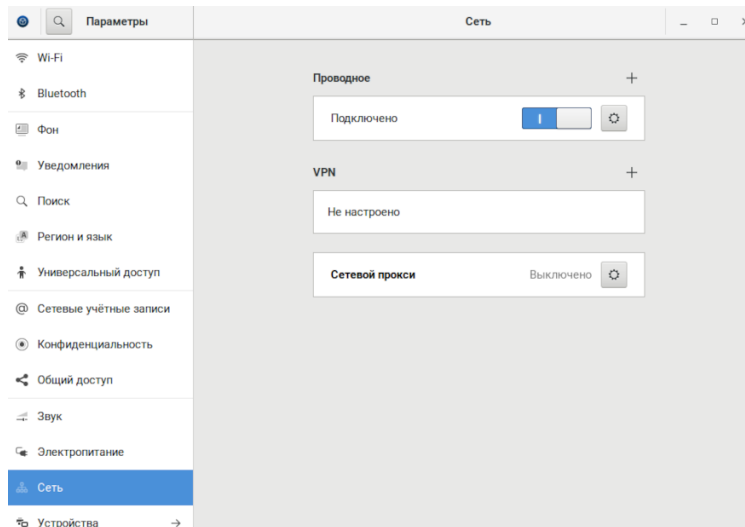
## Электропитание

Для просмотра и управления настройками электропитания перейдите в «Настройки» → «Электропитание».



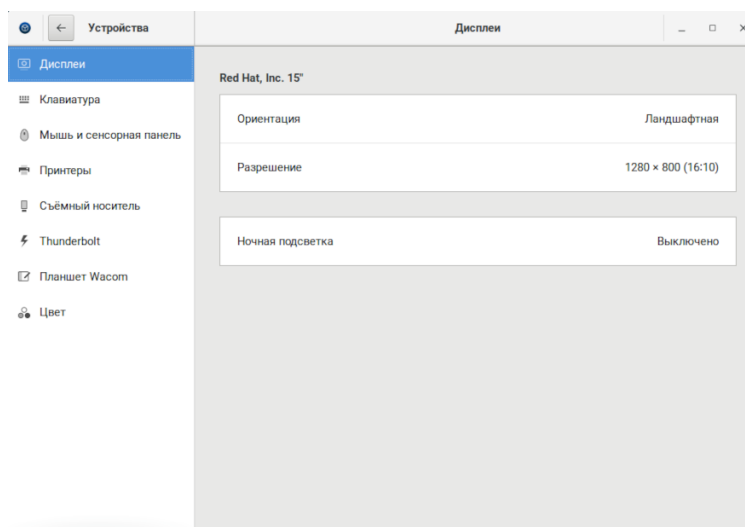
## Сеть

Для настройки и просмотра параметров сети и VPN перейдите в «Настройки» → «Сеть». Нажмите на значок шестерёнки для просмотра и настройки дополнительных параметров. Для добавления нового подключения или VPN нажмите на +, а затем выполните необходимые шаги.



## Устройства. Дисплей

Для просмотра и управления настройками встроенного дисплея перейдите в «Настройки» → «Устройства» → «Дисплей».



Для включения и настройки ночной подсветки нажмите «**Ночная подсветка**». Ночная подсветка делает цвет экрана теплее, что позволяет предотвратить напряжение глаз.

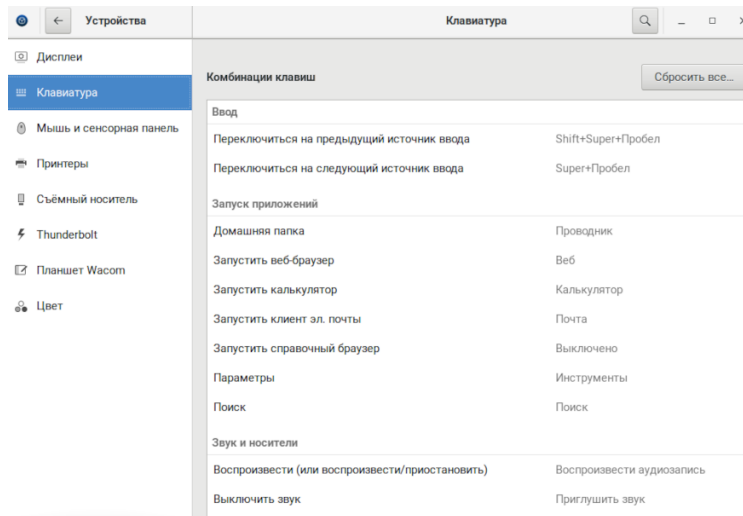
## Устройства. Клавиатура

### Важно

По умолчанию для переключения языка ввода используется комбинация клавиш **Super + Пробел**.

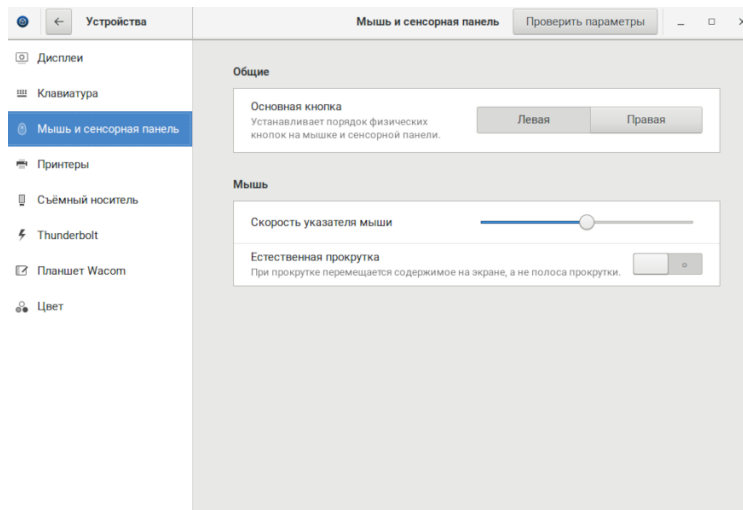
Клавиша «**Super**» располагается, как правило, в левом нижнем углу клавиатуры рядом с клавишей «**Alt**». На многих клавиатурах на клавише «**Super**» изображён логотип Windows. Иногда её называют клавишей Windows или системной клавишей.

Для просмотра и управления настройками клавиатуры панели перейдите в «**Настройки**» → «**Устройства**» → «**Клавиатура**».



## Устройства. Мышь и сенсорная панель

Для просмотра и управления настройками мыши и сенсорной панели перейдите в «**Настройки**» → «**Устройства**» → «**Мышь и сенсорная панель**».

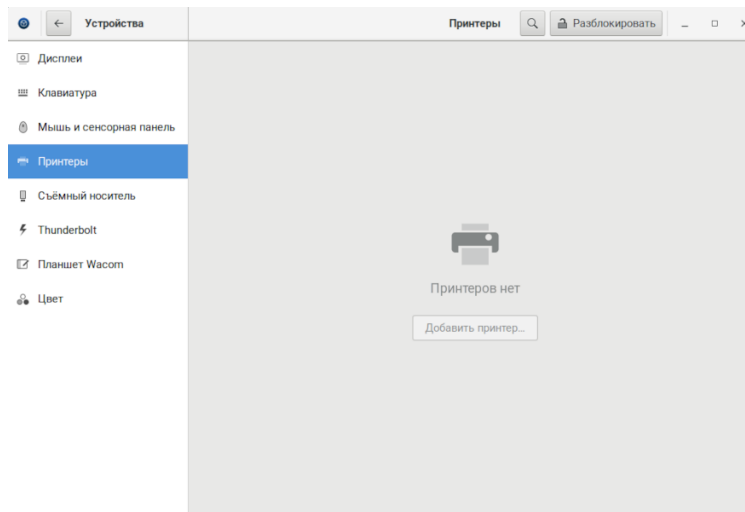


Нажмите на «**Проверить параметры**» для проверки работы мыши/сенсорной панели.

## Устройства. Принтеры

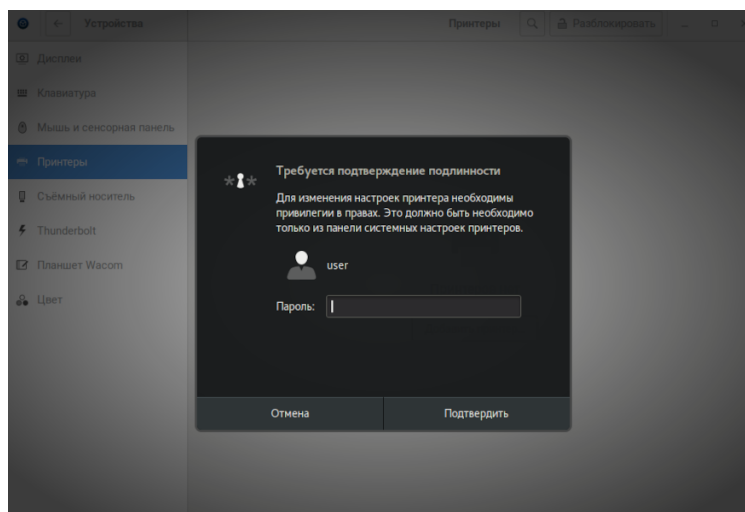


Для просмотра и добавления принтеров перейдите в «**Настройки**» → «**Устройства**» → «**Принтеры**».



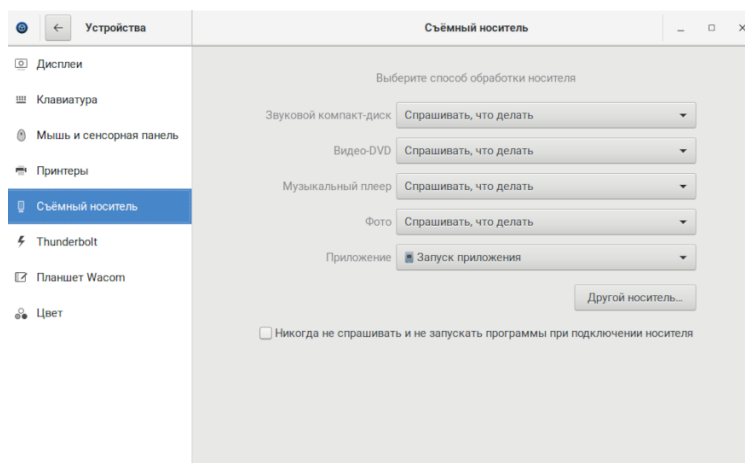
Чтобы разблокировать возможность изменения настроек нажмите «**Разблокировать**» и войдите в систему от имени одного из следующих пользователей:

- Суперпользователь;
- Пользователь с правами администратора `sudo` (такие пользователи перечислены в `/etc/sudoers`);
- Пользователь, принадлежащий группе `printadmin` в `/etc/group`.



## Устройства. Съёмный носитель

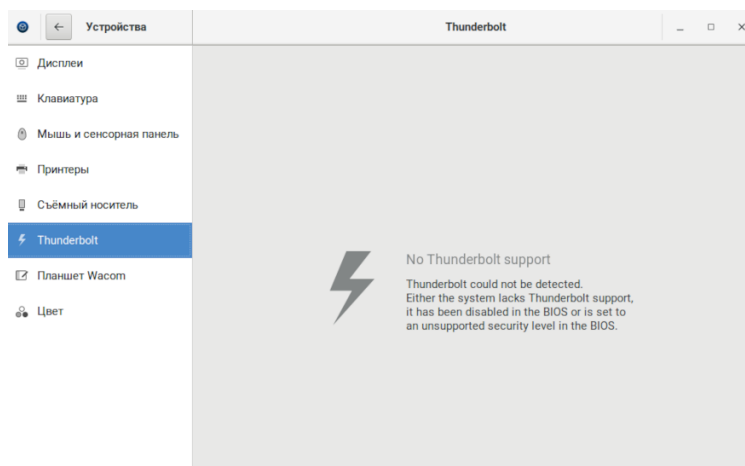
Для просмотра и настройки действий со съёмными носителями перейдите в «**Настройки**» → «**Устройства**» → «**Съёмный носитель**».



Для добавления нового носителя из списка возможных и настройки действий с ним нажмите «**Другой носитель**».

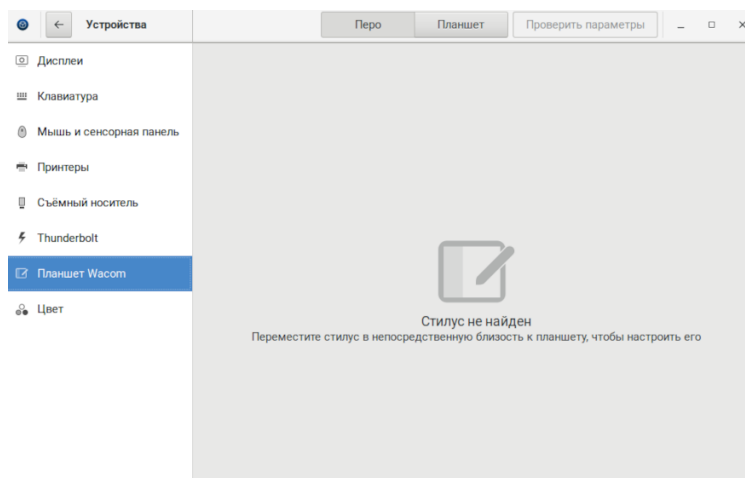
### Устройства. Thunderbolt

Для просмотра и настройки параметров аппаратного интерфейса Thunderbolt (при наличии) перейдите в «**Настройки**» → «**Устройства**» → «**Thunderbolt**».



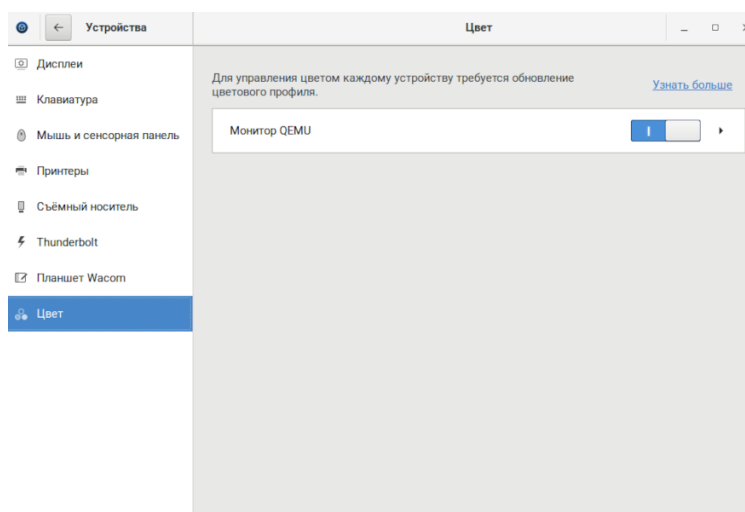
### Устройства. Планшет Wacom

Для просмотра и настройки параметров планшета и стилуса перейдите в «**Настройки**» → «**Устройства**» → «**Планшет Wacom**».



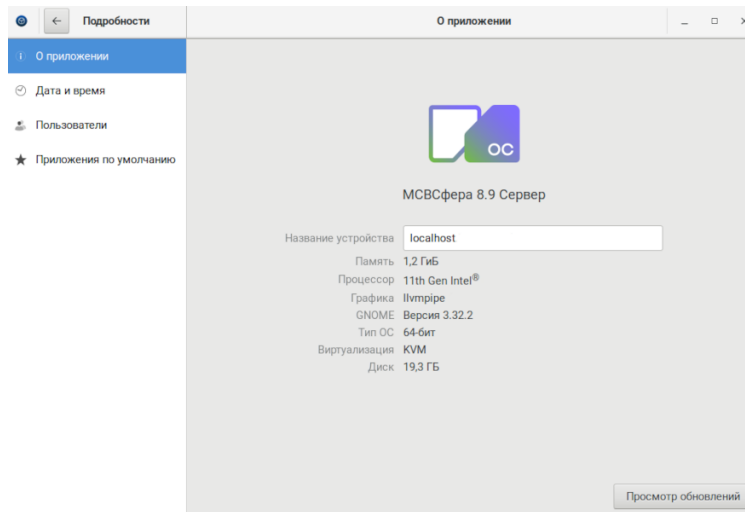
## Устройства. Цвет

Для управления цветом устройства перейдите в «**Настройки**» → «**Устройства**» → «**Цвет**».



## Подробности. О приложении

Для просмотра информации об операционной системе перейдите в «**Настройки**» → «**Подробности**» → «**О приложении**».



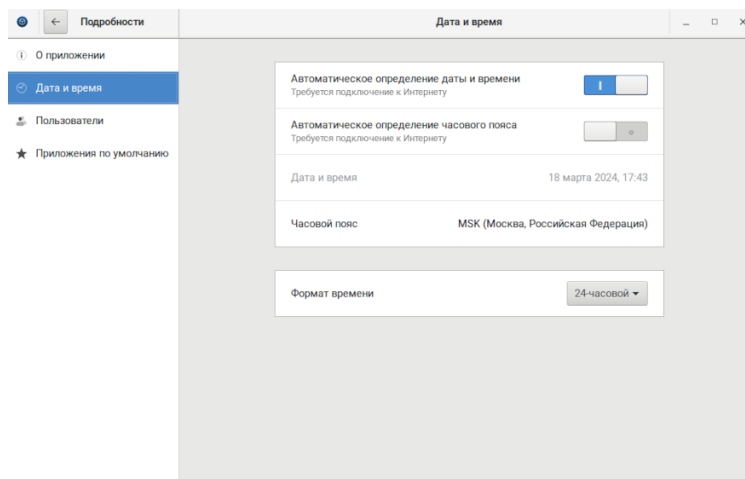
Для изменения имени устройства нажмите на «**Название устройства**».

### Проверка и загрузка обновлений

Для загрузки доступных обновлений нажмите на «**Просмотр обновлений**», вы будете перенаправлены в «**Центр приложений**» → «**Обновления**».

### Подробности. Дата и время

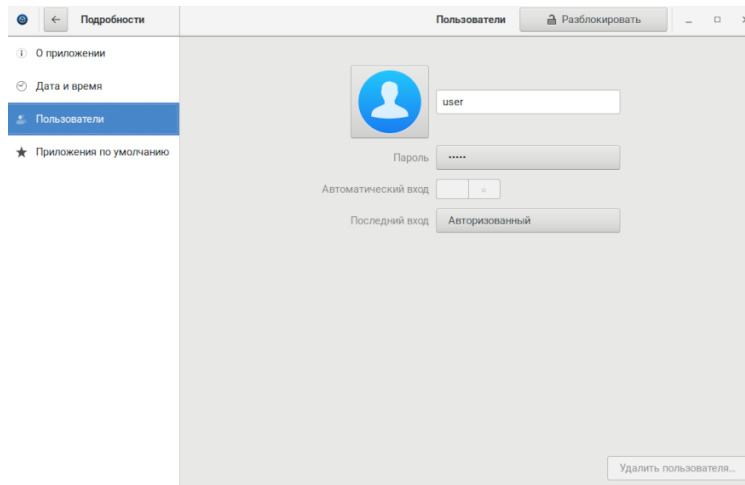
Для настройки даты и времени перейдите в «**Настройки**» → «**Подробности**» → «**Дата и время**».



### Подробности. Пользователи

Для изменения значений своего имени или пароля необходимо перейти в «**Настройки**» → «**Подробности**» → «**Пользователи**».

Здесь можно задать новое значение своего имени пользователя:



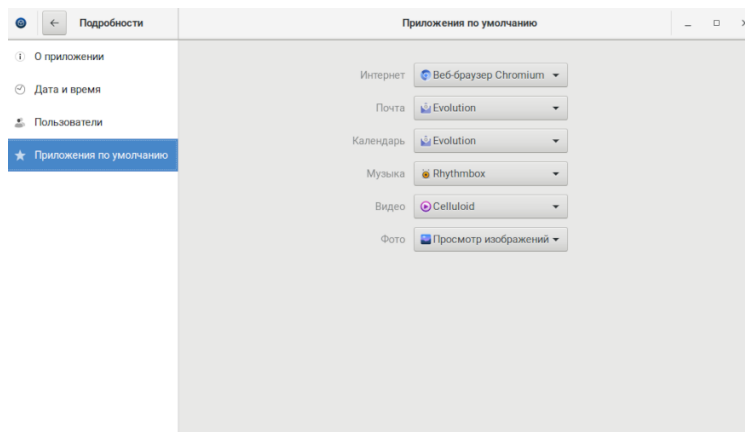
Задать и подтвердить новое значение своего пароля, продемонстрировав предварительно знание текущего значения пароля.

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 шестерёнок, активизирующей генератор паролей.

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

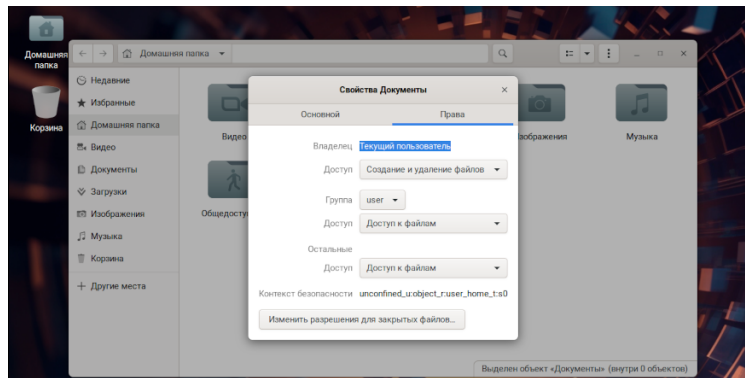
### Подробности. Приложения по умолчанию

Для выбора приложений по умолчанию перейдите в «Настройки» → «Подробности» → «Приложения по умолчанию».



### 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 **«Свойства»**, затем открыть вкладку **«Права»**.

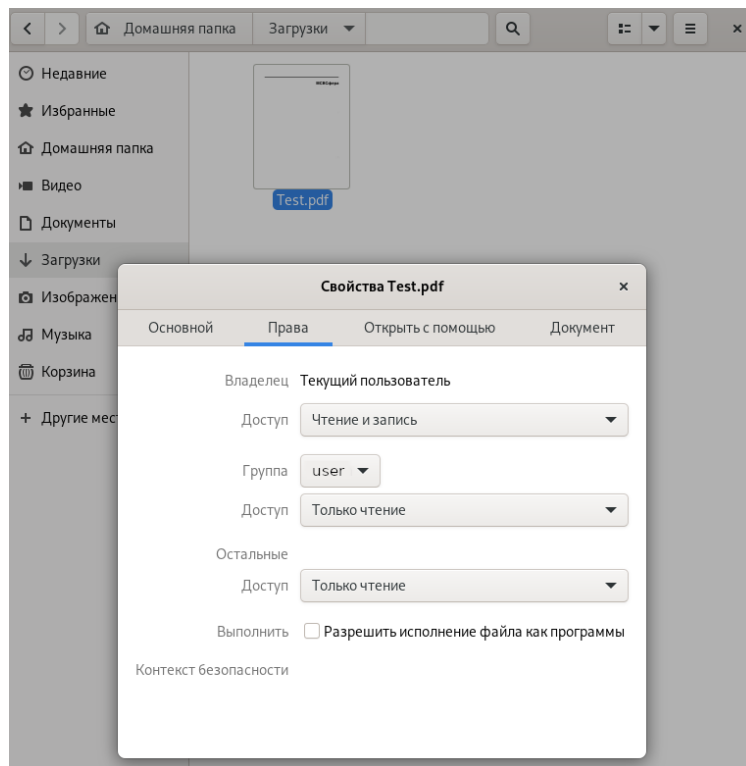


После чего можно определять права доступа для владельца, группы и других пользователей, выбирая их из следующего списка:

- 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 разрешения для закрытых файлов»**.

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.



# Решение задач пользователей

## Специальные возможности графического окружения рабочего стола

### Экранный диктор Orca и синтезатор речи RHVoice

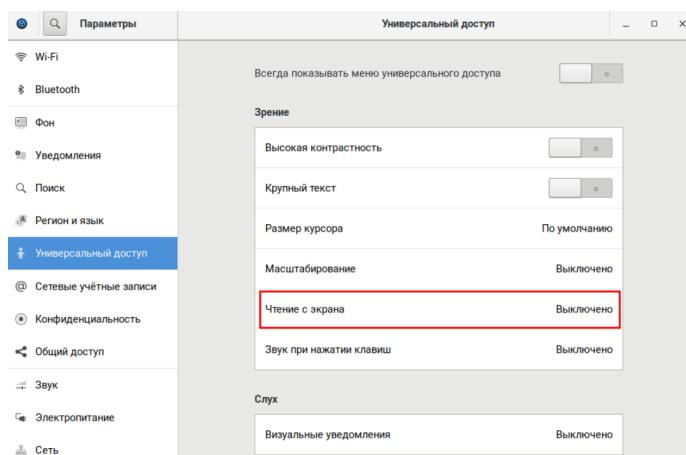
#### Введение

В графическом окружении ОС МСВСфера реализованы специальные возможности для облегчения работы за компьютером людям с ограниченными возможностями здоровья.

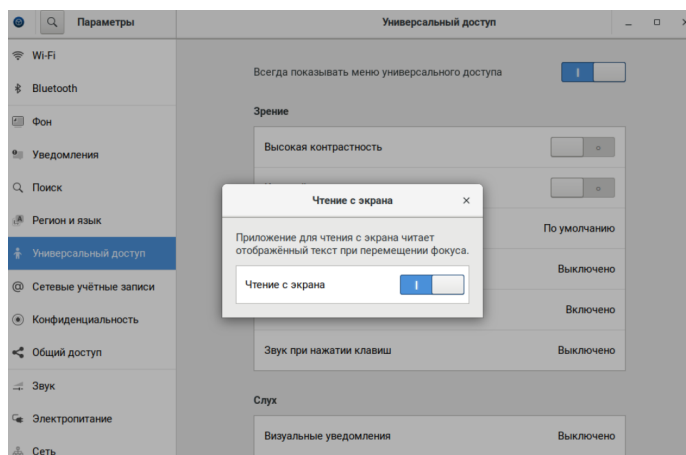
Экранный диктор Orca озвучивает отдельные элементы пользовательского интерфейса.

#### Экранный диктор Orca

Для включения экранного диктора Orca перейдите в «Настройки» → «Универсальный доступ». Затем нажмите «Чтение с экрана».



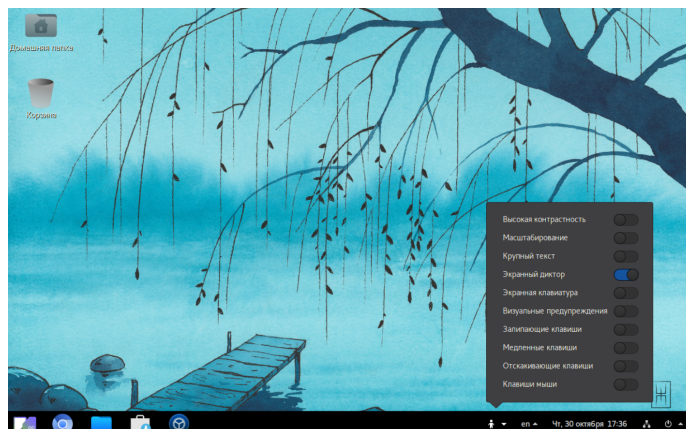
В открывшемся окне включите «Чтение с экрана».





Экранный диктор будет работать сразу же после включения. По наведению курсора мыши на объекты, будет воспроизводиться написанное.

Экранный диктор будет включён даже после перезагрузки системы. Вы можете проверить это, нажав на значок «Универсальный доступ», который отображается рядом с языком и системным меню.



## Синтезатор речи RHVoice

**RHVoice** — российский синтезатор речи с открытым исходным кодом, кроме русского языка поддерживает ещё ряд языков, таких как английский, киргизский, татарский и пр..

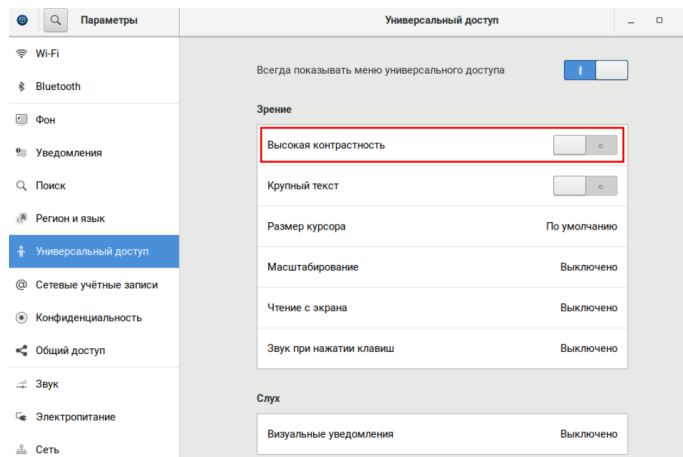
## Высококонтрастные темы оформления рабочего стола

### Введение

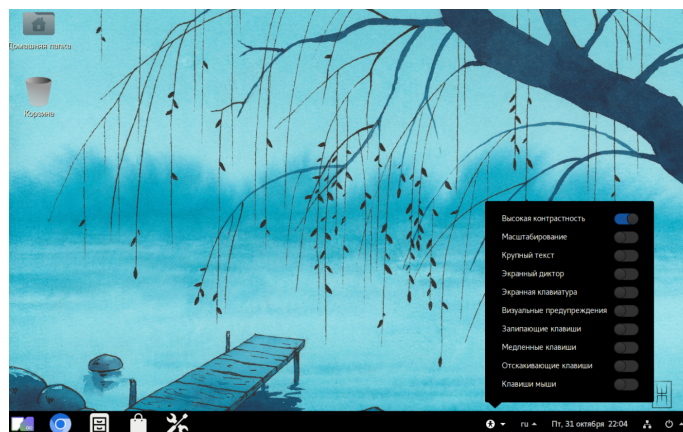
В графическом окружении ОС МСВСфера реализованы специальные возможности для облегчения работы за компьютером людям с ограниченными возможностями здоровья.

### Установка

Для применения высококонтрастной темы перейдите в «Настройки» → «Универсальный доступ» и включите «Высокая контрастность», передвинув слайдер. Изменения вступят в силу немедленно.



При необходимости вы можете быстро переключать режим высокой контрастности, нажав на значок «Универсальный доступ», который отображается рядом с языком и системным меню.



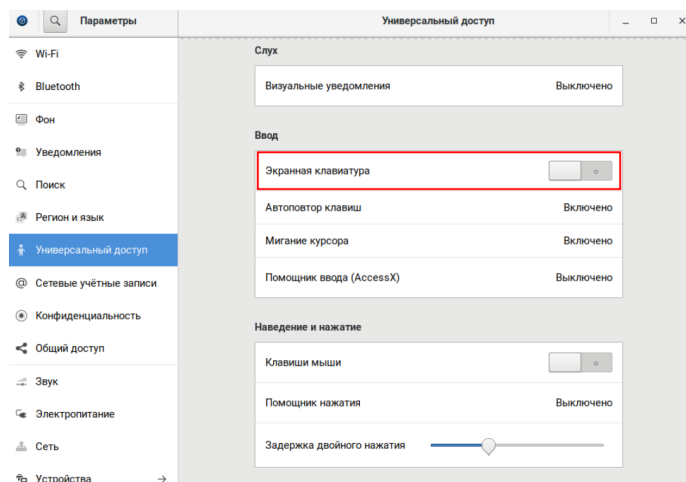
## Экранная клавиатура и экранная лупа

### Введение

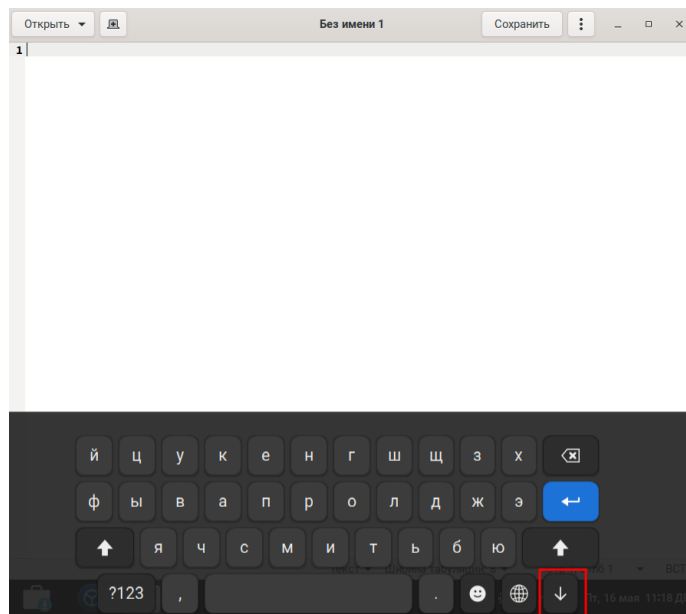
В графическом окружении ОС МСВСфера реализованы специальные возможности для облегчения работы за компьютером людям с ограниченными возможностями здоровья.

### Экранная клавиатура

Для включения экранной клавиатуры перейдите в «Настройки» → «Универсальный доступ» → раздел «Ввод» и включите «Экранная клавиатура», передвинув слайдер. Изменения вступят в силу немедленно.

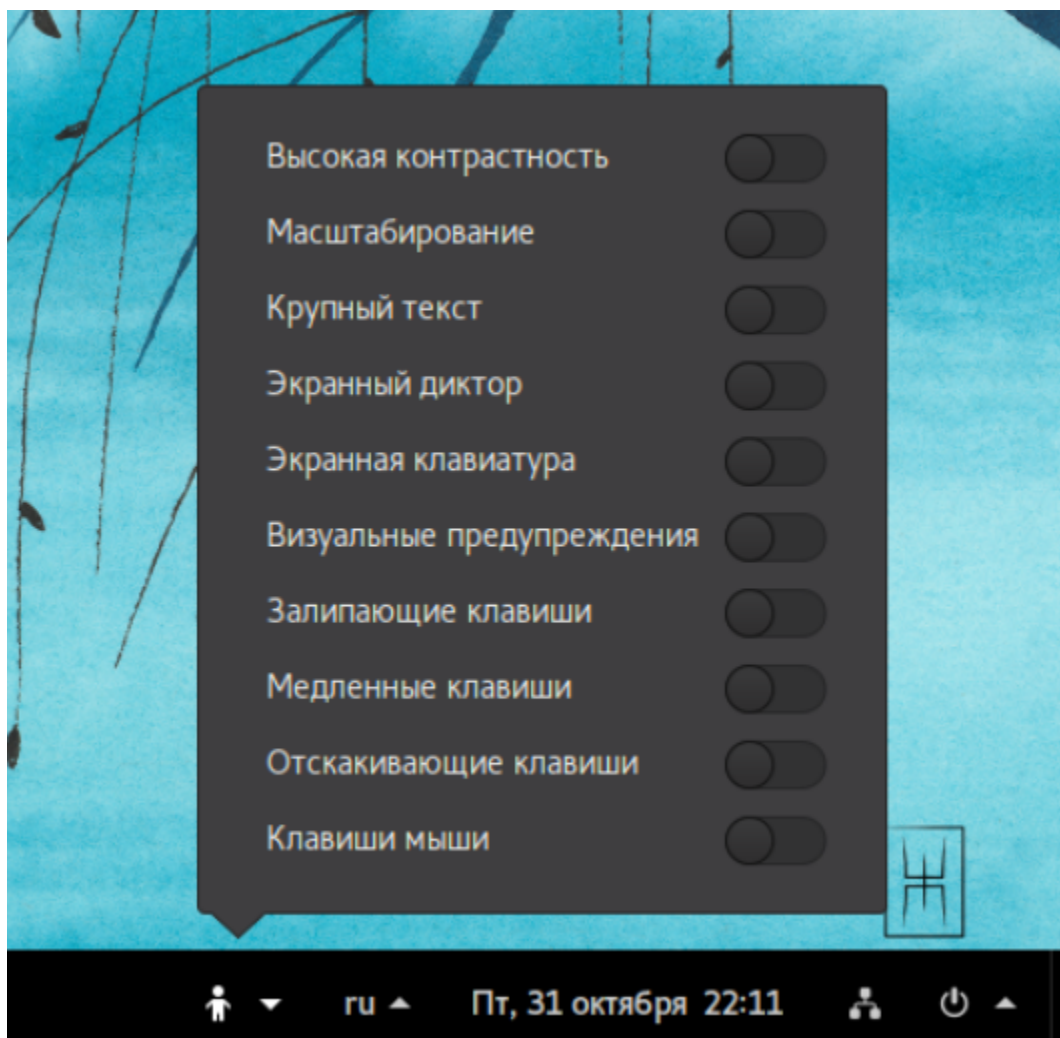


В следующий раз, когда вам потребуется ввести текст, экранная клавиатура появится в нижней части экрана.



Если экранная клавиатура больше не нужна, нажмите кнопку, выделенную красным на снимке экрана, чтобы временно скрыть клавиатуру. Клавиатура снова автоматически появится, когда вы установите курсор мыши в поле ввода.

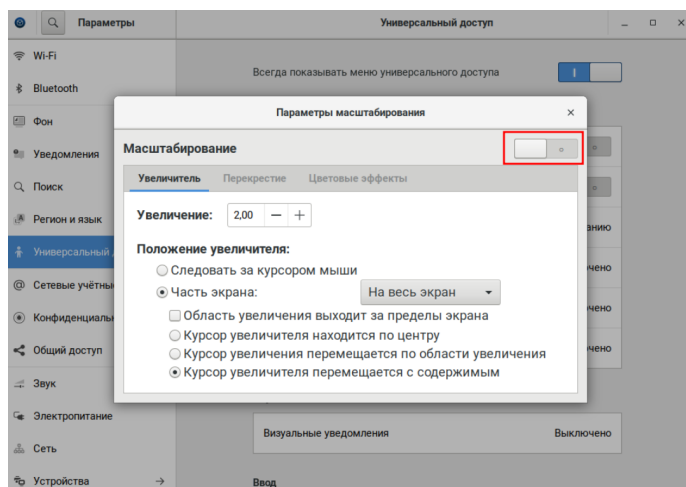
Вы можете быстро включить или выключить экранную клавиатуру, нажав на значок «Универсальный доступ», который отображается рядом с языком и системным меню.



### Экранная лупа (Масштабирование)

Масштабирование предоставляет функцию «экранной лупы», перемещая которую по экрану вы можете увеличивать отдельные его части.

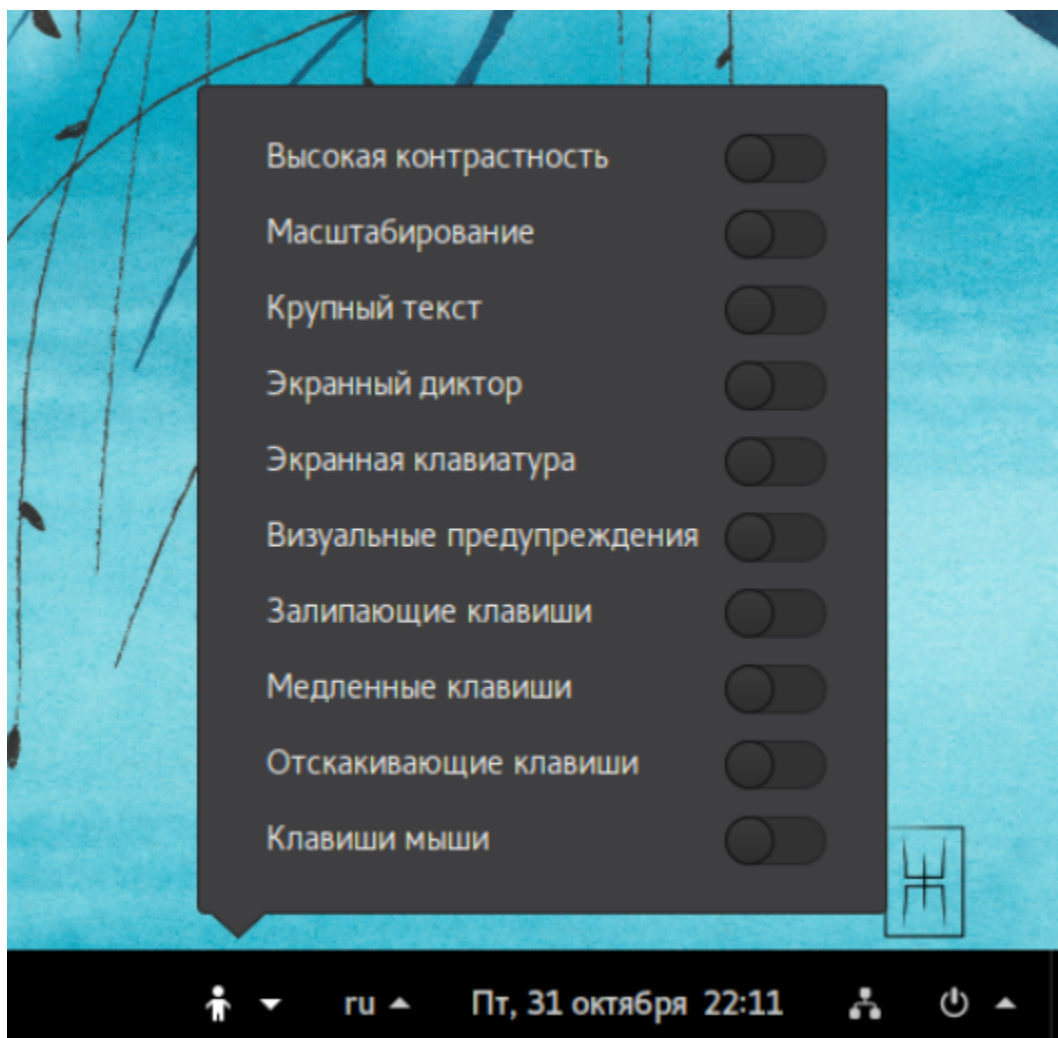
Для включения функции масштабирования перейдите в «Настройки» → «Универсальный доступ» → раздел «Зрение» и нажмите «Масштабирование», откроется окно «Параметры масштабирования».



Для включения масштабирования передвиньте слайдер. Изменения вступят в силу немедленно. Также здесь вы можете выполнить другие необходимые настройки.

Теперь, перемещая мышь, вы можете передвигать «экранную лупу» в различных направлениях, чтобы рассмотреть нужную область экрана.

Вы можете быстро включить или выключить масштабирование, нажав на значок «Универсальный доступ», который отображается рядом с языком и системным меню.



## Технология единого входа (SSO) браузерах

### Аутентификация Kerberos/SSO в браузере Mozilla Firefox

#### Введение

Технология единого входа (Single Sign-On, SSO) — это механизм аутентификации, при котором пользователю достаточно один раз ввести свои учётные данные для получения доступа к нескольким программным продуктам. Доступ осуществляется с использованием одного набора учётных данных, без необходимости повторной авторизации при переходе между продуктами.

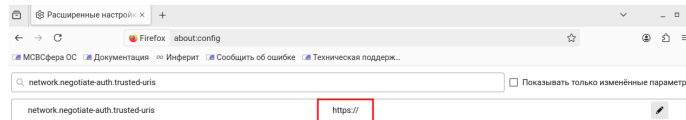
Перед использованием SSO необходимо выполнить следующие подготовительные шаги:

- добавить устройство в домен;

- убедиться, что доменный пользователь успешно получает Kerberos-билет, подтверждающий корректность аутентификации в доменной среде.

## Порядок действий

В ОС МСВСфера в браузере Mozilla Firefox аутентификация Kerberos/SSO разрешена по умолчанию для всех доменов.



`https://` означает, что разрешена аутентификация Kerberos/SSO для любых сайтов, использующих протокол TLS (англ. «transport layer security» — протокол защиты транспортного уровня). Протокол TLS позволяет обеспечивать защищённое соединение между любыми узлами в сети.

## Аутентификация Kerberos/SSO в браузере Chromium

### Введение

Технология единого входа (Single Sign-On, SSO) — это механизм аутентификации, при котором пользователю достаточно один раз ввести свои учётные данные для получения доступа к нескольким программным продуктам. Доступ осуществляется с использованием одного набора учётных данных, без необходимости повторной авторизации при переходе между продуктами.

Перед использованием SSO необходимо выполнить следующие подготовительные шаги:

- добавить устройство в домен;
- убедиться, что доменный пользователь успешно получает Kerberos-билет, подтверждающий корректность аутентификации в доменной среде.

## Порядок действий

1. Откройте «Терминал».
2. Создайте каталог `/etc/chromium/policies/managed/` с помощью следующей команды:

```
$ sudo mkdir -p /etc/chromium/policies/managed/
```

3. В этом каталоге создайте файл с именем, например, `policy.json` (имя до точки может быть любым) следующего вида:

```
{
  "AuthServerAllowlist": "*.test.example.ru",
  "AuthNegotiateDelegateAllowlist": "*.test.example.ru"
}
```

где \*.test.example.ru — имя вашей kerberos-области (realm).

Чтобы включить возможность единого входа для нескольких доменов, перечислите их через запятую, например:

```
{
  "AuthServerAllowlist": "*.test1.example.ru,test2.example.ru,test3.example.ru",
  "AuthNegotiateDelegateAllowlist": "*.test1.example.ru,test2.example.ru,test3.example.ru"
}
```

4. Сохраните файл.

5. Теперь вы можете посмотреть созданные политики в браузере Chromium по адресу chrome://policy.

The screenshot shows the Chromium browser interface at the chrome://policy page. The 'Правила' (Policies) tab is active. Below the search bar, there are buttons for 'Повторно загрузить правила' and 'Другие действия'. The 'Chrome Policies' section contains a table with two rows of policies. The 'Policy Precedence' section shows a list of precedence rules.

Название правила	Значение правила	Источник	Объект применения	Уровень	Состояние
AuthNegotiateDelegateAllowlist	*.test.example.ru	Платформа	Локальный ко...	Обязательная	Ок
AuthServerAllowlist	*.test.example.ru	Платформа	Локальный ко...	Обязательная	Ок

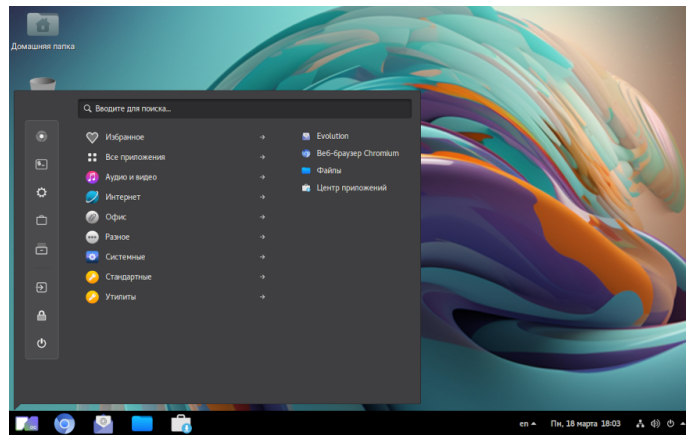
**Policy Precedence**

Название правила	Значение правила	Источник	Объект применения	Уровень	Состояние
Правила не заданы					
Текущий порядок приоритетности: Устройство платформы > Устройство облака > Пользователь платформы > Пользователь облака					



# Приложения

Все приложения, установленные на устройстве, доступны из «Главного меню».

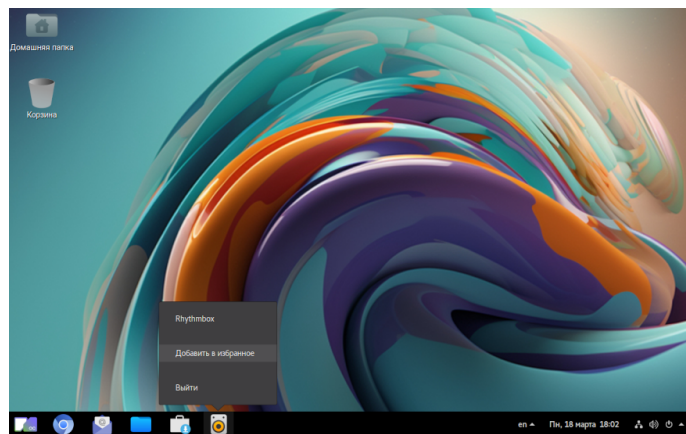


Ниже показано как добавить приложение в «Избранное».

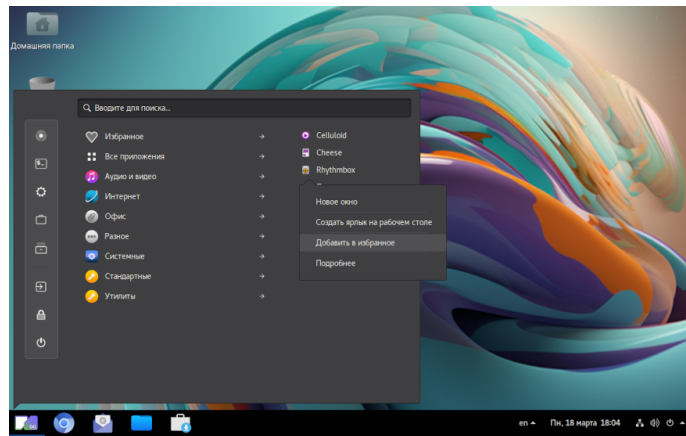
## Добавление в «Избранное»

«Избранное» позволяет осуществлять быстрый доступ к часто используемым приложениям.

Чтобы добавить или удалить приложение из «Избранного», нажмите на значок приложения в панели задач правой клавишей мыши и выберите «Добавить в избранное»/» Удалить из избранного».



Или в меню «Приложения» навести курсор мыши на приложение и нажать правой клавишей мыши, затем выбрать «Добавить в избранное»/» Удалить из избранного».



## Обзор приложений

Для удобства пользователя в дистрибутив включен широкий спектр сервисов и приложений для ежедневной работы. Рассмотрим некоторые из них:

- **Офисные приложения**

- **Libre Office** – мощный и одновременно простой в использовании офисный пакет, готовый к использованию без дополнительной подготовки всеми, кто уже работал с какими-либо офисными программами. Libre Office поддерживает большинство существующих форматов «офисных» файлов. Libre Office состоит из нескольких компонентов:

- \* Текстовый редактор Writer;
- \* Табличный редактор Calc;
- \* Средство создания и демонстрации презентаций Impress;
- \* Векторный редактор Draw;
- \* Редактор формул Math.

- **Почтовые программы**

- Evolution – программа для работы с электронной почтой, управления адресной книгой и функцией планировщика задач.

- **Веб-браузеры**

- Chromium – безопасный и быстрый браузер с открытым исходным кодом.

А также другие пользовательские приложения, которые можно установить в «**Центре приложений**».

Интерфейс всех приложений интуитивно понятный. При возникновении вопросов по использованию приложения, рекомендуется обратиться к справочной информации о приложении.

# Центр приложений

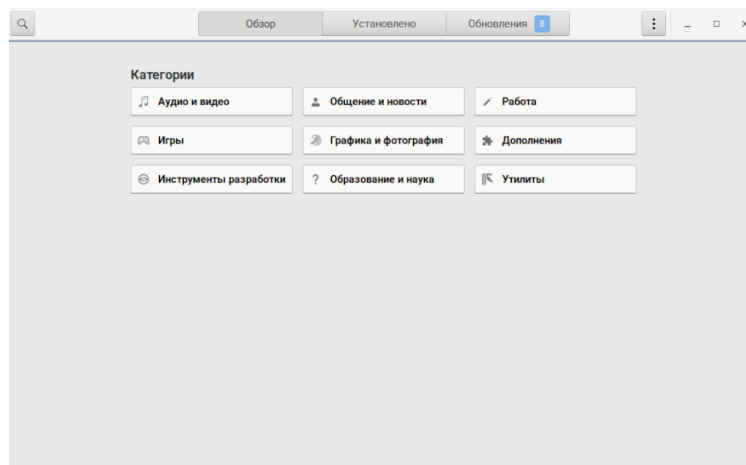
«Центр приложений» предоставляет пользователям удобный интерфейс для управления, установки и обновления приложений и системных пакетов.

Для запуска «Центра приложений» нажмите на его значок:

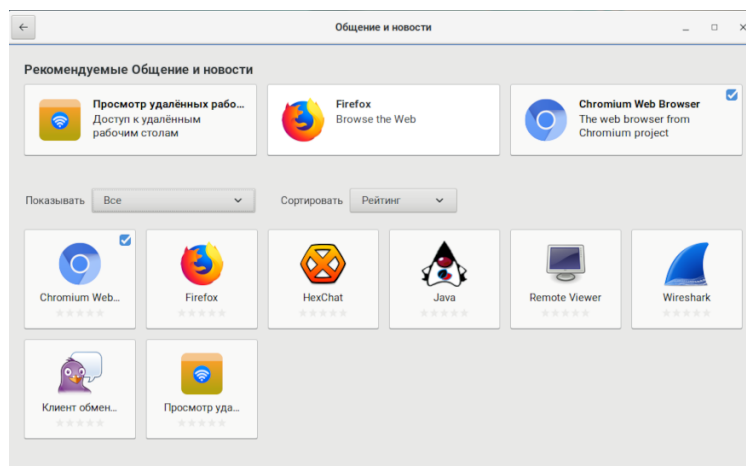


## Управление приложениями

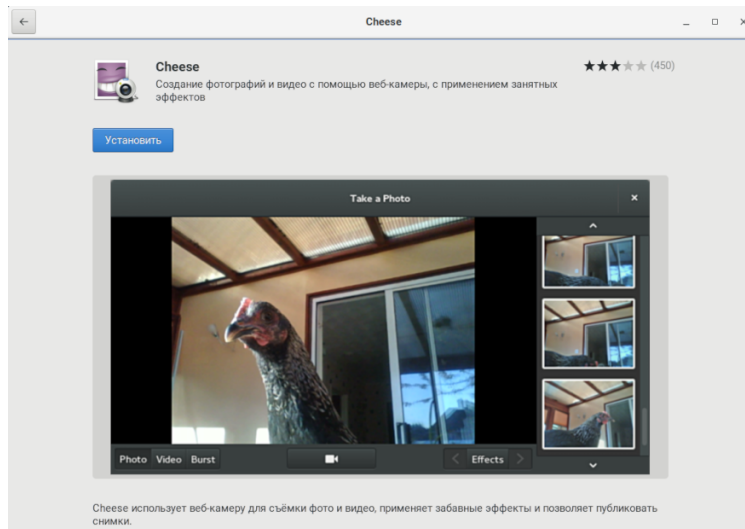
Во вкладке «Обзор» представлены все приложения, доступные для загрузки.



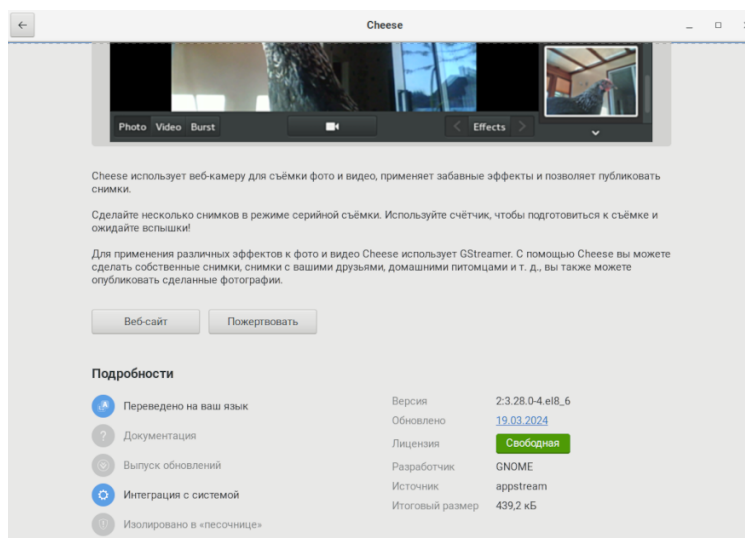
Приложения разделены по категориям. Нажмите на категорию для просмотра всех имеющихся в ней приложений.



Для просмотра информации о приложении нажмите на него.



Для просмотра дополнительной информации о приложении, а также об источнике установки, обратитесь к разделу «**Подробности**».



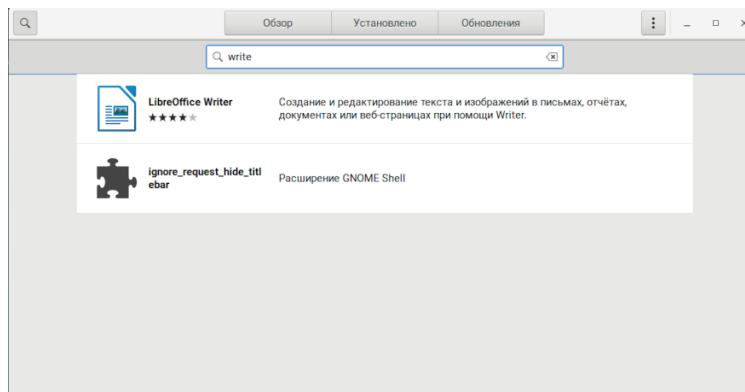
Для возврата в основное меню нажмите на стрелку «Назад».

## Поиск приложения

Для поиска приложения нажмите на значок поиска:

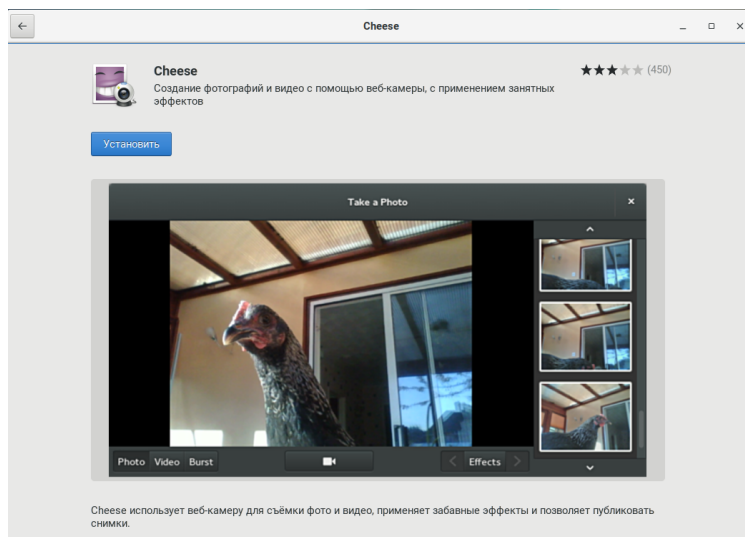


Затем укажите название приложения или ключевые слова, описывающие, что должно делать приложение.



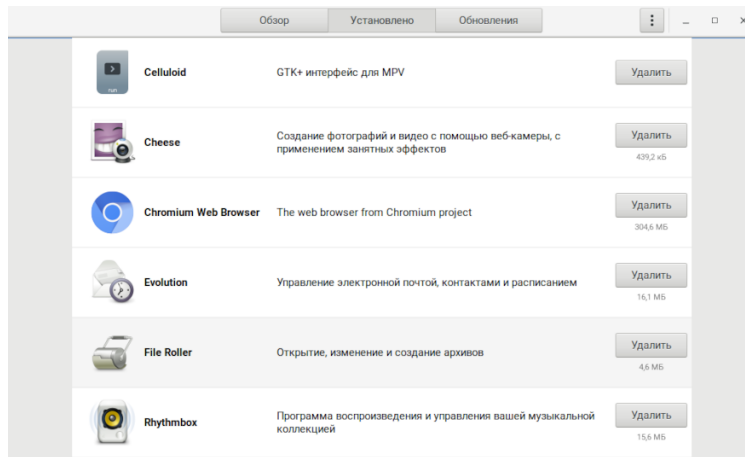
## Установка приложения

Для установки приложения войдите в него и нажмите на кнопку **«Установить»**. Загрузка необходимых пакетов и установка приложения начнётся автоматически.



## Просмотр списка установленных приложений

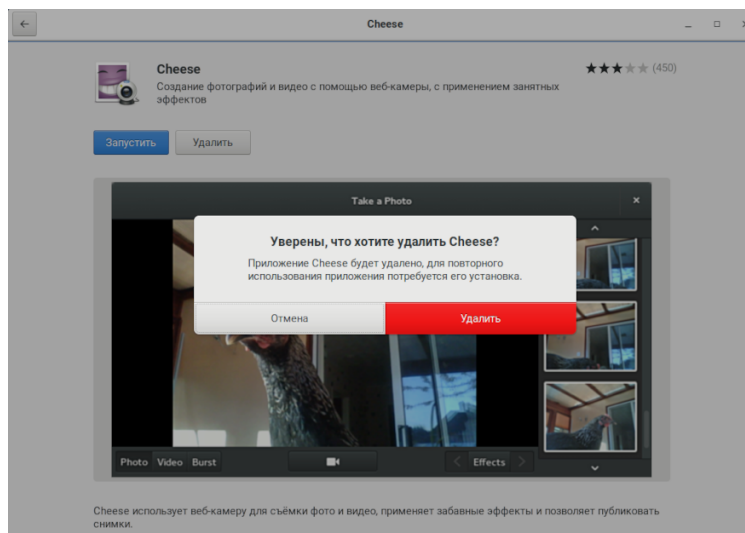
Перейдите во вкладку **«Установлено»** для управления уже установленными приложениями.



## Удаление приложения

Для удаления приложения, находясь в нём, нажмите на значок корзины и подтвердите свой выбор.

Для удаления приложения, находясь во вкладке «Установлено», нажмите «Удалить» и подтвердите свой выбор.

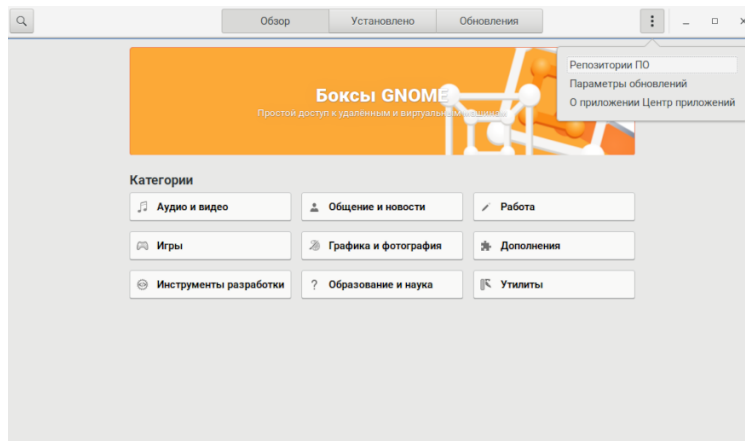


## Управление репозиториями

Репозиторий – в данном случае это место хранения программ и приложений. В разных репозиториях хранятся различные программы и приложения, поэтому может быть подключено несколько репозиториях.

## Включение и выключение репозитория

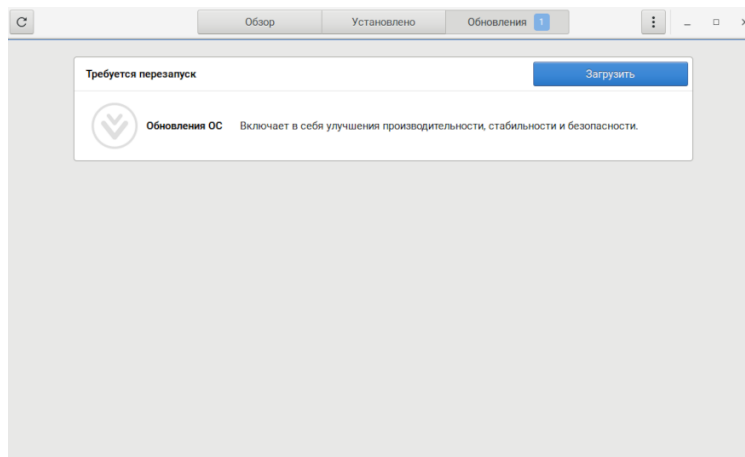
Для управления репозиториями нажмите на значок «Дополнительно» в правом верхнем углу, находясь в любой вкладке и выберите «Репозитории ПО».



По умолчанию подключены только необходимые репозитории. Для включения репозитория нажмите на него, а затем нажмите на кнопку **«Включить»**. После этого выполните аутентификацию. Для отключения репозитория также необходимо выполнить аутентификацию.

## Параметры обновления

Перейдите во вкладку **«Обновления»** для управления обновлениями. Новые обновления отображаются в списке. Нажмите **«Загрузить»** для загрузки. В некоторых случаях может потребоваться перезагрузка устройства для установки и применения загруженных обновлений.

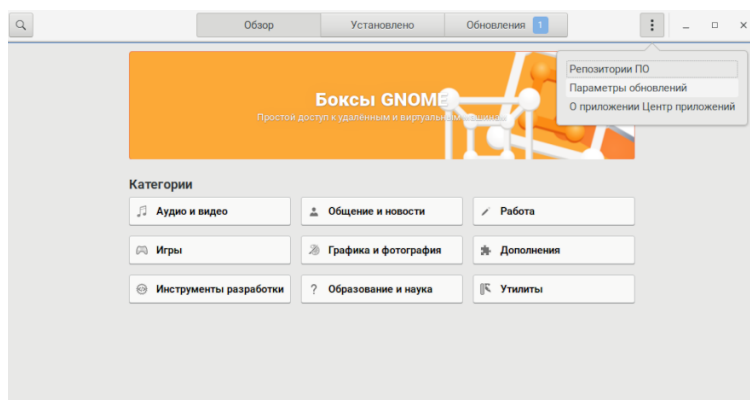


Для проверки наличия обновлений нажмите на значок **«Обновить»**.

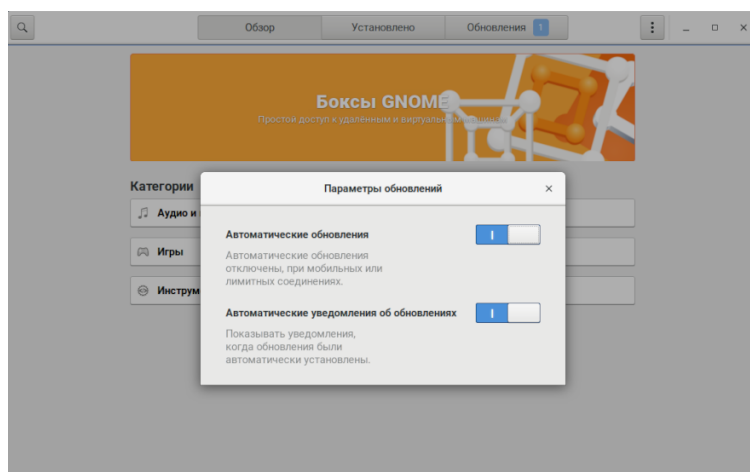
## Включение и выключение автоматических обновлений и уведомлений о новых версиях ПО

Для управления уведомлениями нажмите на значок **«Дополнительно»** в правом верхнем углу, находясь в любой вкладке, и выберите **«Параметры обновлений»**.





Для включения или выключения обновлений или уведомлений передвиньте ползунок в активное состояние.



[illegible]