ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«НАЦИОНАЛЬНЫЙ ЦЕНТР ПОДДЕРЖКИ И РАЗРАБОТКИ»

УТВЕРЖДЕН
ЦАУВ.27001-01 32 01-ЛУ

Подпись и дата	
Инв. № дубл.	
Взам. инв №	
Подпись и дата	
Инв. № подл.	

Операционная система «МСВСфера»

Руководство пользователя

ЦАУВ.27001-01 32 01

(Листов - 85)

2025

Содержание

АННОТАЦИЯ

Настоящее руководство предназначено для пользователей операционной системы МСВСфера 9 Сертифицированная (ФСТЭК). Руководство ориентировано на специалистов, знакомых с операционными системами и имеющих минимальный практический опыт работы с ними. Руководство снабжено примерами, сделанными в операционной системе МСВСфера 9 Сертифицированная (ФСТЭК), установленной в конфигурации «Сервер с графическим интерфейсом».

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и область применения

Операционная система МСВСфера 9 Сертифицированная (ФСТЭК) — это операционная система на основе ядра Linux, выпускается в следующих редакциях:

- МСВСфера 9 Сервер;
- МСВСфера 9 АРМ.

МСВСфера 9 Сервер — операционная система 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 9 Сервер предназначена для организации многоцелевых серверов на базе 64-х разрядных аппаратных платформ Intel и AMD).

МСВСфера 9 АРМ (АРМ — автоматизированное рабочее место) — клиентская операционная система с набором интегрированных спользовательских приложений, включающих пакет офисных программ, браузер, почтовую программу, редакторы текстов и графики, проигрыватели аудио и видео, менеджеры файлов и архивов, программу записи и копирования оптических дисков, программу сканирования документов, множество других программ, а также средства администрирования и защиты информации. МСВСфера 9 АРМ предназначена для организации многофункциональных рабочих мест на базе 64-х разрядных аппаратных платформ Intel и AMD.

Как правило, ОС МСВСфера 9 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.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. 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.

1.6. 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.

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 своё имя из предлагаемого системой списка имён 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.

При первом входе в систему пользователю будет предложено выбрать вид рабочего стола.

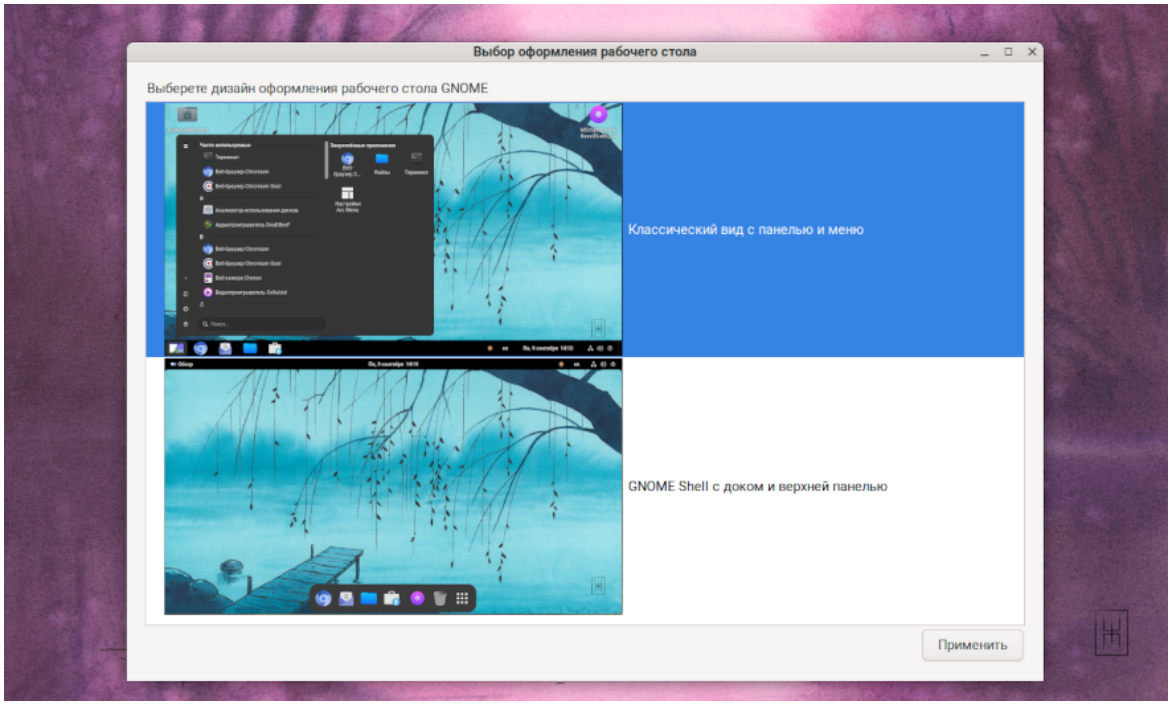

Рис. 1: Вид оформления рабочего стола

Вы можете изменить вид в любой момент в приложении «Выбор оформления рабочего стола».

2.2. Структура меню

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

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

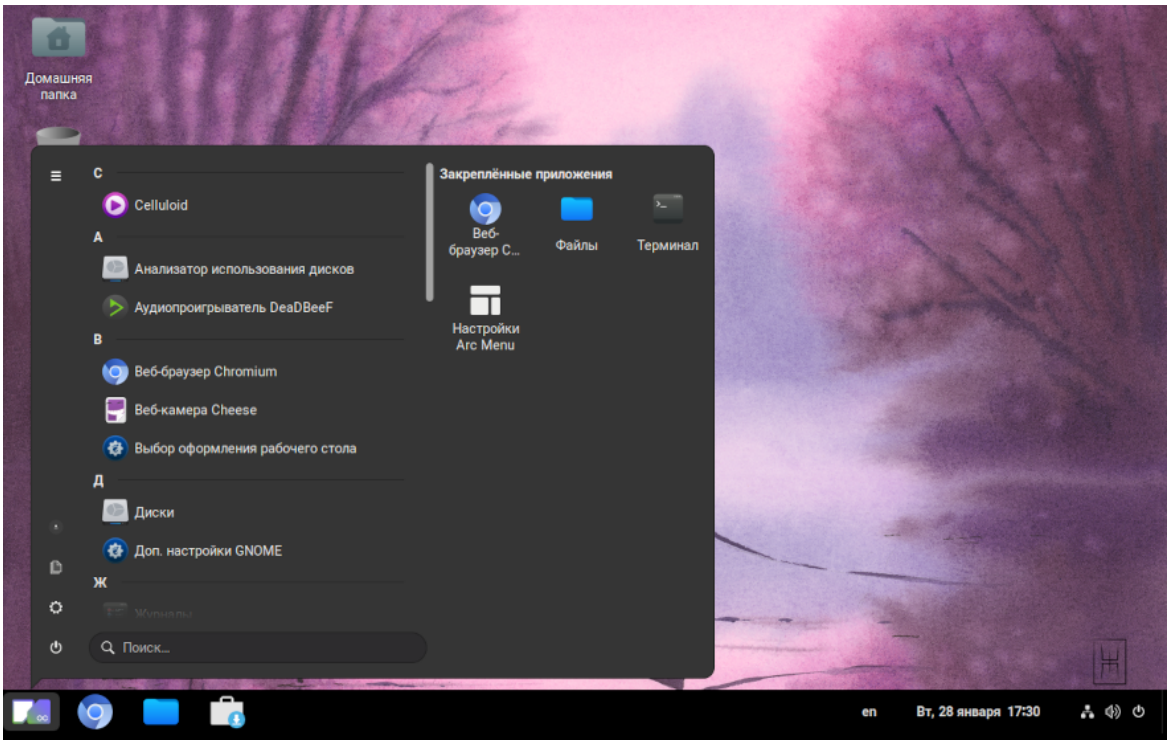

Рис. 2: Меню Приложения

Меню выбора языка ввода:

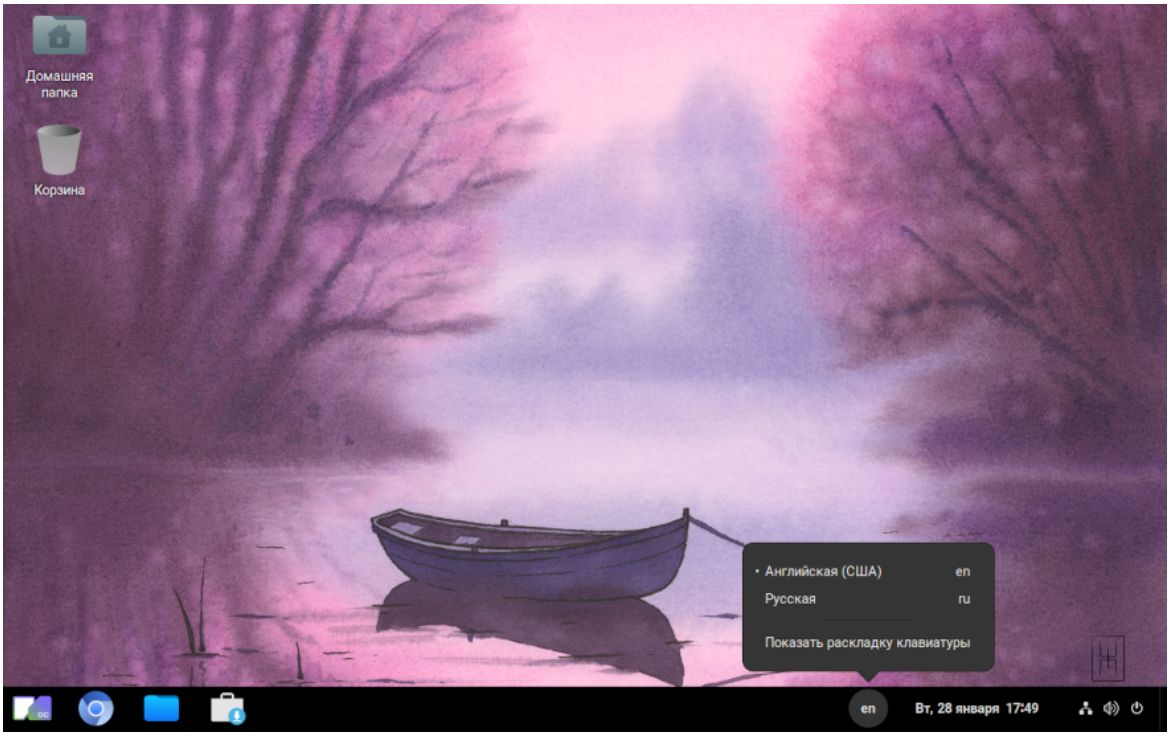

Рис. 3: Меню выбора языка ввода

Меню настройки даты и времени:

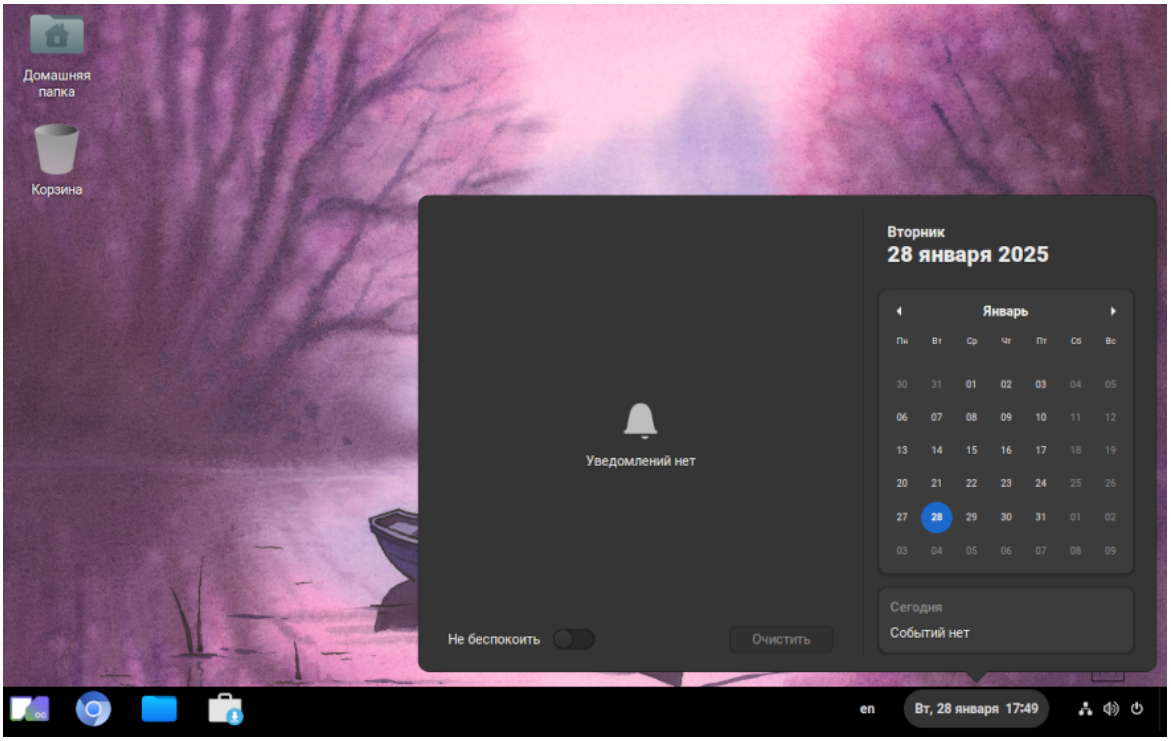

Рис. 4: Меню настройки даты/времени и уведомлений

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.

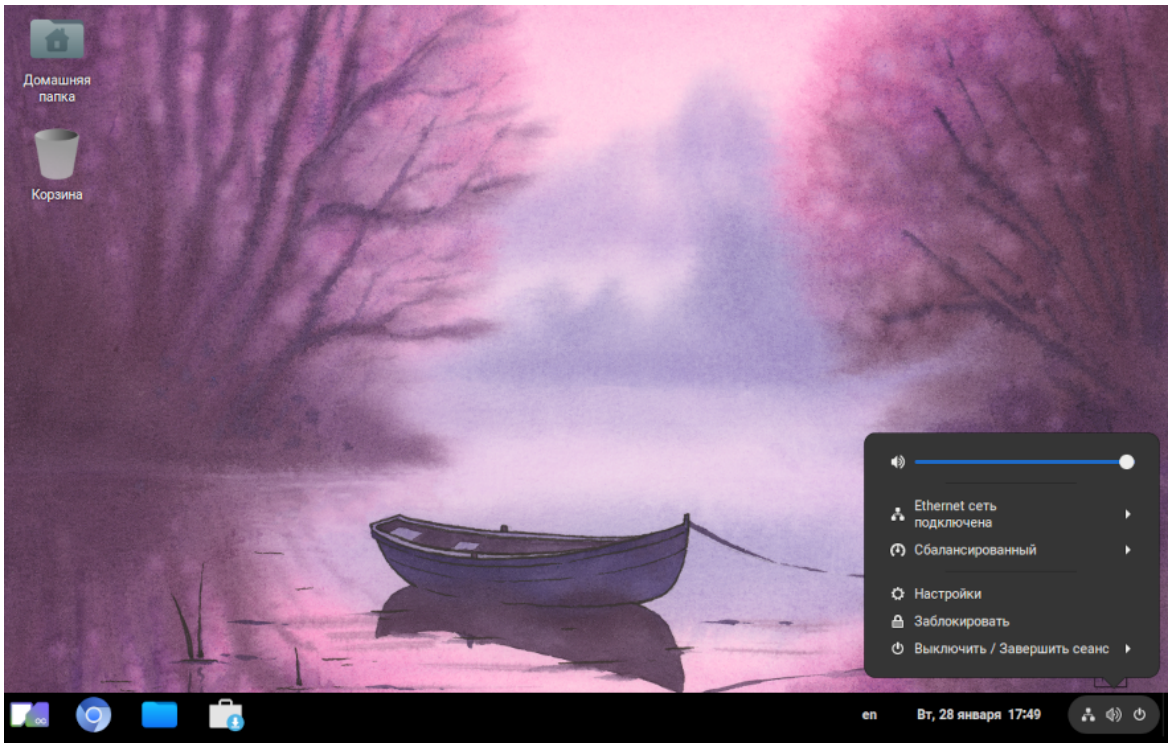

Рис. 5: Системное меню

Подробнее о составе и функциональных возможностях вышеперечисленных меню изложено ниже.

2.2.1. Блокировка экрана

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

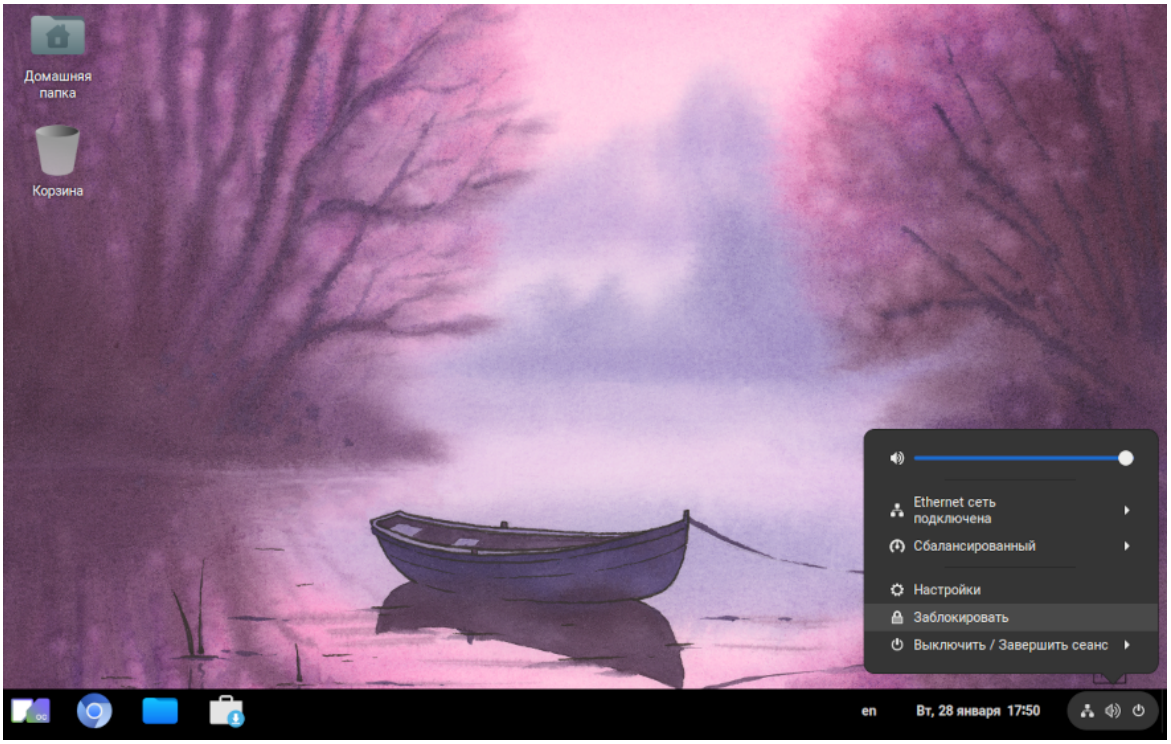

Рис. 6: Заблокировать

Либо из меню «Приложения».

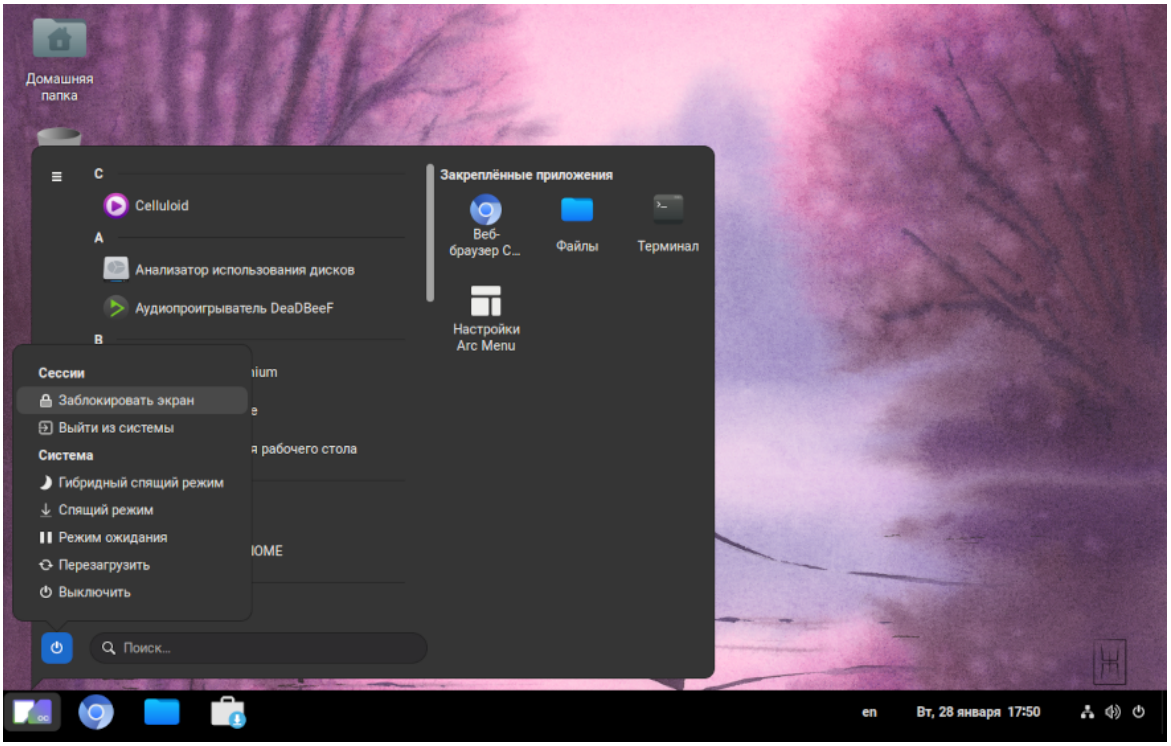

Рис. 7: Заблокировать из меню «Приложения»

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.

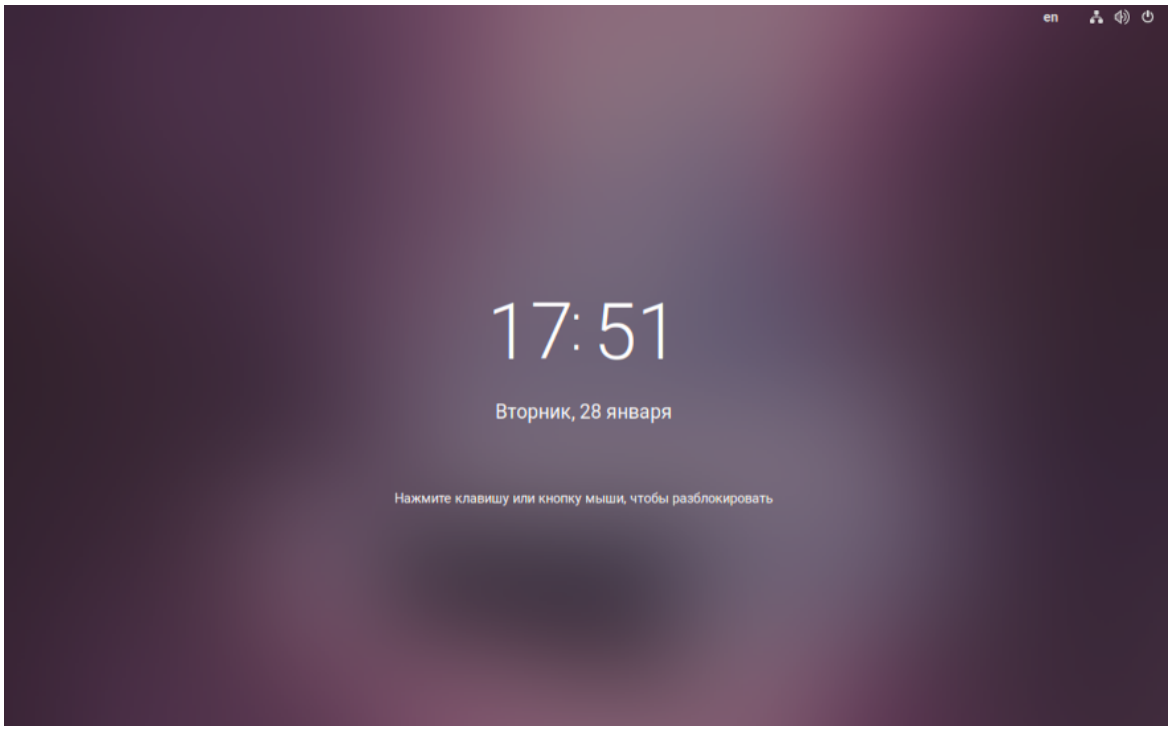

Рис. 8: Экран блокировки

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

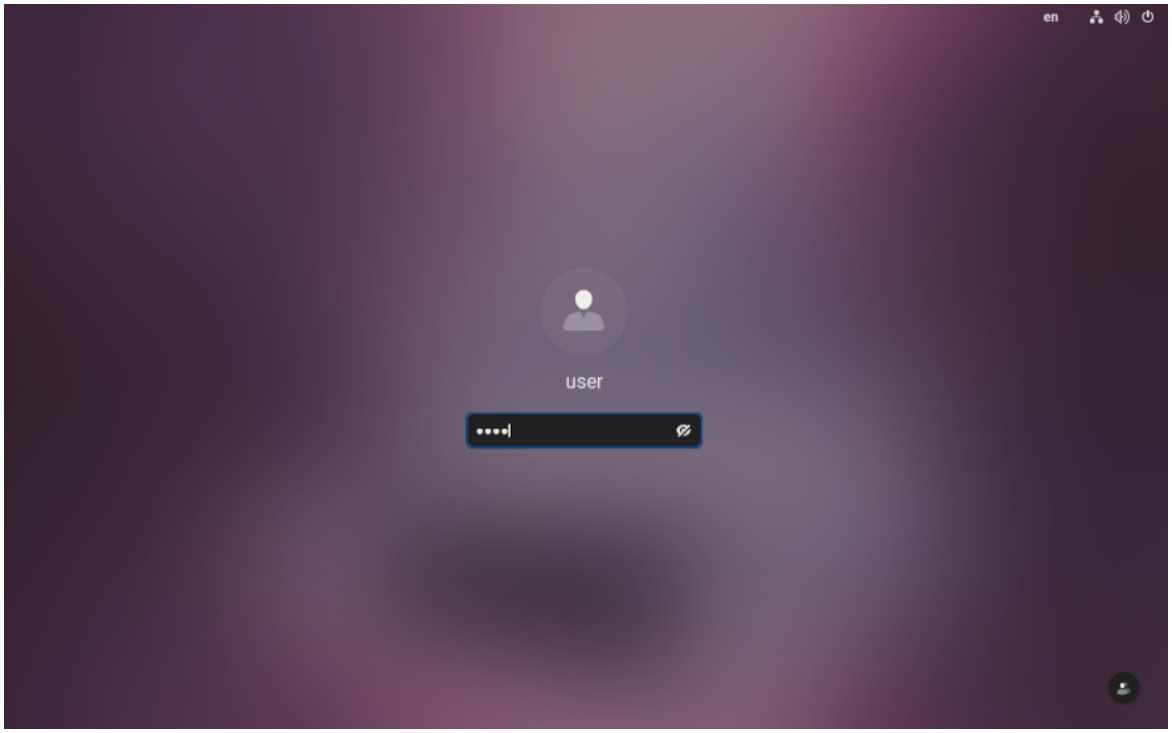

Рис. 9: Разблокировка экрана

2.3. Завершение сеанса

Завершение сеанса работы пользователя с системой осуществляется нажатием в системном меню на «Выключить/Завершить сеанс» и выбором «Завершить сеанс».

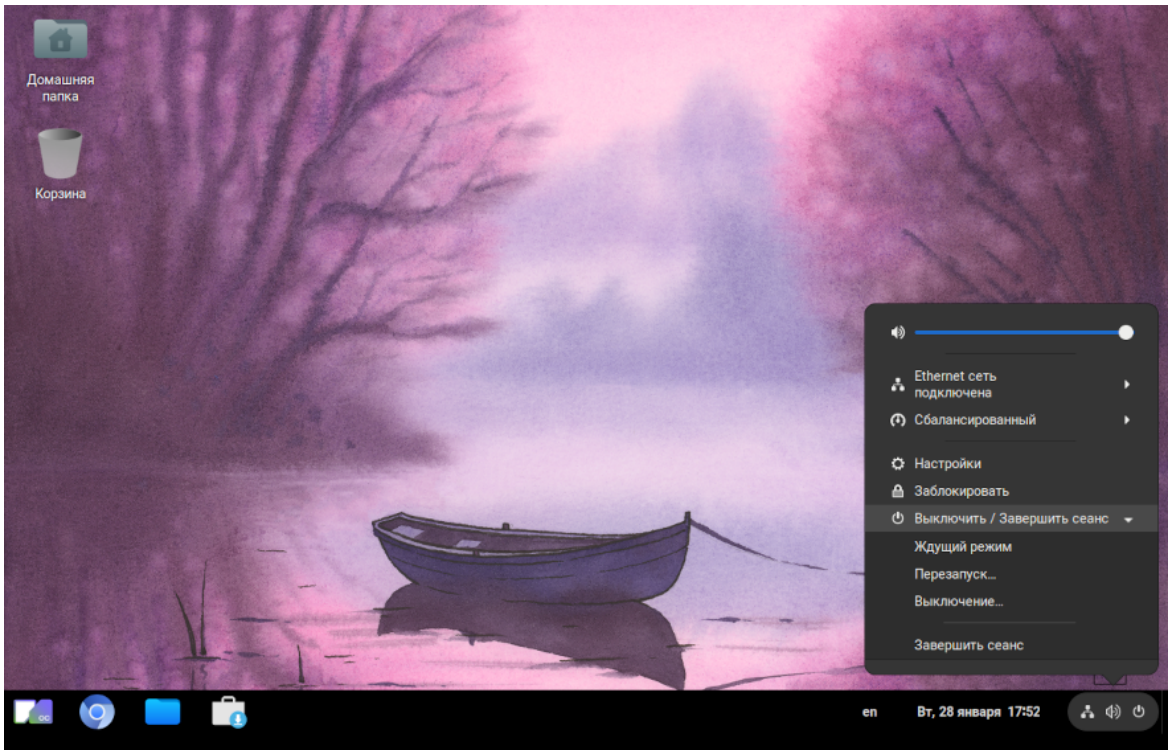

Рис. 10: Выключить/Завершить сеанс

Или в меню «Приложения» нажатием на значок выключения и выбором «Выйти из системы».

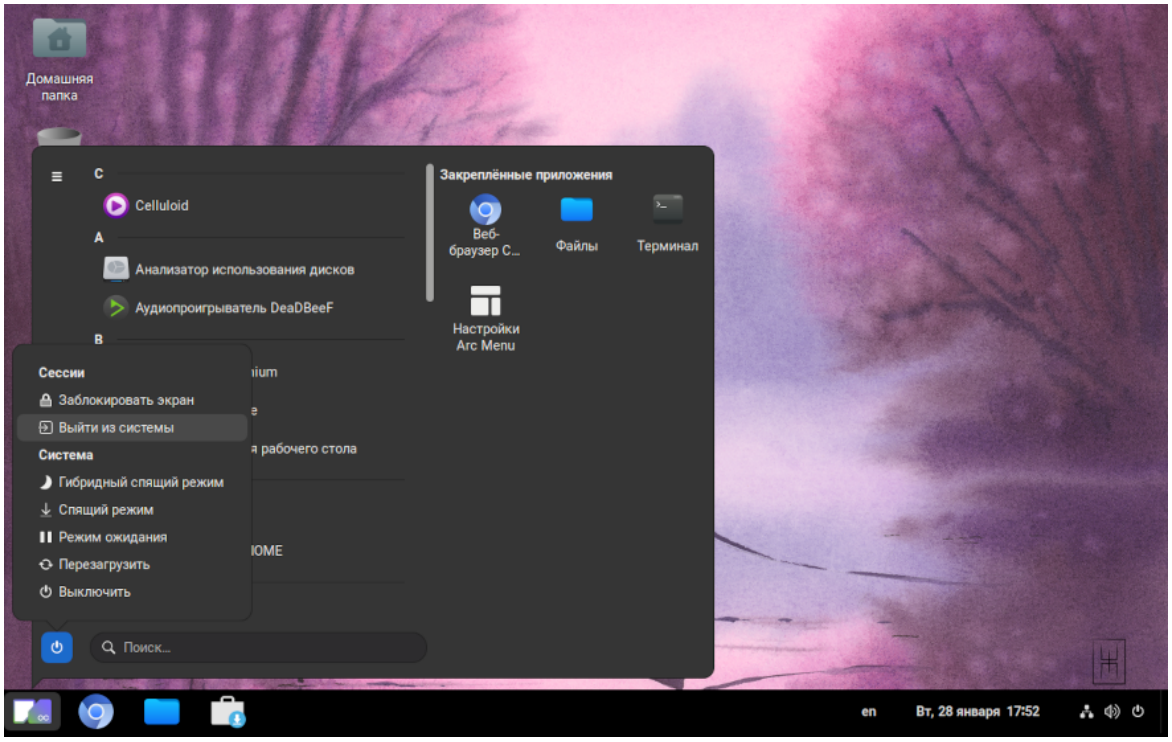

Рис. 11: Выключить/Завершить сеанс из меню «Приложения»

И подтверждением данного выбора.

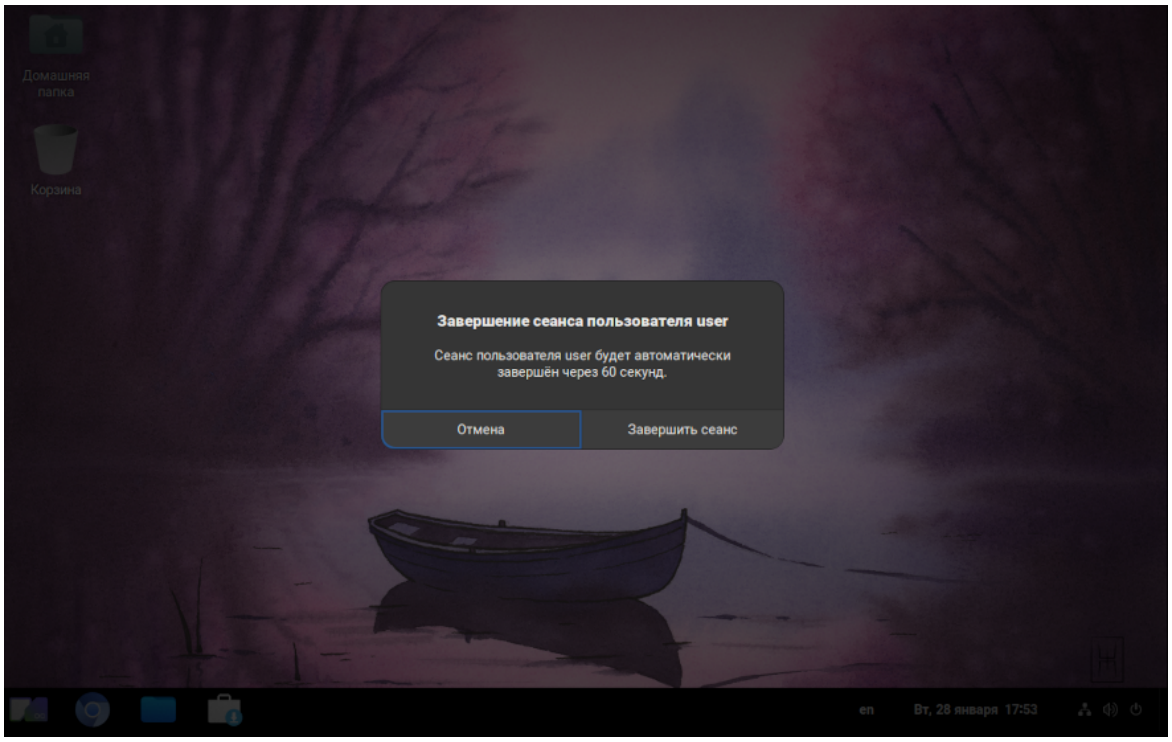

Рис. 12: Подтверждение выбора

Завершение сеанса сопровождается завершением работы всех запущенных пользователем приложений.

2.4. Перезапуск/выключение/ждущий режим

Перезапуск и выключение системы, а также перевод в ждущий режим осуществляются нажатием в системном меню на «Выключить/Завершить сеанс».

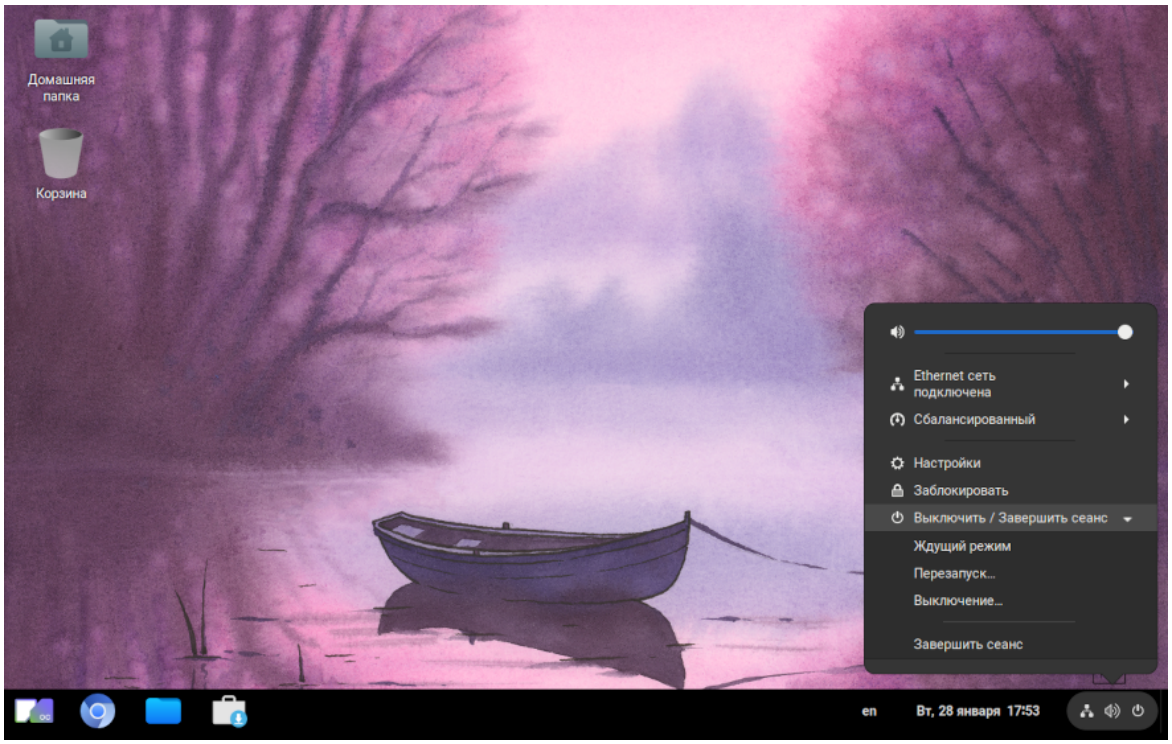

Рис. 13: Меню «Выключить/Завершить сеанс»

И последующим нажатием на «Перезапуск/ Выключение/ Ждущий режим».

Или в меню «Приложения» нажатием на значок выключения и последующим нажатием на «Перезагрузить/ Выключить/ Режим ожидания».

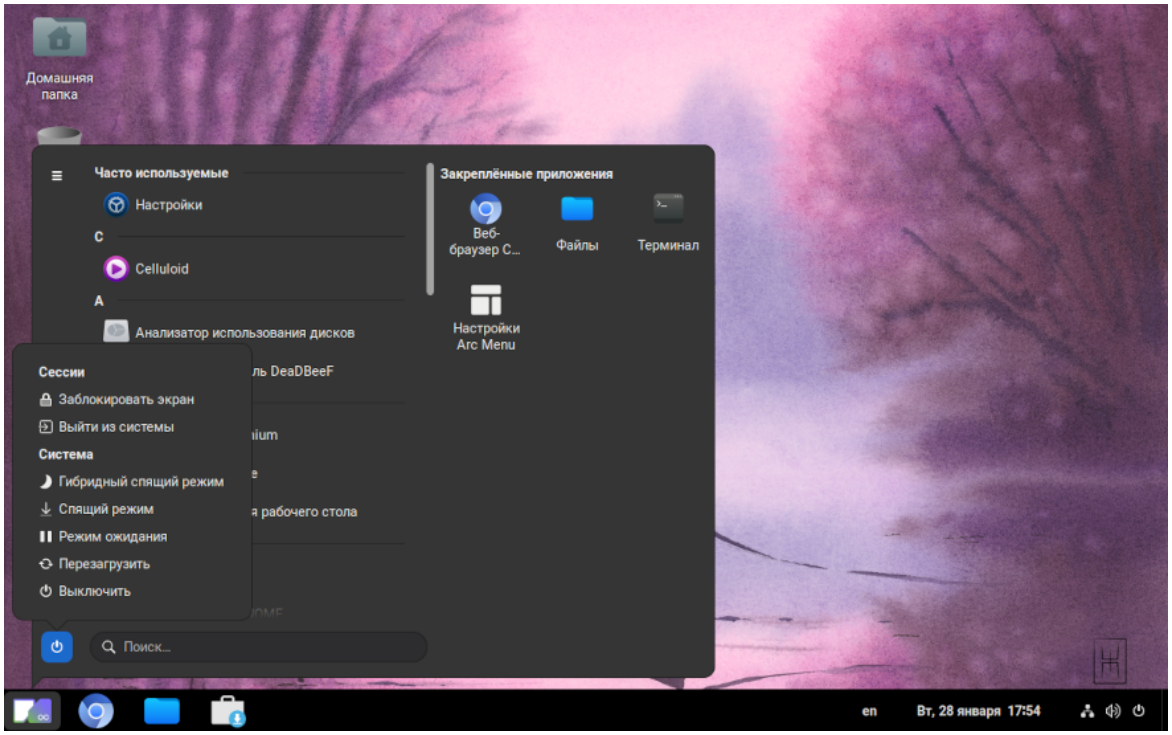

Рис. 14: Меню «Выключить/Завершить сеанс»

2.5. Гибридный спящий режим

Переход в гибридный спящий режим осуществляется из меню «Приложения» нажатием на значок выключения и последующим нажатием на «Гибридный спящий режим»:

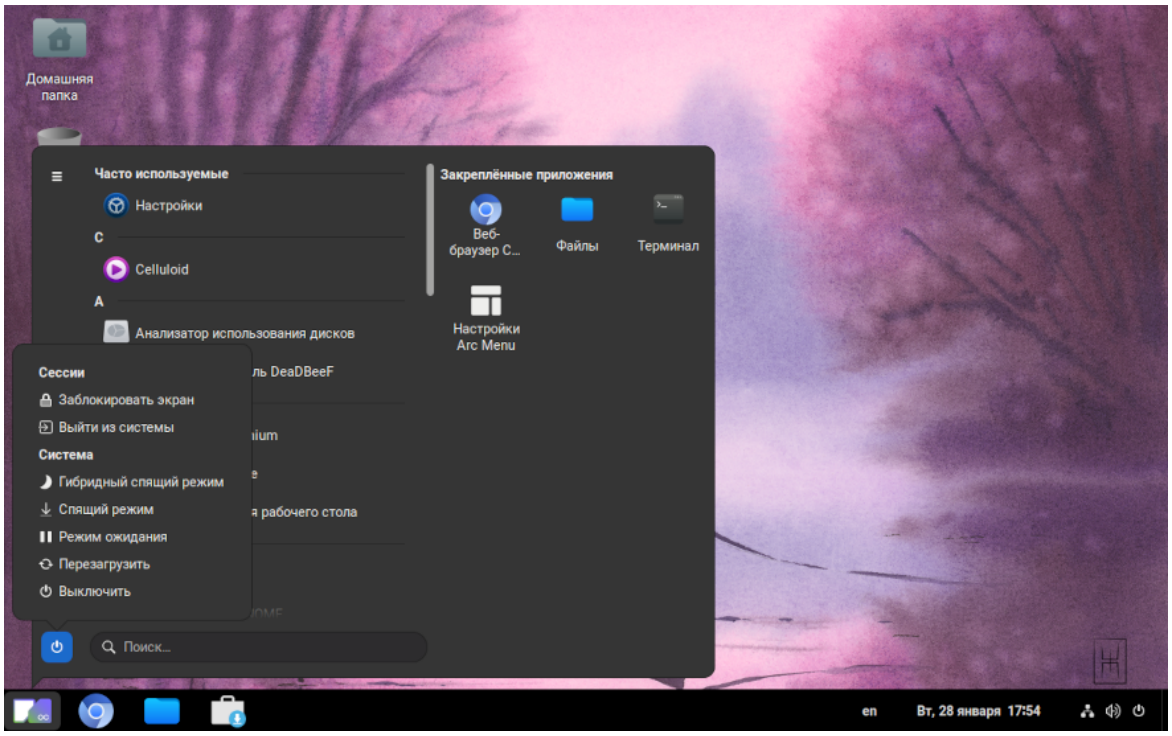

Рис. 15: Гибридный спящий режим из меню «Приложения»

При переходе в «Гибридный спящий режим» состояние устройства (компьютера, ноутбука) сохраняется в пространстве подкачки (swap). При этом само устройство не выключается, а переводится в спящий режим.

Таким образом, если батарея не разряжена, система может возобновить работу мгновенно. Если батарея разряжена, работу системы можно возобновить с диска, что медленнее, чем из ОЗУ, но состояние устройства сохранится.

3. 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.

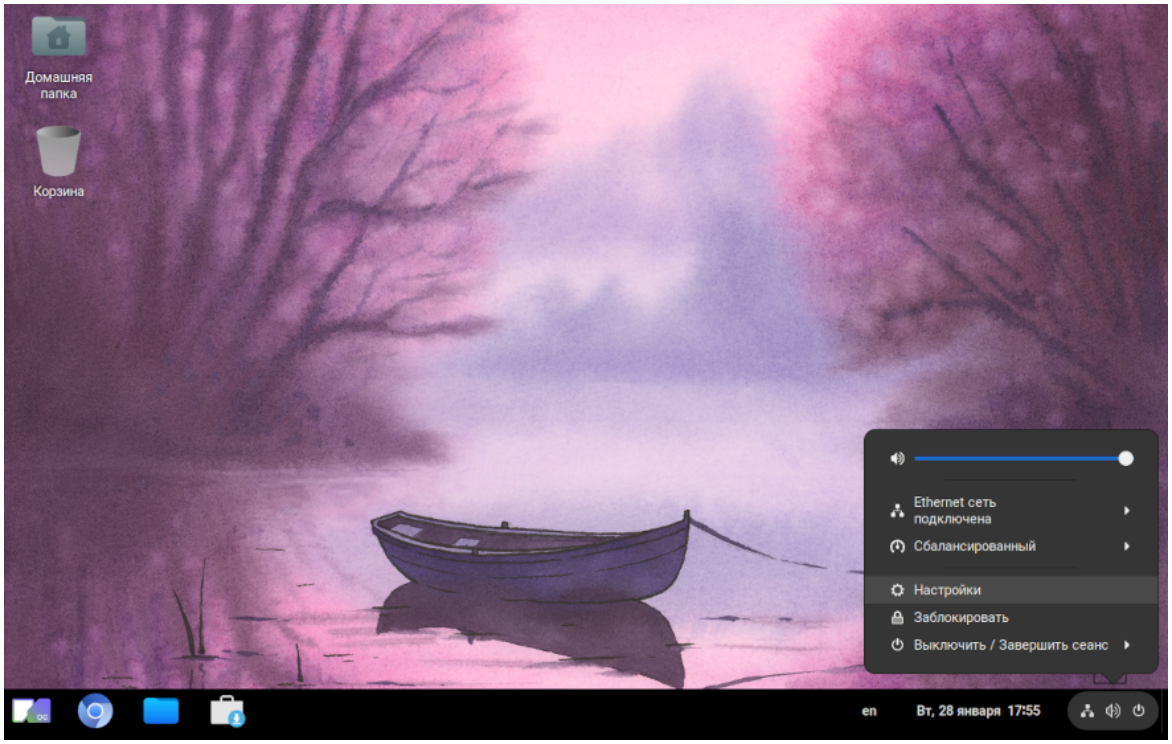

Рис. 16: «Настройки»

3.1. Беспроводная сеть Wi-Fi

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

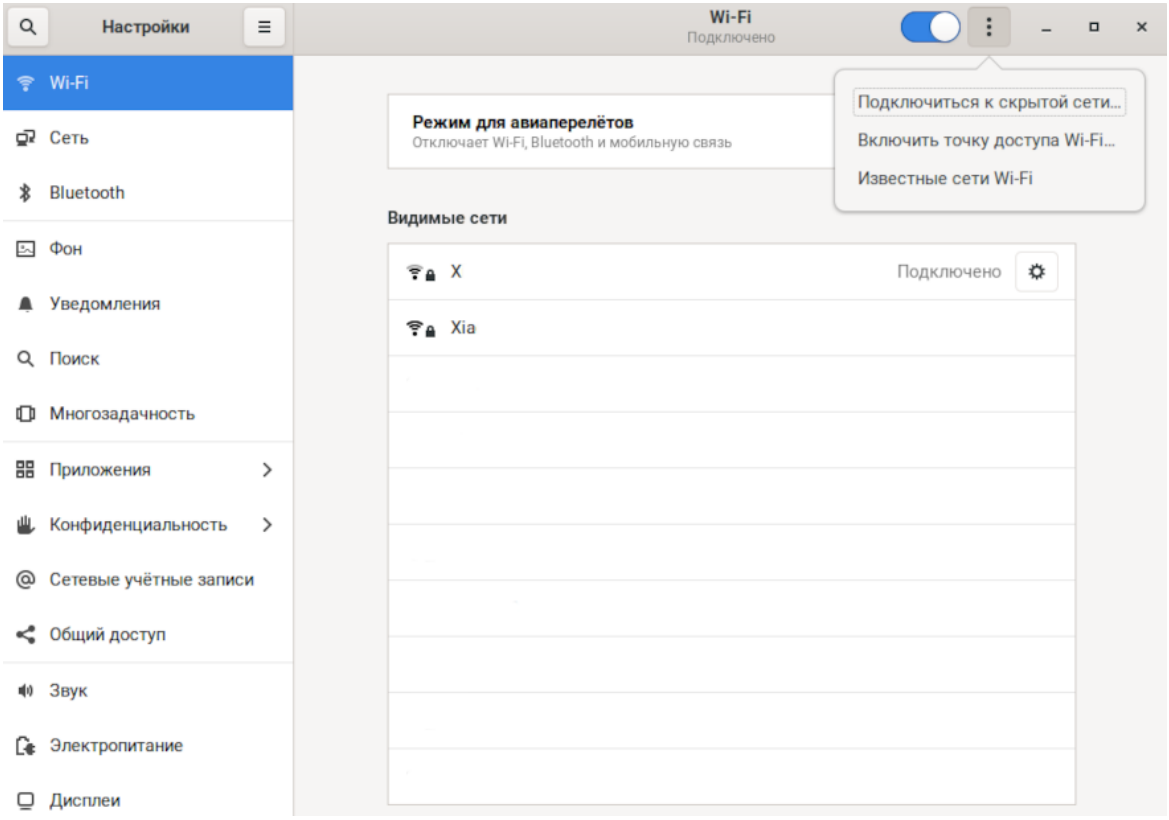

Рис. 17: Дополнительные возможности Wi-Fi

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.

3.2. Сеть

Для настройки и просмотра параметров сети и VPN перейдите в «Настройки» → «Сеть». Нажмите на значок шестерёнки для просмотра и настройки дополнительных параметров.

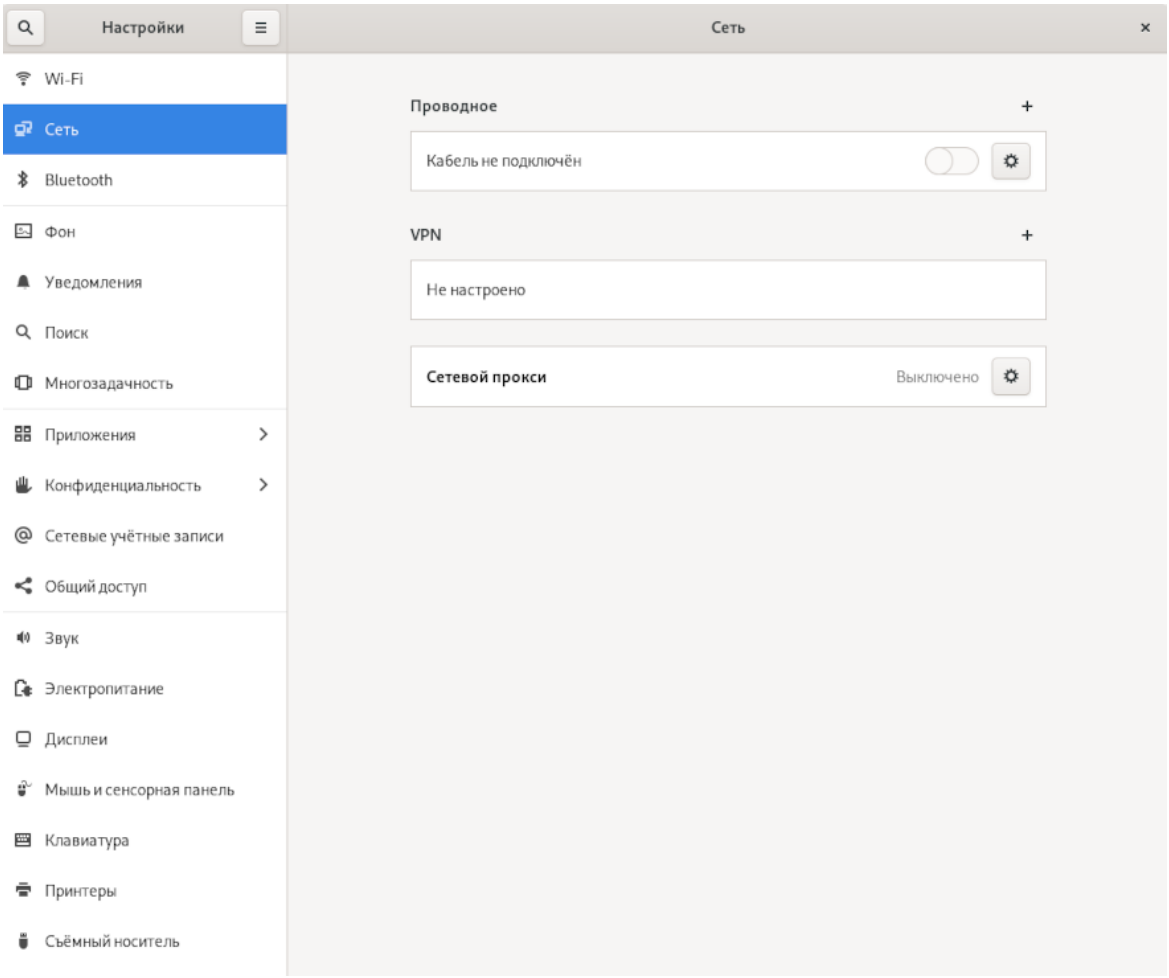

Рис. 18: Сеть

3.2.1. Настройка VPN

В ОС МСВСфера 9 реализована поддержка следующих VPN-сервисов:

- OpenConnect
- OpenVPN
- PPTP
- L2TP

Ниже мы рассмотрим как подключить каждый из них.

OpenConnect

Для добавления соединения OpenConnect выполните следующие действия:

1) Перейдите в «Настройки» → «Сеть» и нажмите на знак «+» напротив VPN.
2) В окне «Добавить VPN» выберите «Multi-protocol VPN client (openconnect)».

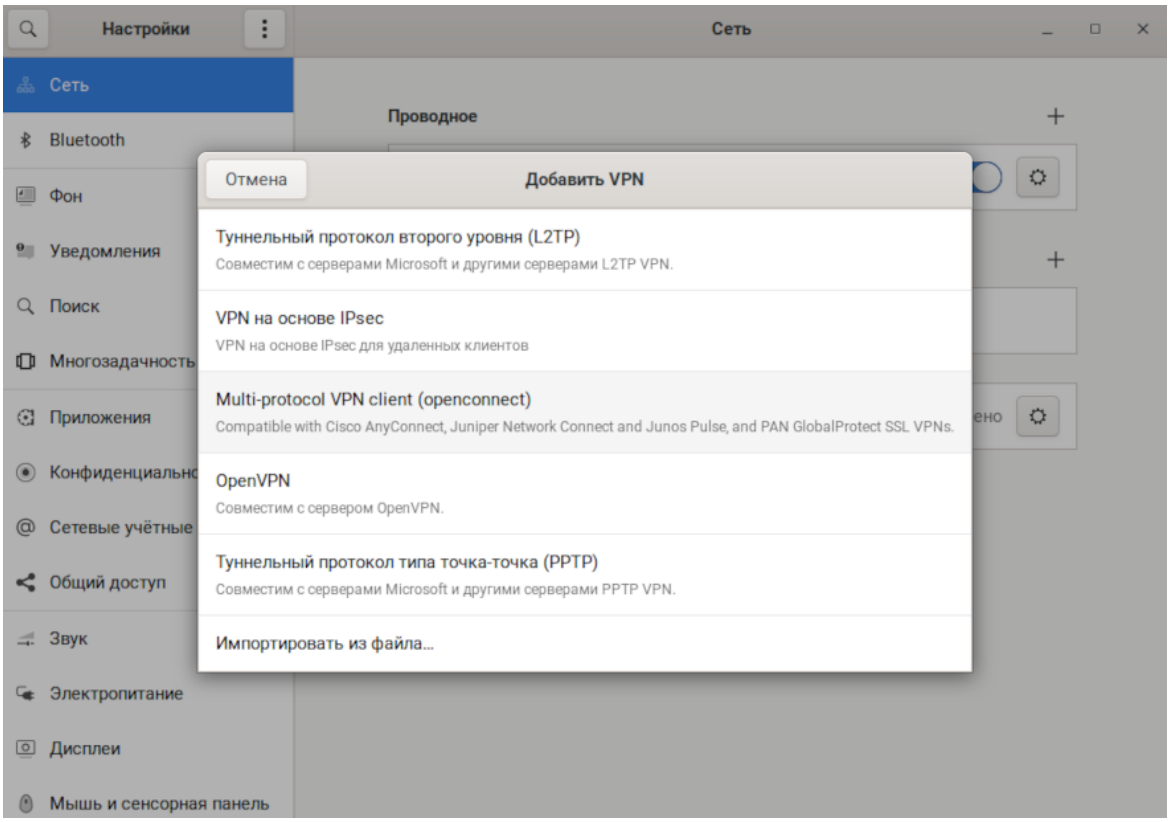

Рис. 19: OpenConnect

3) Во вкладке «Идентификация» укажите «Название» и заполните все необходимые поля.

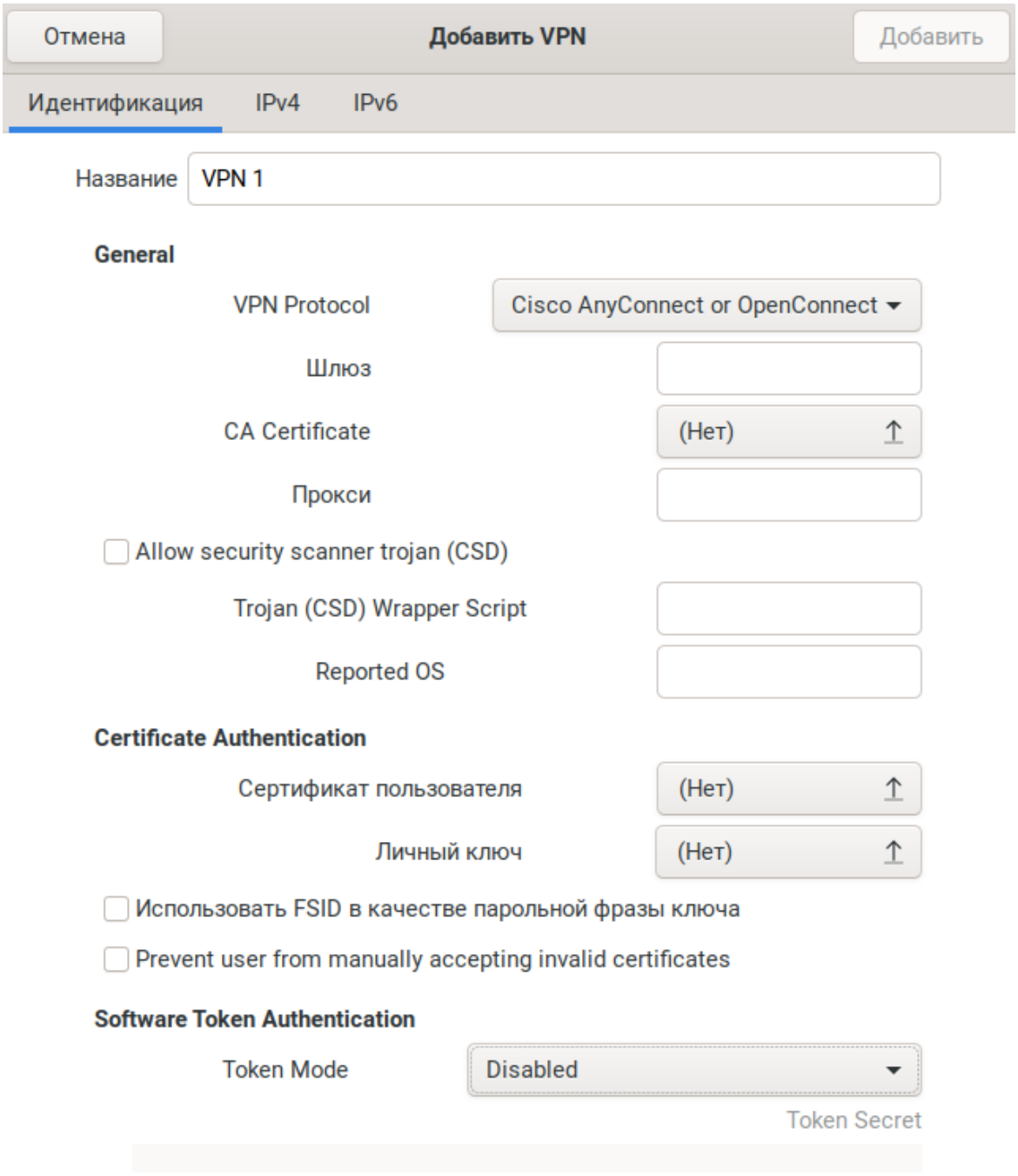

Рис. 20: «Идентификация»

4) При необходимости загрузите соответствующие сертификаты.
5) Перейдите во вкладку «IPv4» и поставьте галочку в поле «Использовать это подключение только для ресурсов в этой сети».

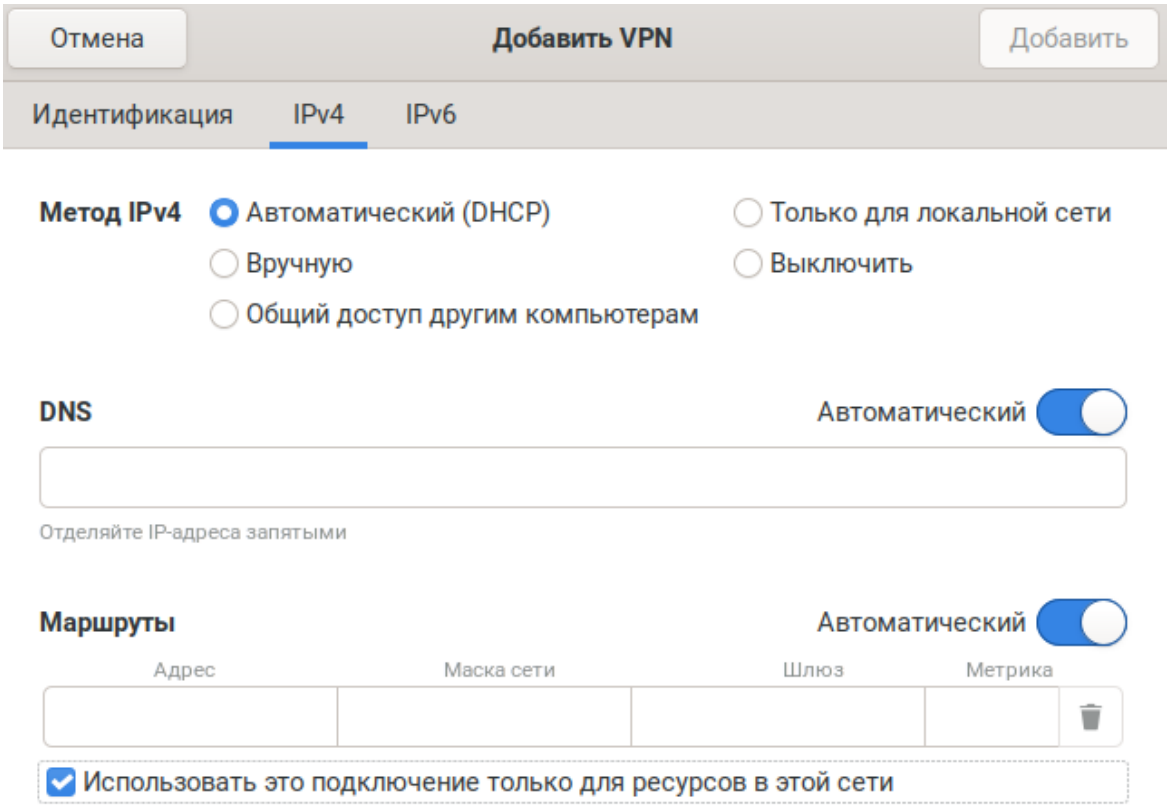

Рис. 21: IPv4/Использовать это подключение только для ресурсов в этой сети

6) Нажмите на кнопку «Добавить».
7) Добавленный VPN появится в списке.
8) Для включения VPN передвиньте слайдер. Вы также можете управлять подключением из системного меню.

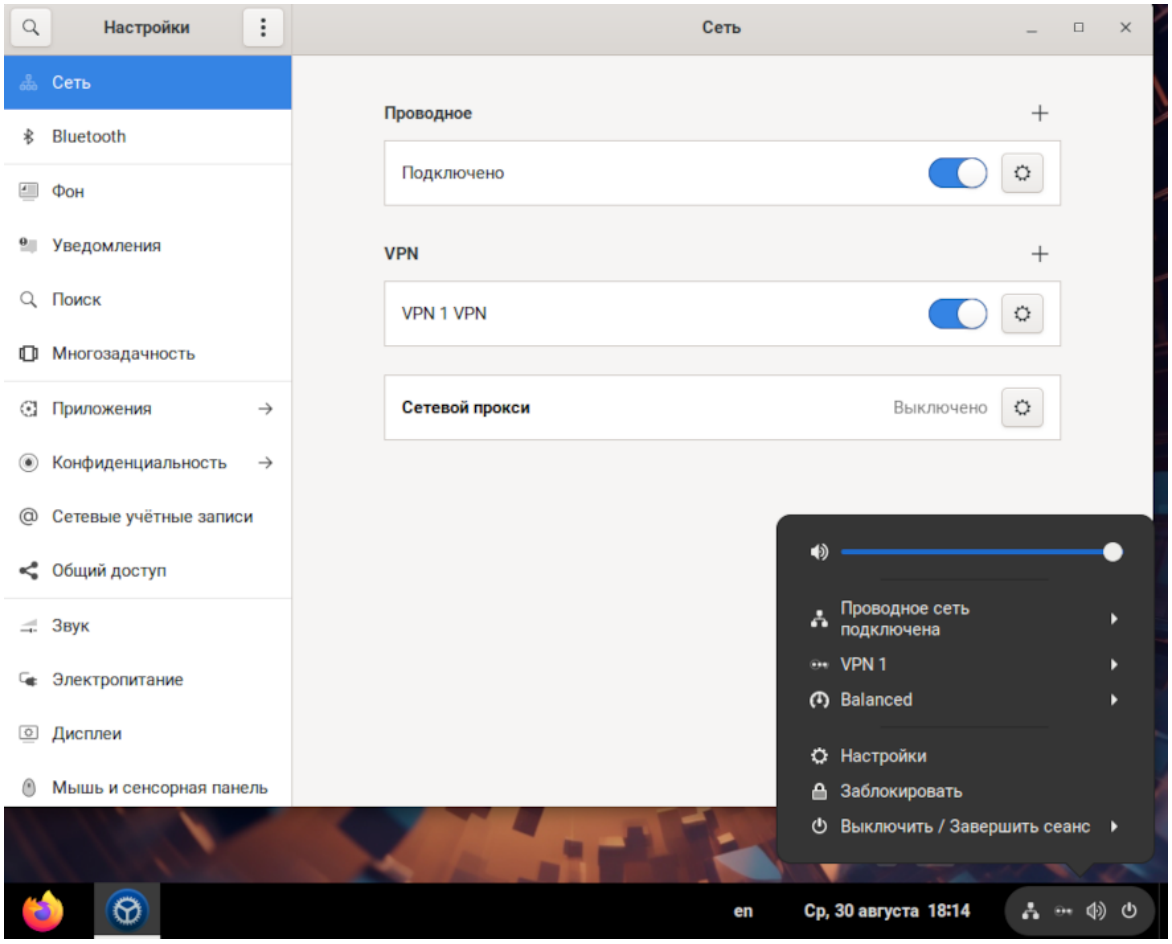

Рис. 22: Включённый VPN

OpenVPN

Для добавления соединения OpenVPN выполните следующие действия:

1) Перейдите в «Настройки» → «Сеть» и нажмите на знак «+» напротив VPN.
2) В окне «Добавить VPN» выберите «OpenVPN».
3) Во вкладке «Идентификация» укажите «Название» и «Шлюз».
4) Выберите необходимый тип аутентификации и загрузите соответствующие сертификаты.
5) Перейдите во вкладку «IPv4» и поставьте галочку в поле «Использовать это подключение только для ресурсов в этой сети».
7) Нажмите на кнопку «Добавить».
8) Добавленный VPN появится в списке.
9) Для включения VPN передвиньте слайдер. Вы также можете управлять подключением из системного меню.

PPTP

Для добавления PPTP выполните следующие действия:

1) Перейдите в «Настройки» → «Сеть» и нажмите на знак «+» напротив VPN.
2) В окне «Добавить VPN» выберите «Туннельный протокол типа точка-точка (PPTP)».
3) Во вкладке «Идентификация» заполните поля «Название», «Шлюз» и «Имя пользователя».
4) В строке «Пароль» нажмите на значок пользователя и выберите «Запомнить пароль только для этого пользователя».
5) Нажмите на «Дополнительно» и поставьте галочку в поле «Использовать шифрование MPPE», затем нажмите на «ОК».
6) Перейдите во вкладку «IPv4» и поставьте галочку в поле «Использовать это подключение только для ресурсов в этой сети» и нажмите «Применить».
7) Нажмите на кнопку «Добавить».
8) Добавленный VPN появится в списке.
9) Для включения VPN передвиньте слайдер. Вы также можете управлять подключением из системного меню.

L2TP

В целях безопасности поддержка протокола IKEv1 по умолчанию отключена. Чтобы включить её, добавьте опцию `ikev1-policy=accept` в секцию `config setup` файла `/etc/ipsec.conf`.

Для добавления L2TP выполните следующие действия:

1) Перейдите в «Настройки» → «Сеть» и нажмите на знак «+» напротив VPN.
2) В окне «Добавить VPN» выберите «Туннельный протокол второго уровня (L2TP)».
3) Во вкладке «Идентификация» заполните поля «Название», «Шлюз», «Имя пользователя» и «Пароль».
4) В строке «Пароль» нажмите на значок пользлвателя и выберите «Запомнить пароль только для этого пользователя».
5) Нажмите на «Параметры IPsec» и поставьте галочку в поле «Enable IPsec tunnel to L2 TP host». Затем укажите «Pre-shared key» и нажмите

«Применить».

6) Перейдите во вкладку «IPv4» и поставьте галочку в поле «Использовать это подключение только для ресурсов в этой сети».
7) Нажмите на кнопку «Добавить».
8) Добавленный VPN появится в списке.
9) Для включения VPN передвиньте слайдер. Вы также можете управлять подключением из системного меню.

3.3. Беспроводная связь Bluetooth

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

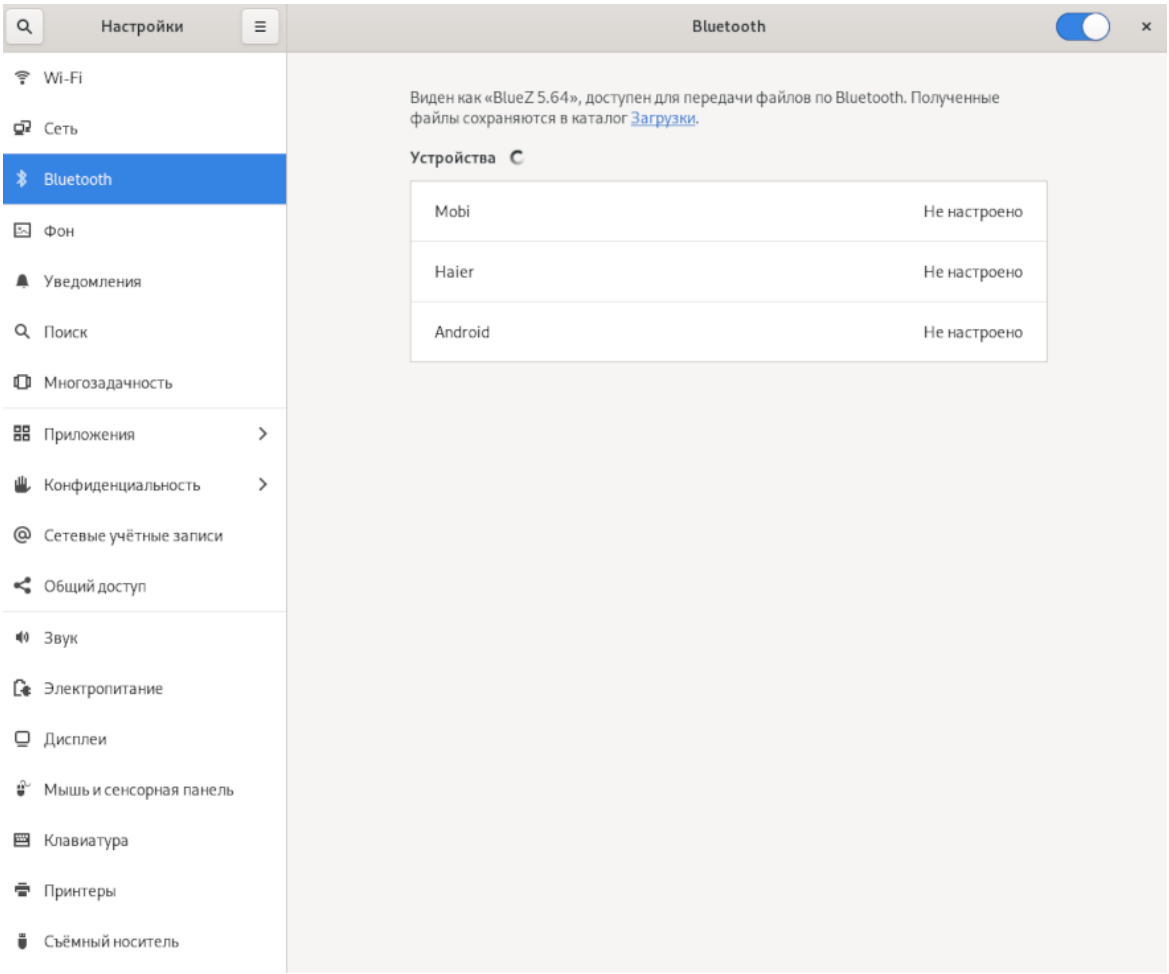

Рис. 23: Bluetooth

3.4. Фон

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

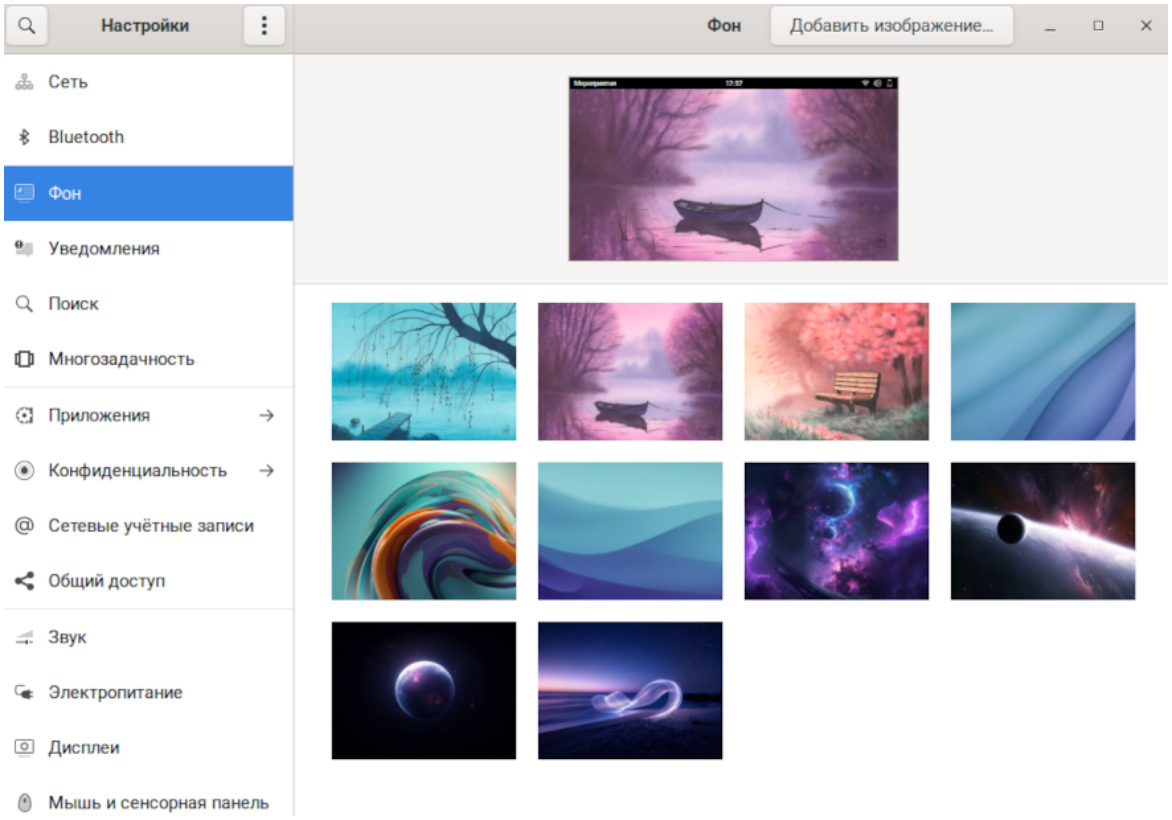

Рис. 24: Фон

3.5. Уведомления

Перейдите в «Настройки» → «Уведомления» для настройки уведомлений приложений или включения/выключения режима «Не беспокоить». Нажмите на приложение для настройки уведомлений отдельно для него.

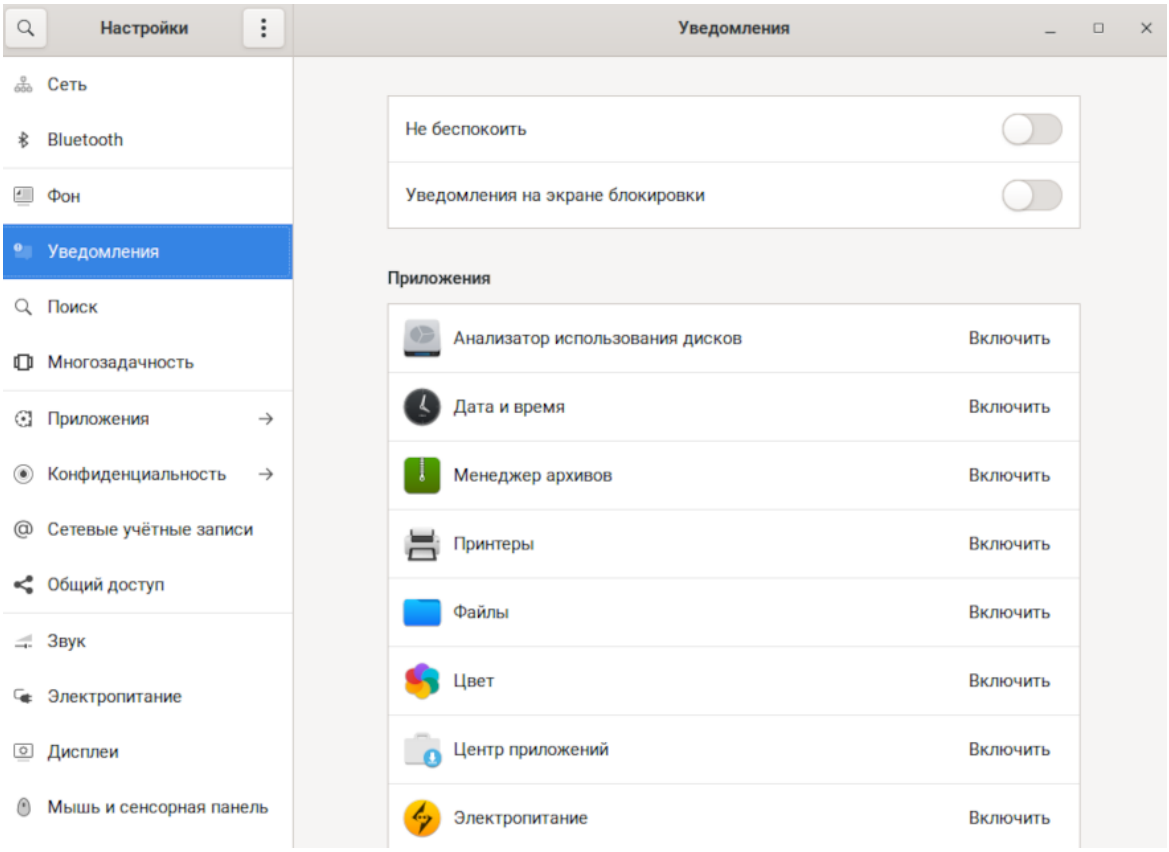

Рис. 25: Уведомления

3.6. Поиск

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

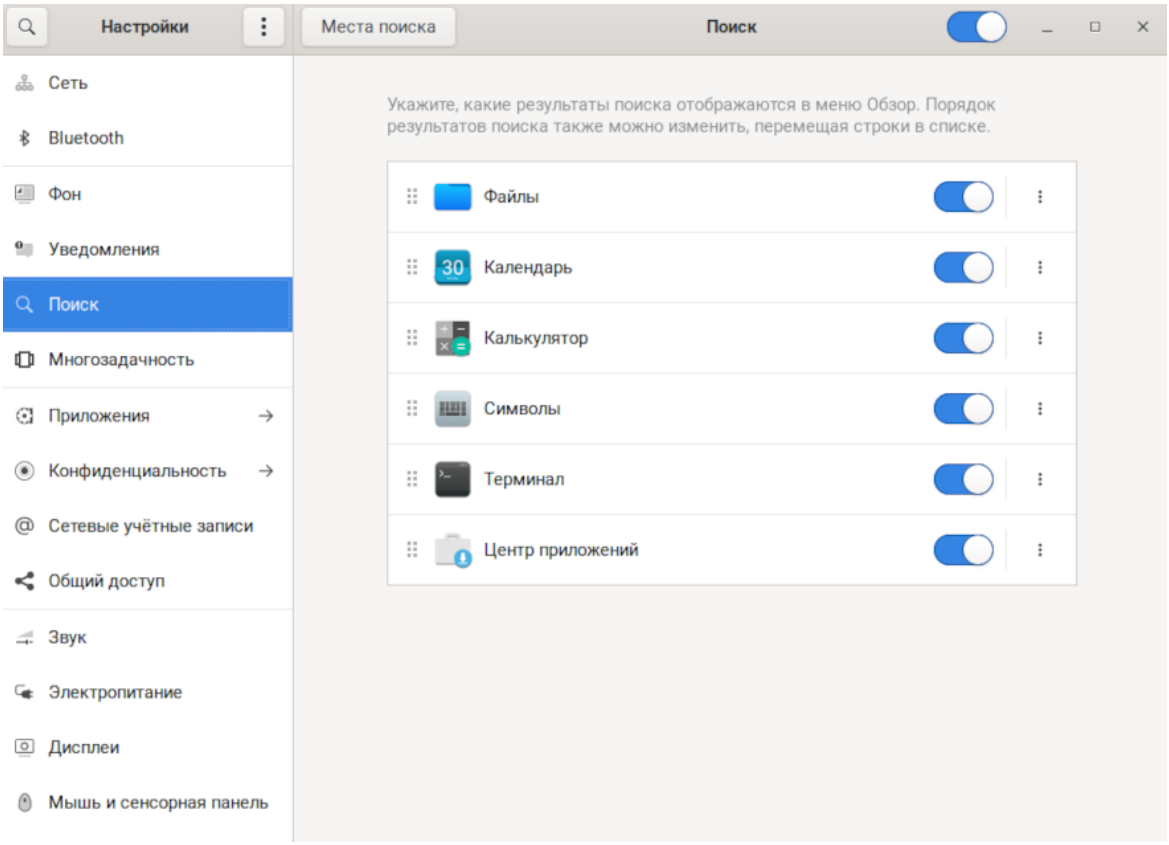

Рис. 26: Поиск

3.7. Многозадачность

Перейдите в «Настройки» → «Многозадачность» для настройки параметров работы с несколькими рабочими столами/мониторами и приложениями.

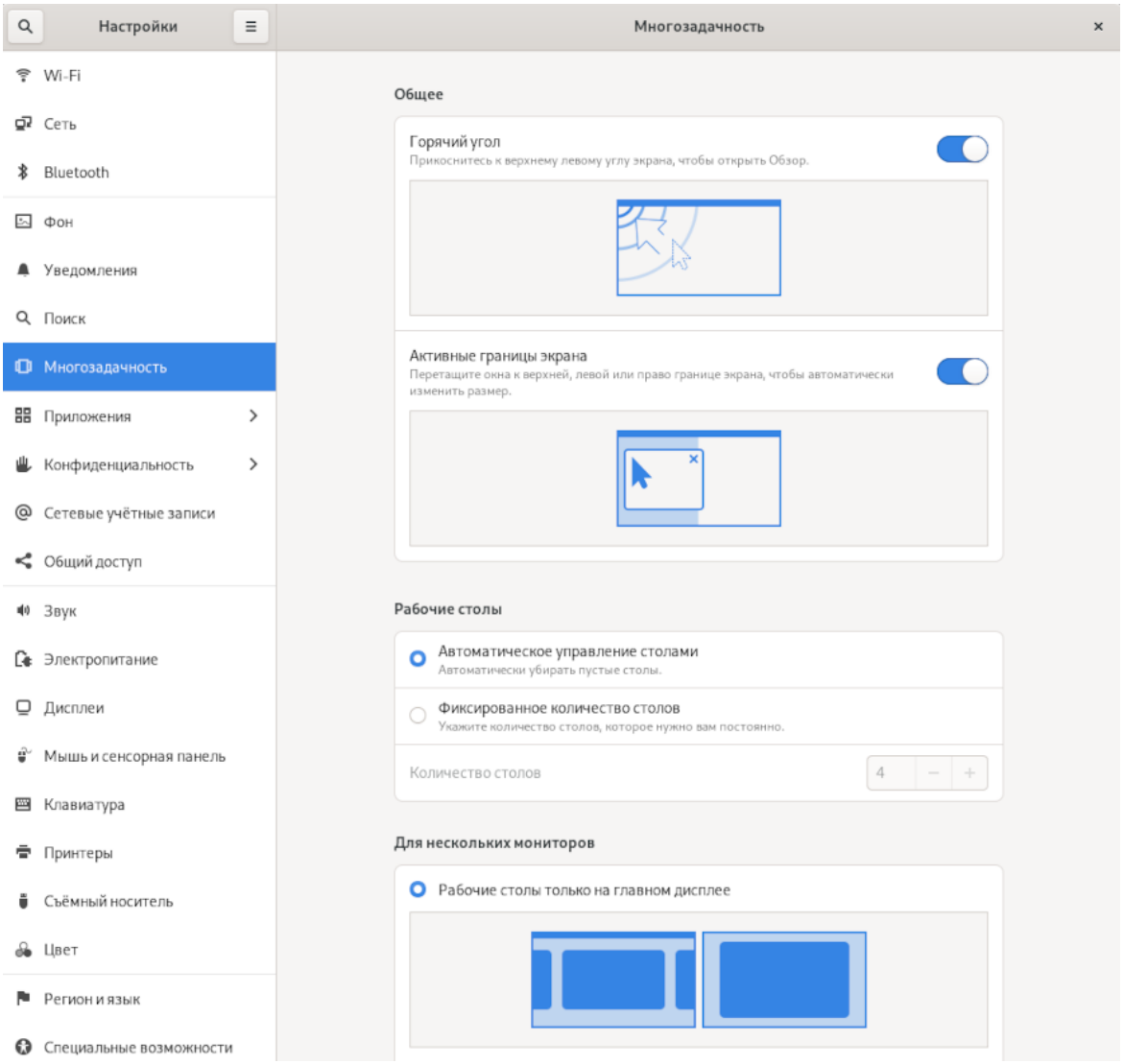

Рис. 27: Многозадачность

3.8. Приложения

Перейдите в «Настройки» → «Приложения» для просмотра и настройки параметров приложений. Нажмите на приложение для просмотра и редактирования его параметров.

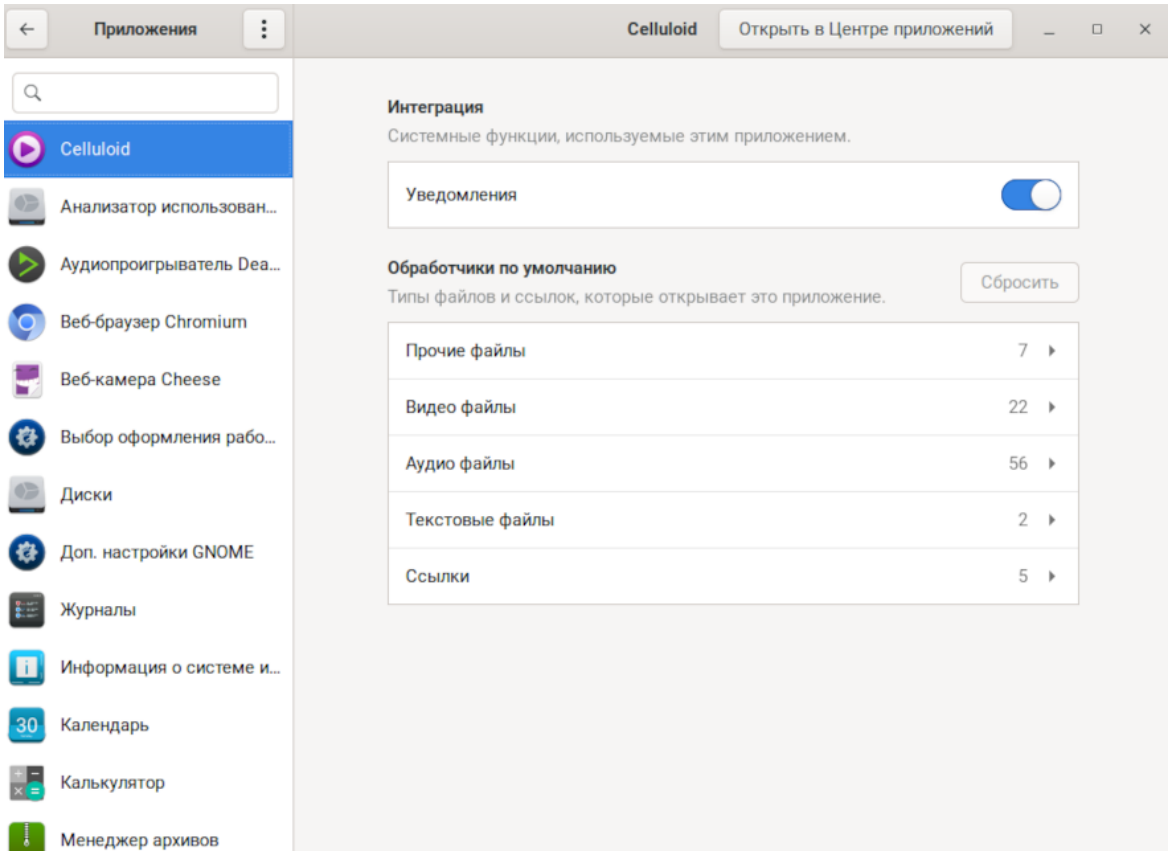

Рис. 28: Приложения

Могут использоваться следующие параметры:

- **Права и доступ** — данные и сервисы, к которым это приложение запрашивает доступ, и разрешения, которые ему требуются.
- **Интеграция** — системные функции, используемые этим приложением.
- **Обработчики по умолчанию** — типы файлов и ссылок, которые открывает это приложение.
- **Использование** — сколько ресурсов использует это приложение.

3.9. Конфиденциальность. Сервисы местоположения

Для просмотра и настройки параметров получения приложениями информации о местоположении перейдите в «Настройки» → «Конфиденциальность» → «Сервисы местоположения».

Включение сервисов местоположения позволяет автоматически изменять часовые пояса и синхронизировать текущее время.

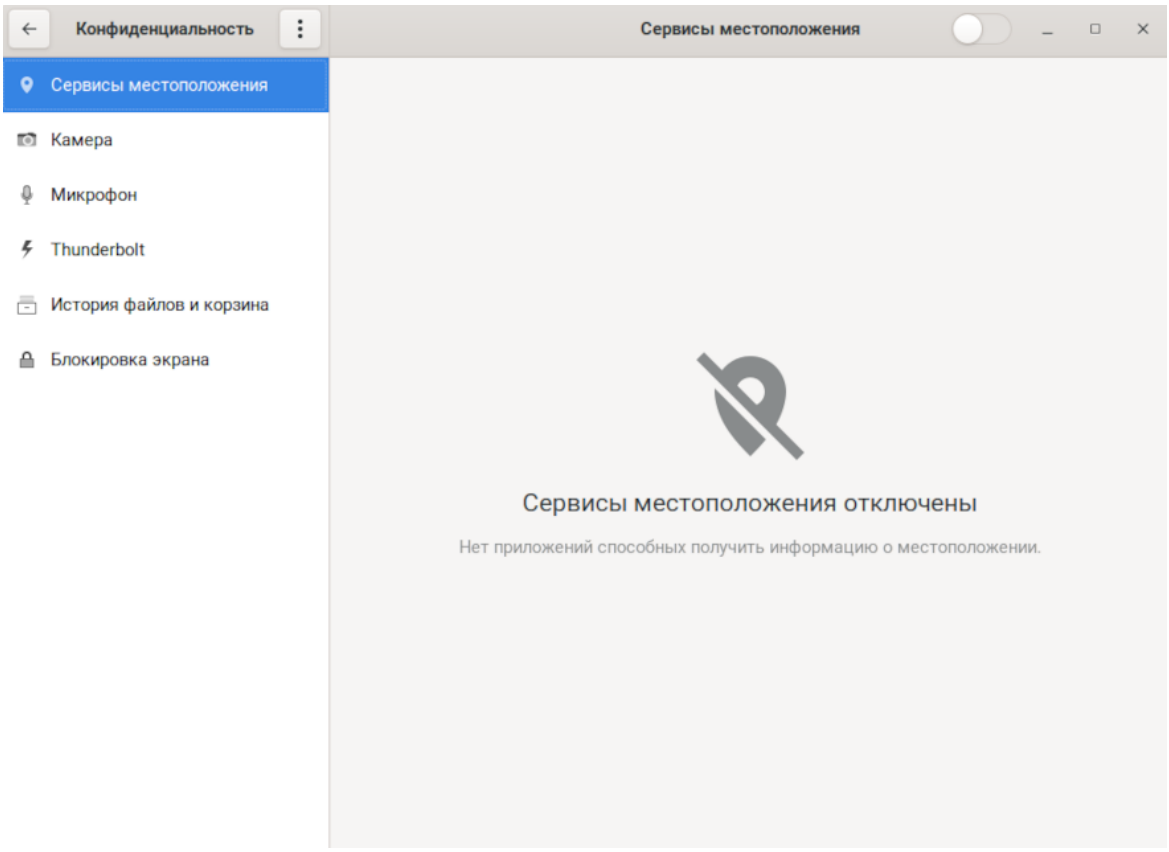

Рис. 29: Сервисы местоположения

3.10. Конфиденциальность. Камера

Для просмотра и настройки параметров использования приложениями камеры перейдите в «Настройки» → «Конфиденциальность» → «Камера».

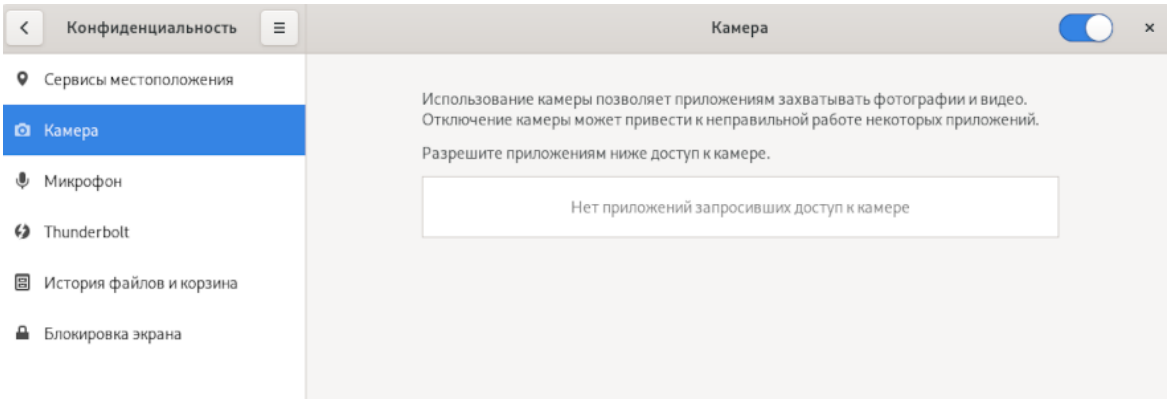

Рис. 30: Камера

3.11. Конфиденциальность. Микрофон

Для просмотра и настройки параметров использования приложениями микрофона перейдите в «Настройки» → «Конфиденциальность» → «Микрофон».

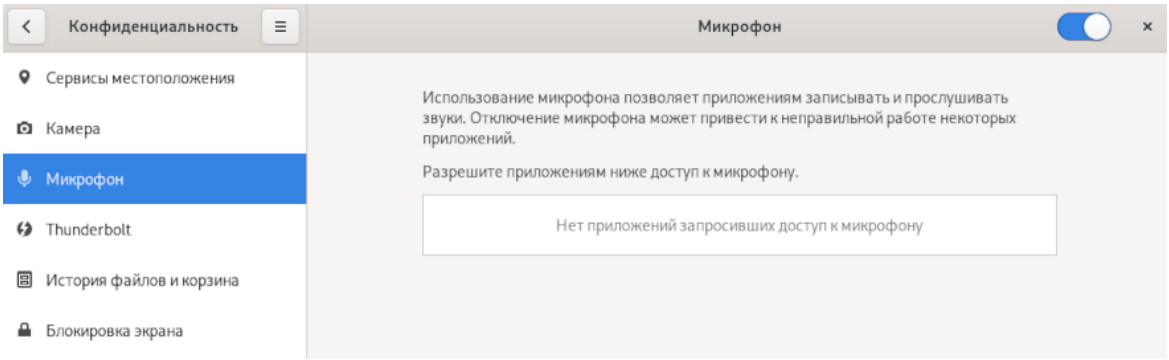

Рис. 31: Микрофон

3.12. Конфиденциальность. Аппаратный интерфейс Thunderbolt

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

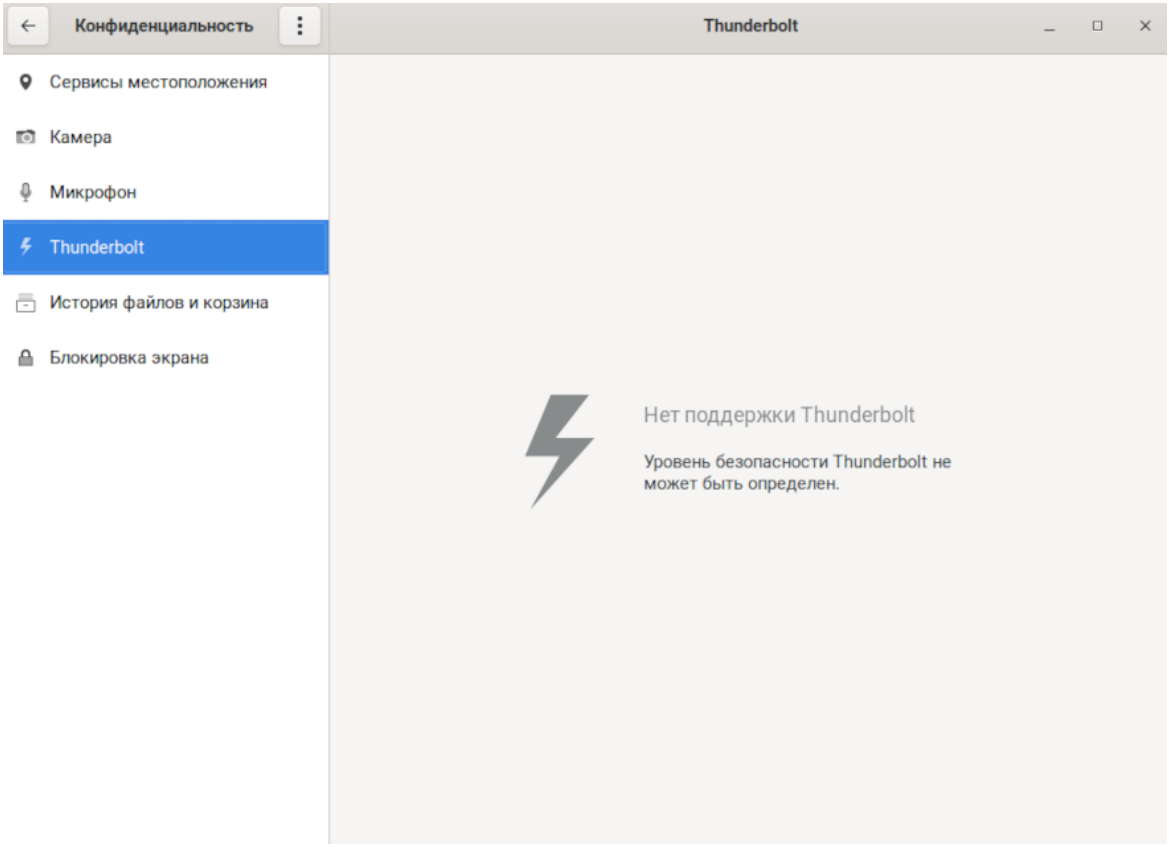

Рис. 32: Thunderbolt

3.13. Конфиденциальность. История файлов и корзина

Для настройки параметров ведения и хранения статистики и истории перейдите в «Настройки» → «Конфиденциальность» → «История файлов и корзина» → «История файлов».

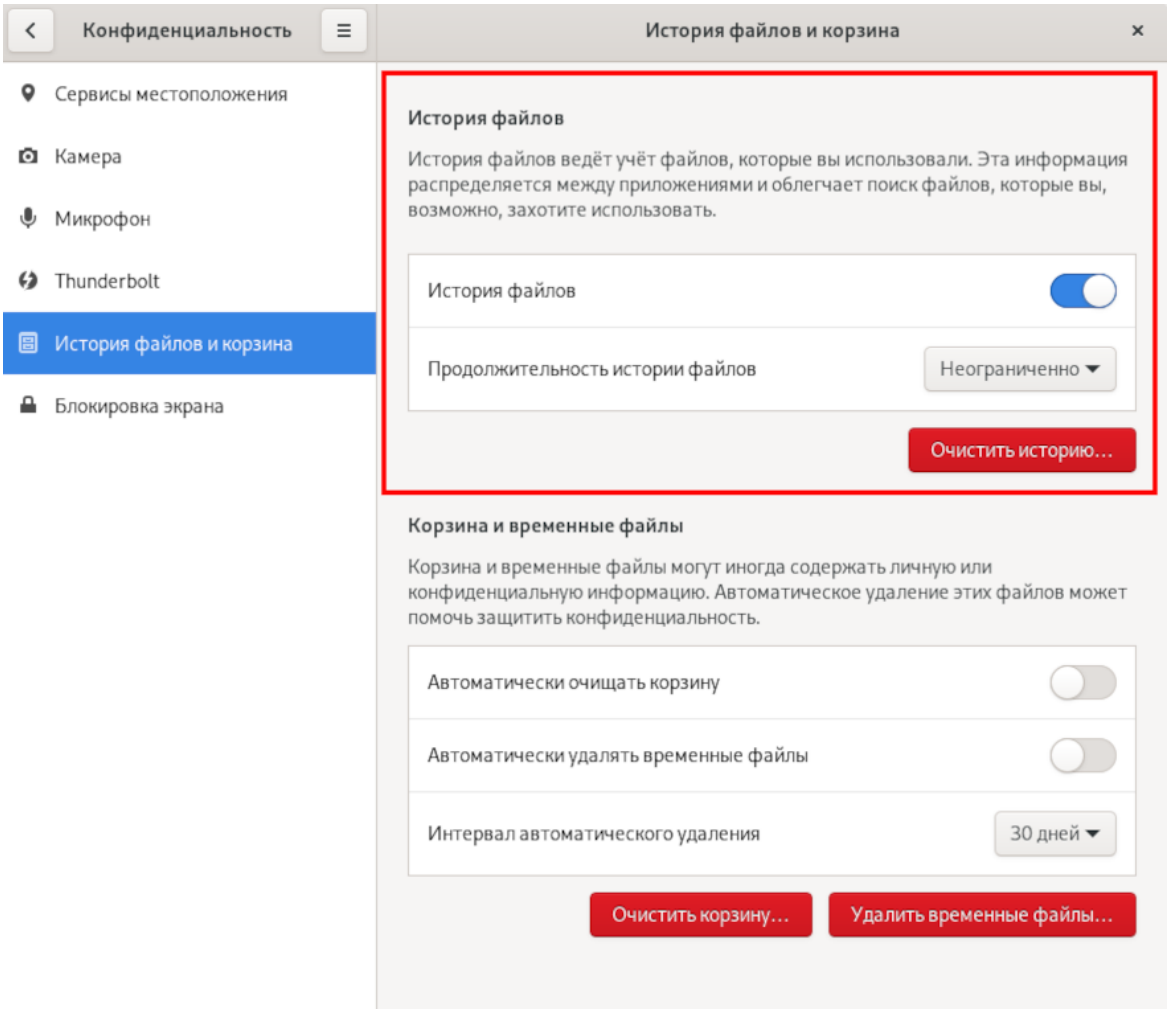

Рис. 33: Статистика и история

Очистка корзины и временные файлы

Для настройки параметров автоматической очистки корзины и удаления временных файлов перейдите в «Настройки» → «Конфиденциальность» → «История файлов и корзина» → «Корзина и временные файлы».

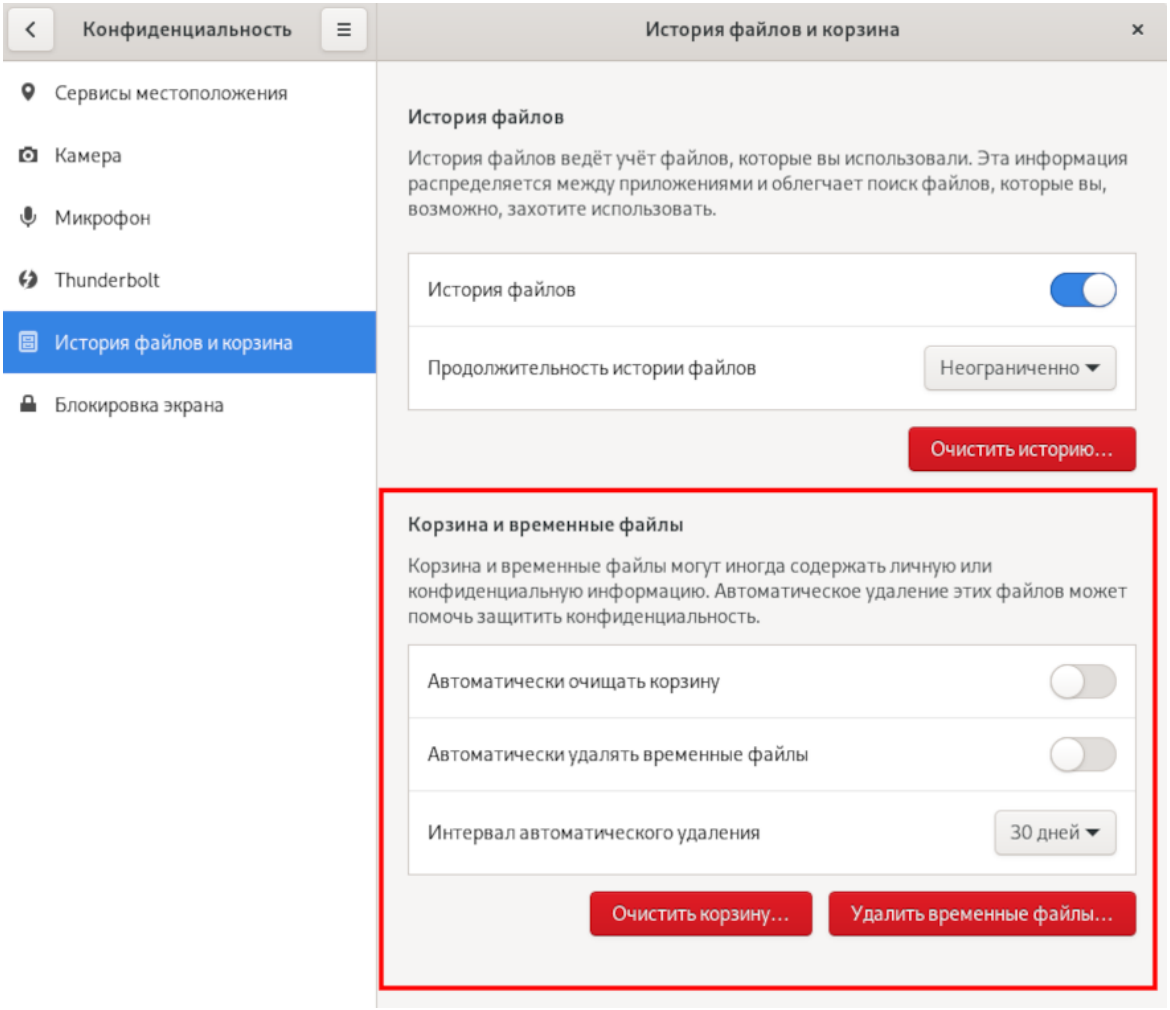

Рис. 34: Корзина и временные файлы

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.

3.14. Конфиденциальность. Блокировка экрана

Для настройки параметров блокировки экрана перейдите в «Настройки» → «Конфиденциальность» → «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».

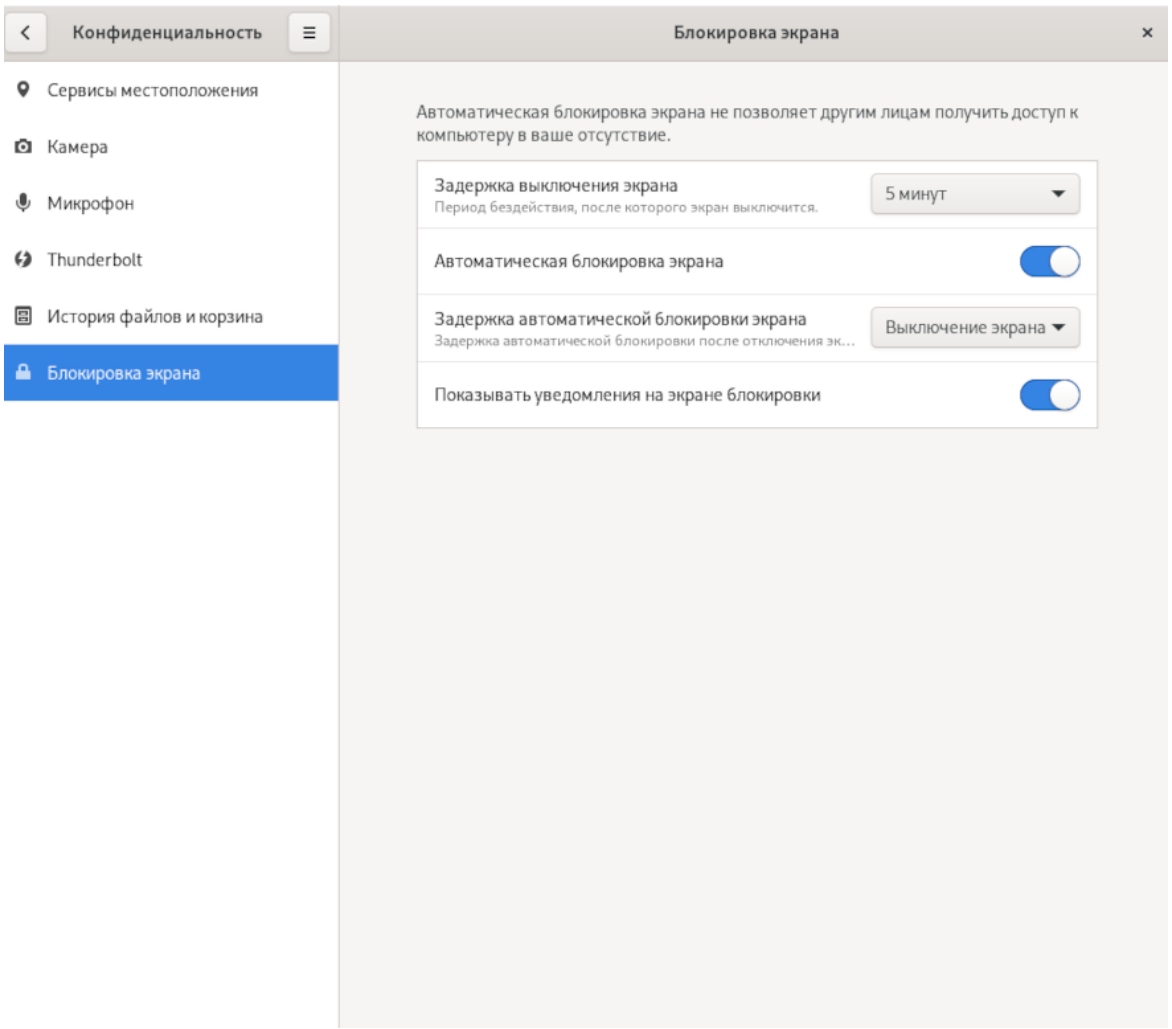

Рис. 35: Блокировка экрана

3.15. Сетевые учётные записи

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

Нажмите на сервис для добавления учётной записи.

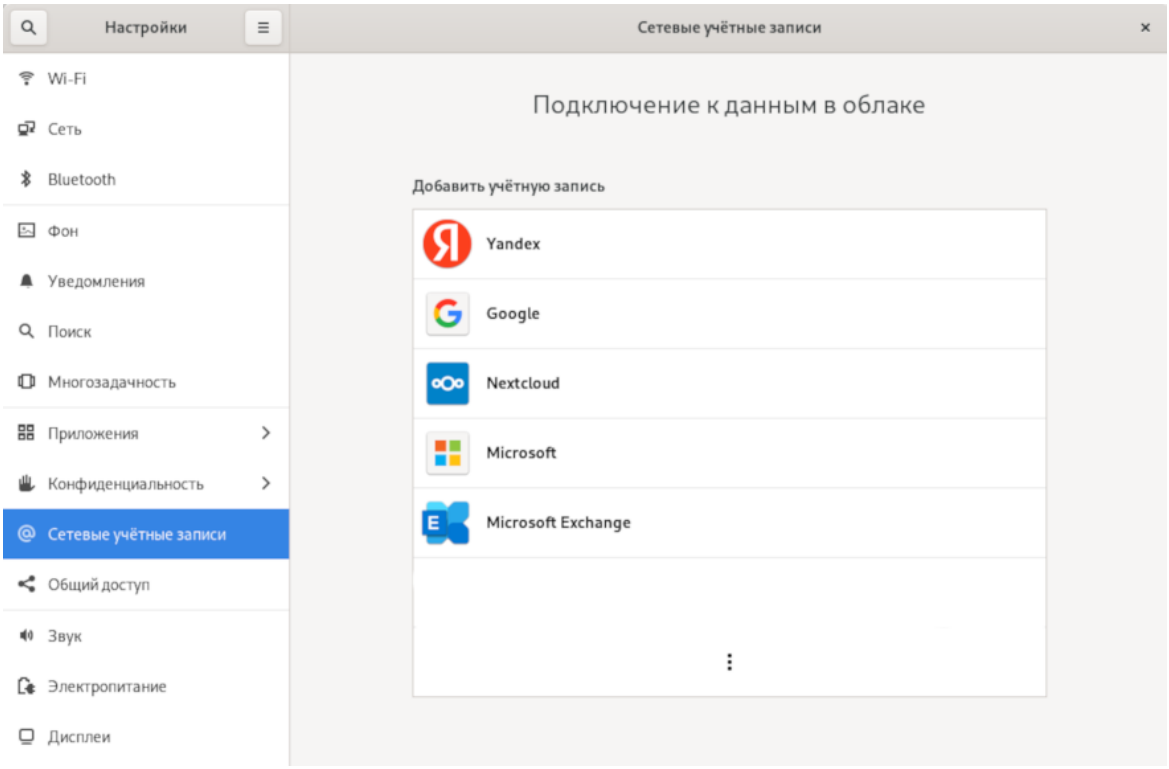

Рис. 36: Сетевые учётные записи

3.15.1. Подключение учётной записи Яндекс

Для подключения учётной записи Яндекс перейдите в «Настройки» → «Сетевые учётные записи» и выберите «Yandex».

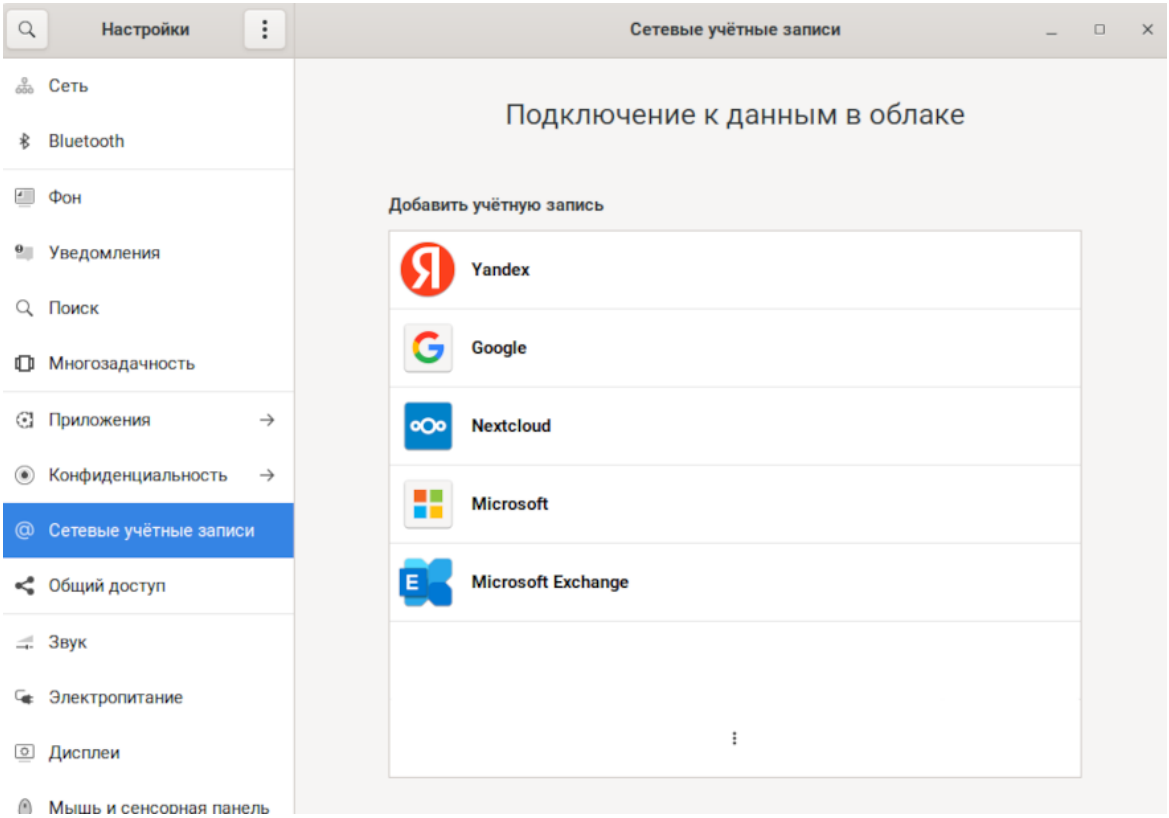

Рис. 37: Добавление учётной записи Яндекс

Укажите ваш номер телефона, привязанный к «Яндекс ID». Или выберите «Другие способы входа» и укажите необходимые данные для входа или же войдите по QR-коду.

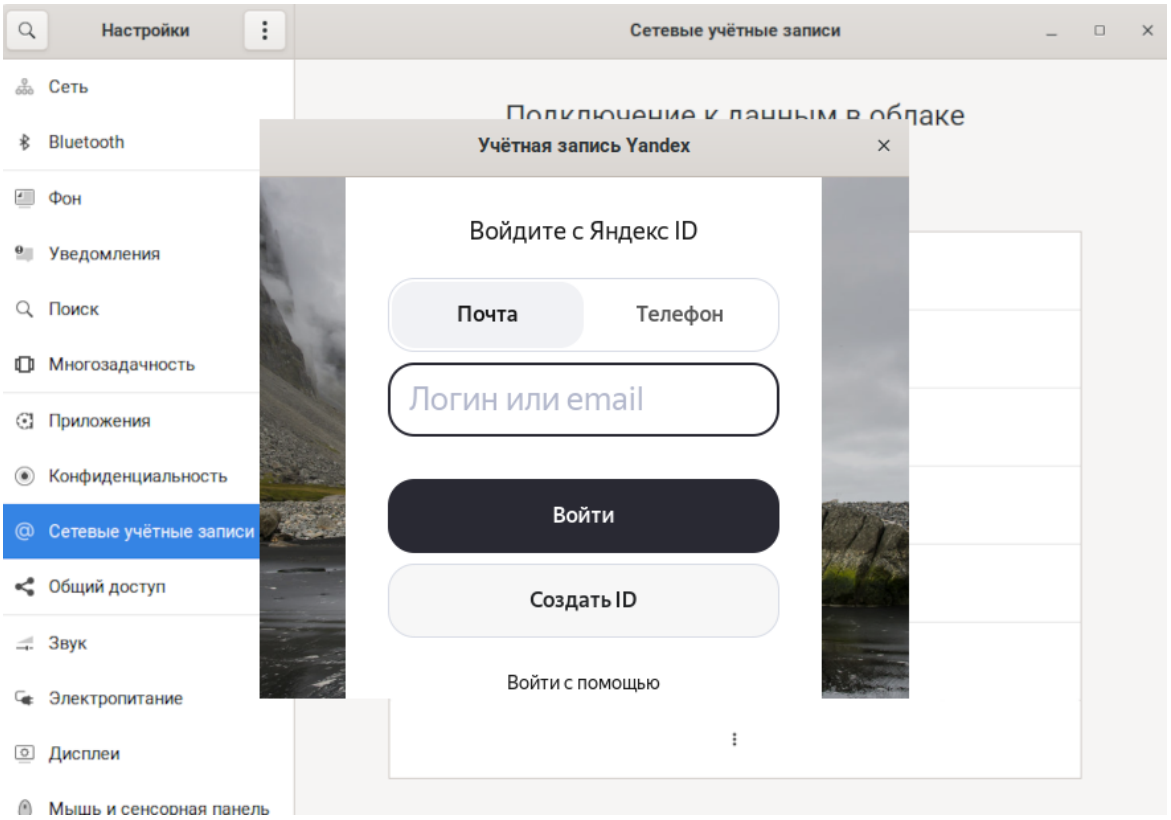

Рис. 38: Другие способы входа

Выберите необходимые сервисы, к которым вы хотите иметь доступ.

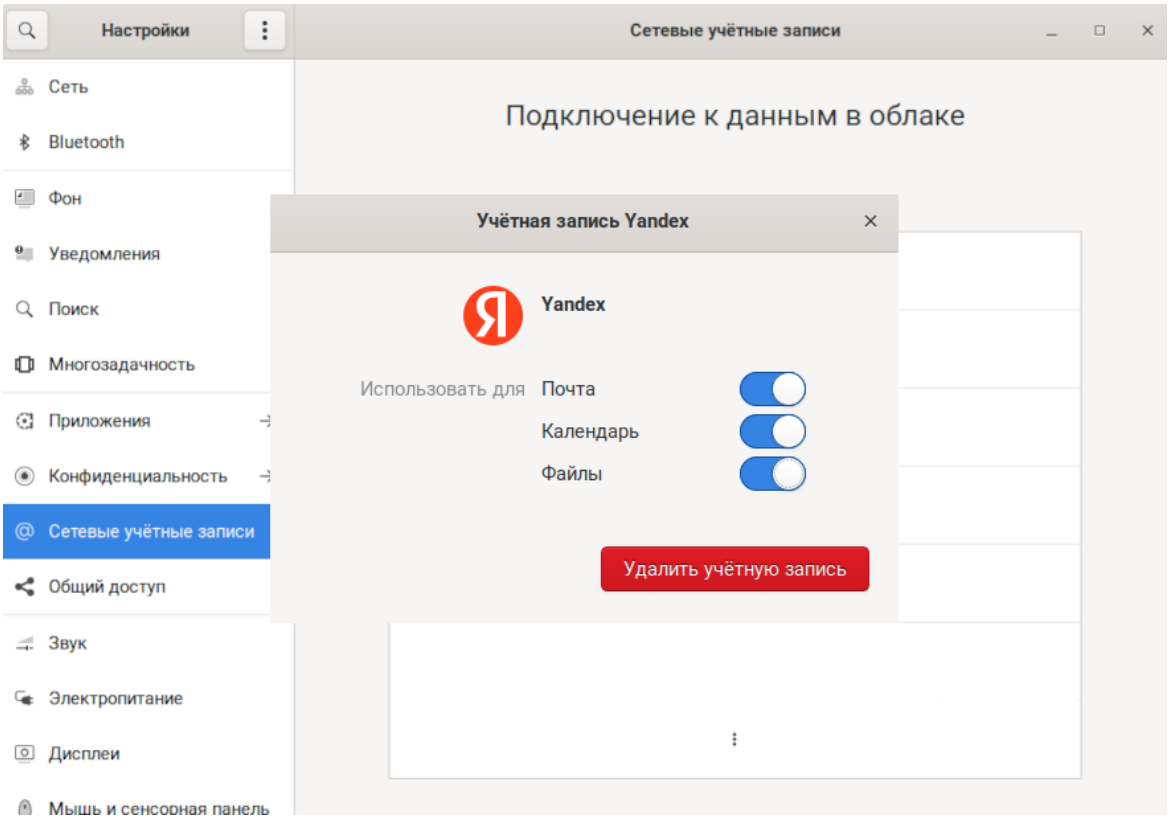

Рис. 39: Учётная запись добавлена

Ваша учётная запись Яндекс будет добавлена. И появится в списке.

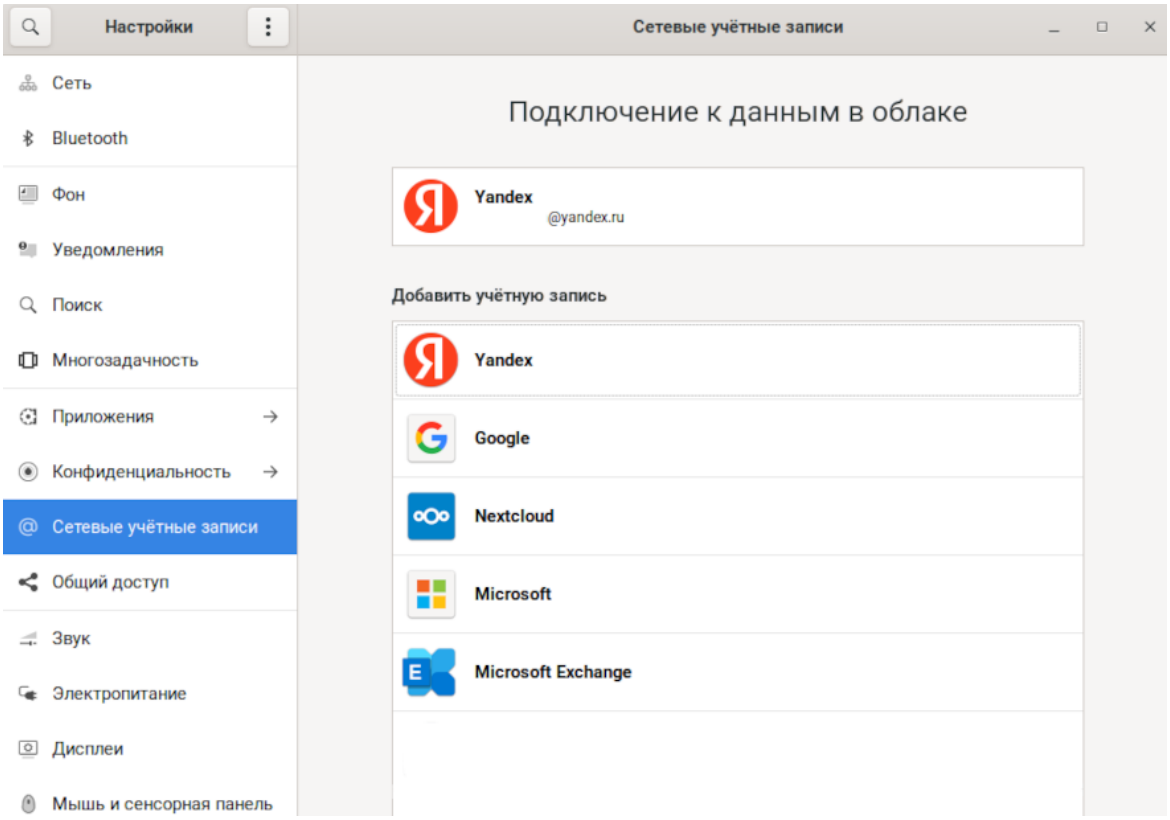

Рис. 40: Учётная запись Яндекс

Теперь вы можете просматривать и редактировать файлы с вашего «Яндекс Диска», они отображаются в приложении «Файлы».

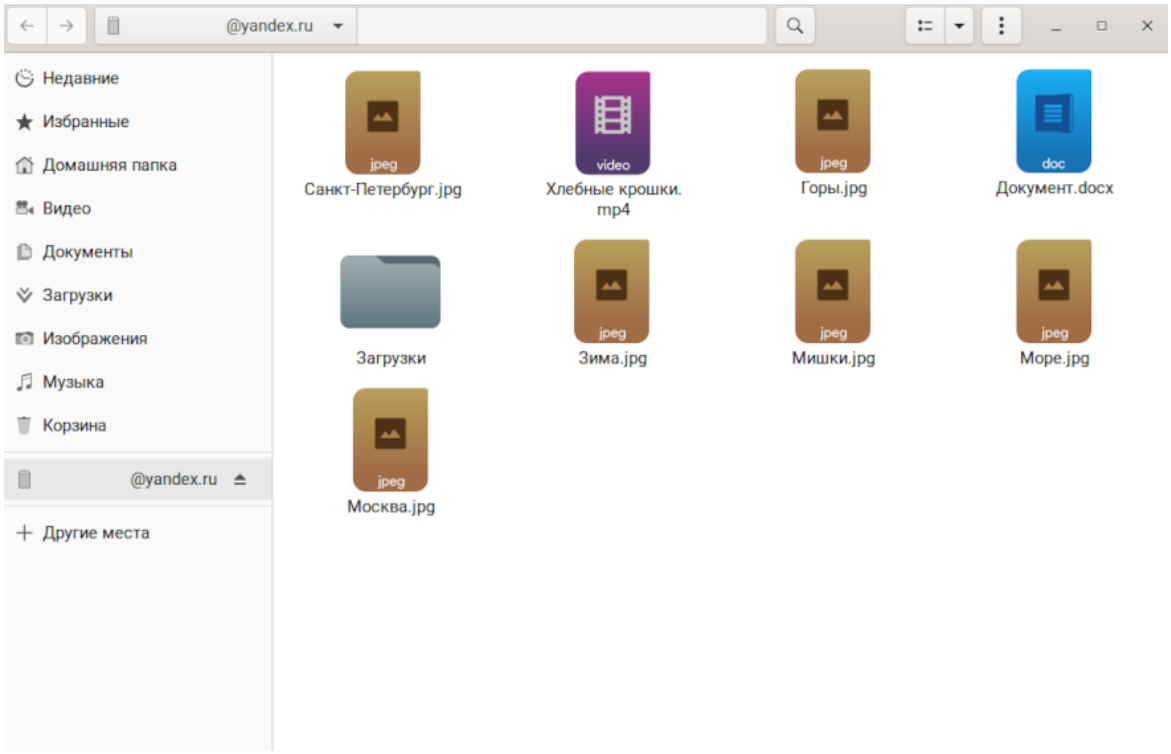

Рис. 41: Яндекс Диск

Также ваша «Яндекс Почта» теперь доступна из приложения «Evolution».

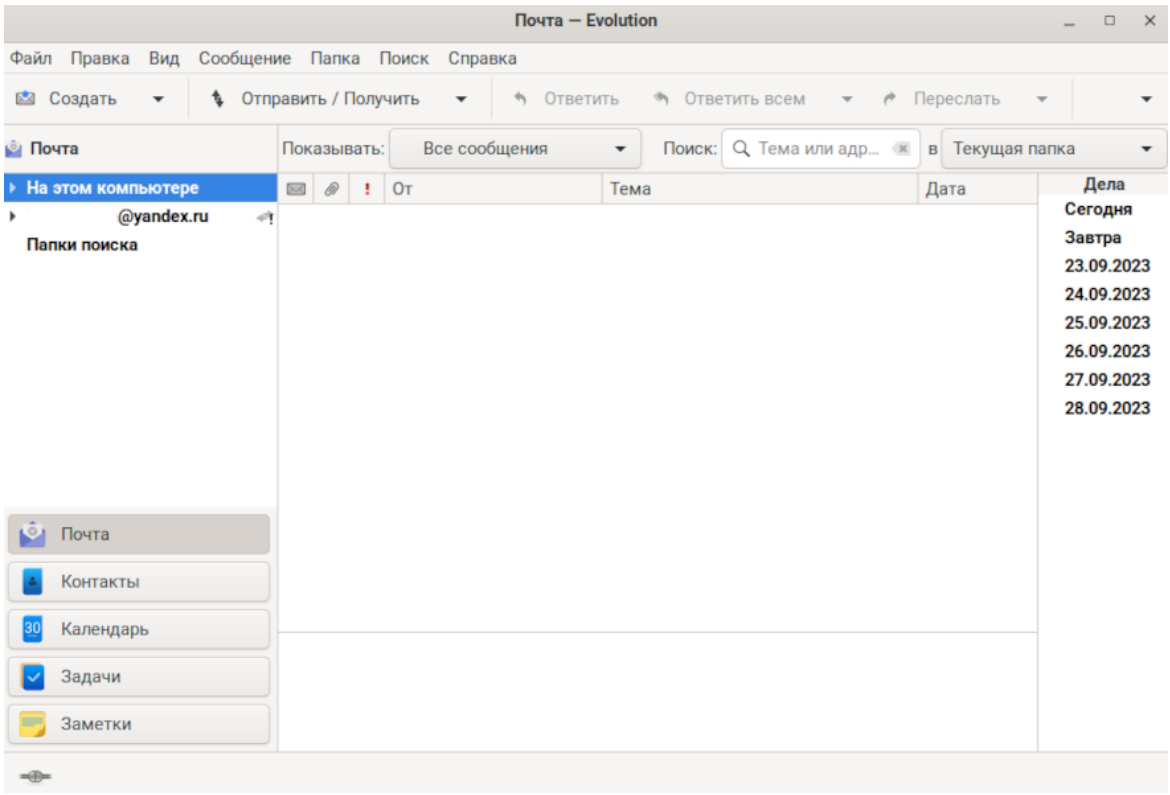

Рис. 42: Яндекс Почта

3.16. 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» → «Общий доступ к экрану».

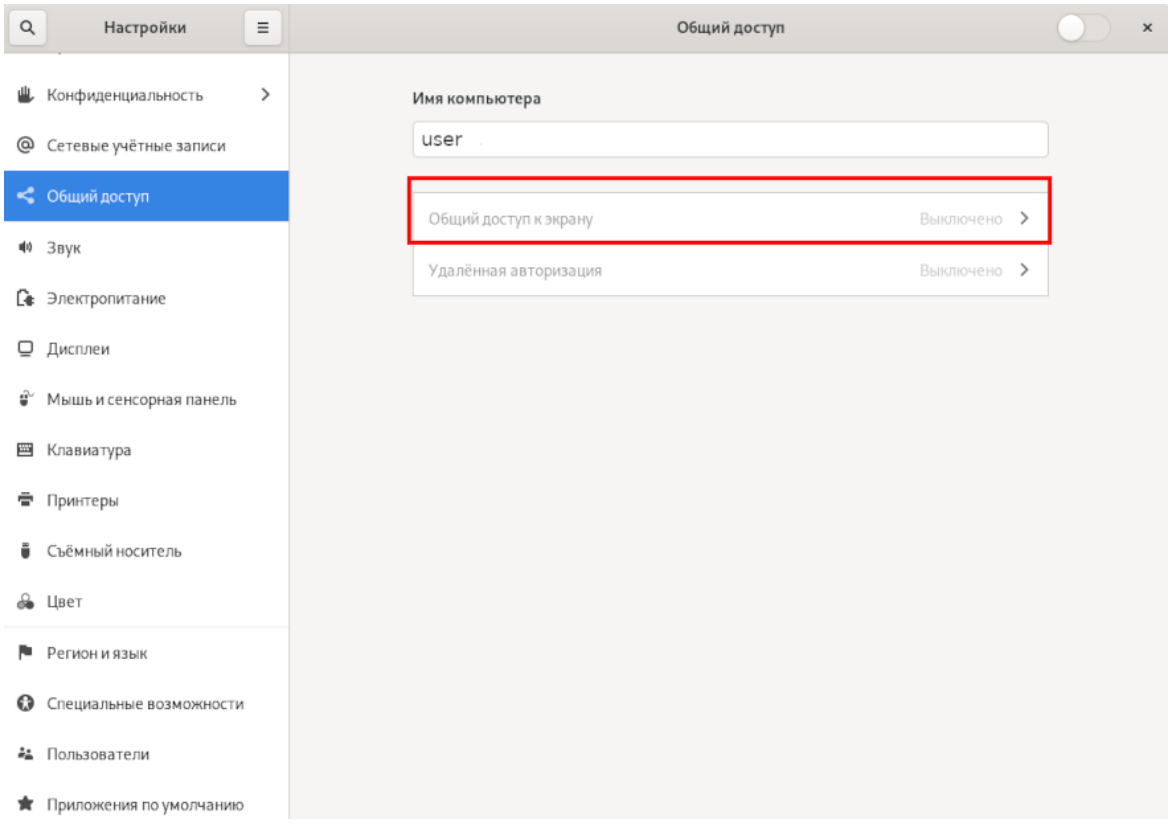

Рис. 43: Общий доступ к экрану

Удалённая авторизация

Удалённая авторизация предоставляет возможность удалённым пользователям подключаться к системе при помощи SSH-соединения через терминал.

Для настройки параметров общего доступа к экрану перейдите в «Настройки» → «Общий доступ» → «Удалённая авторизация».

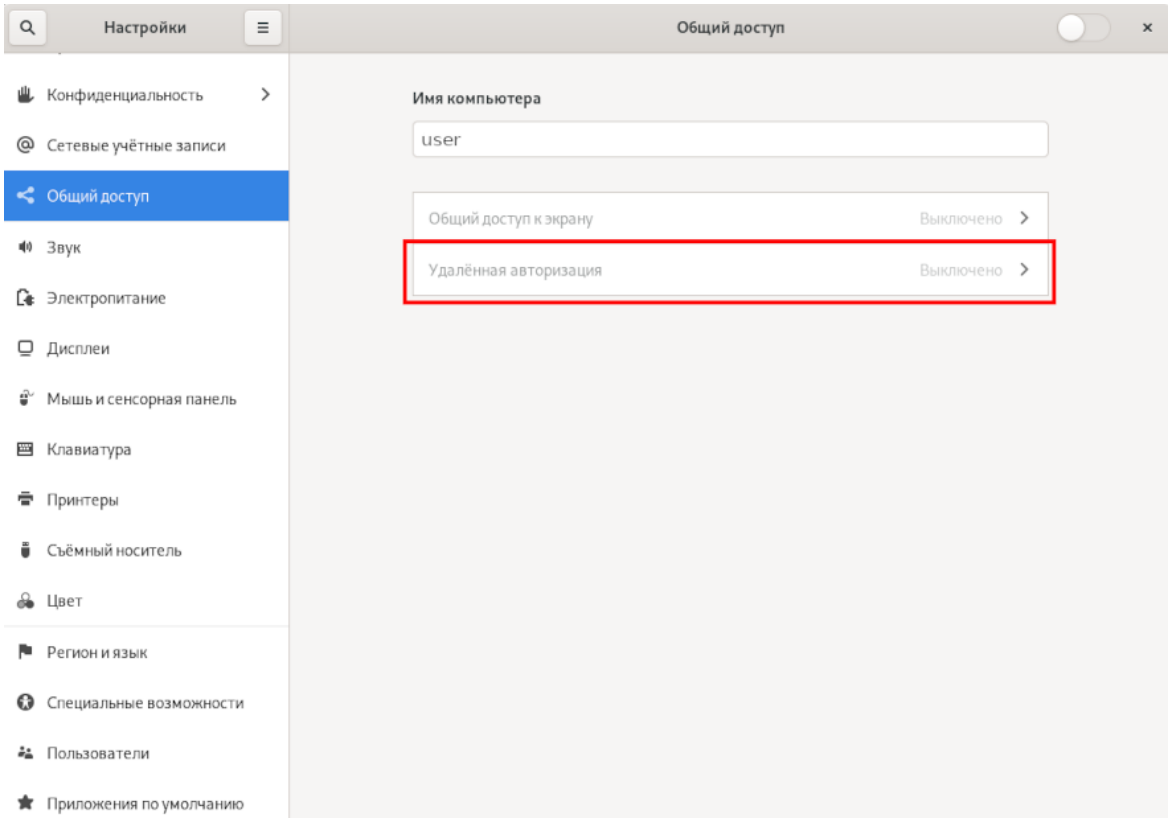

Рис. 44: Удалённая авторизация

3.17. Звук

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

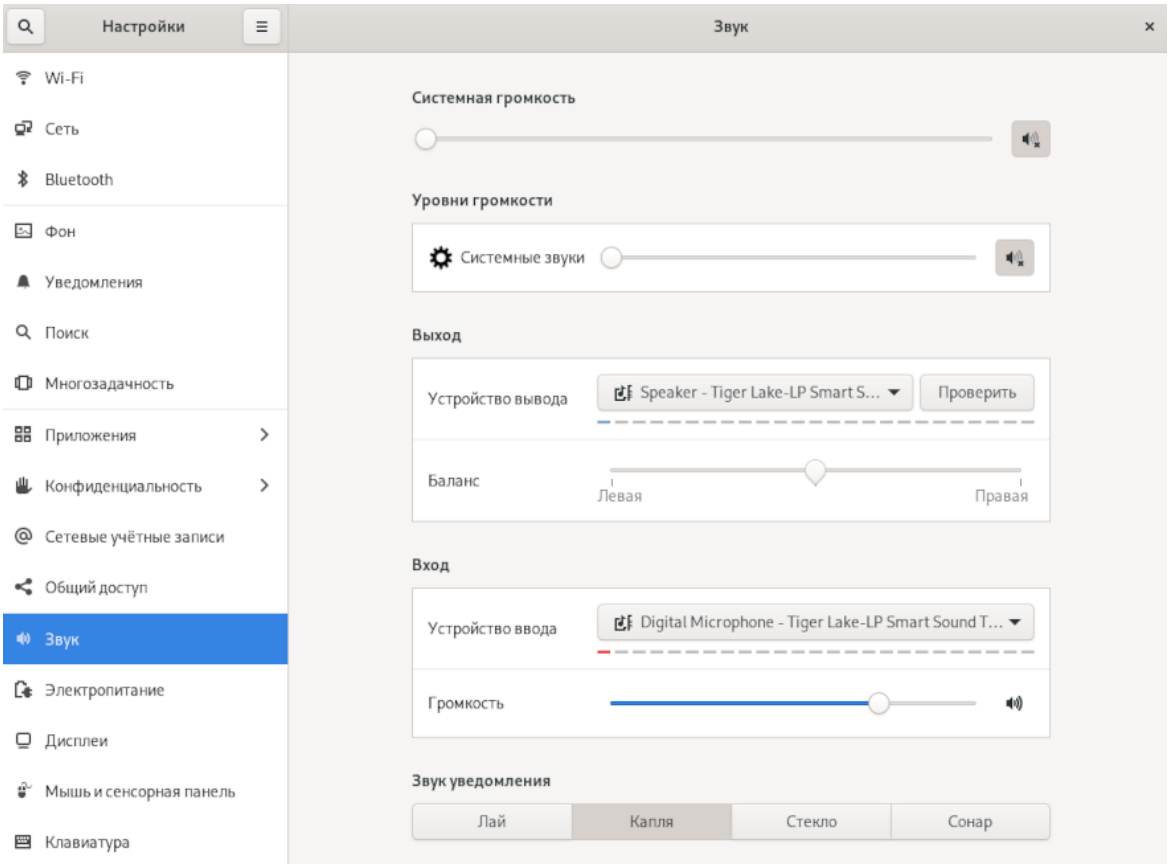

Рис. 45: Звук

3.18. Электропитание

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

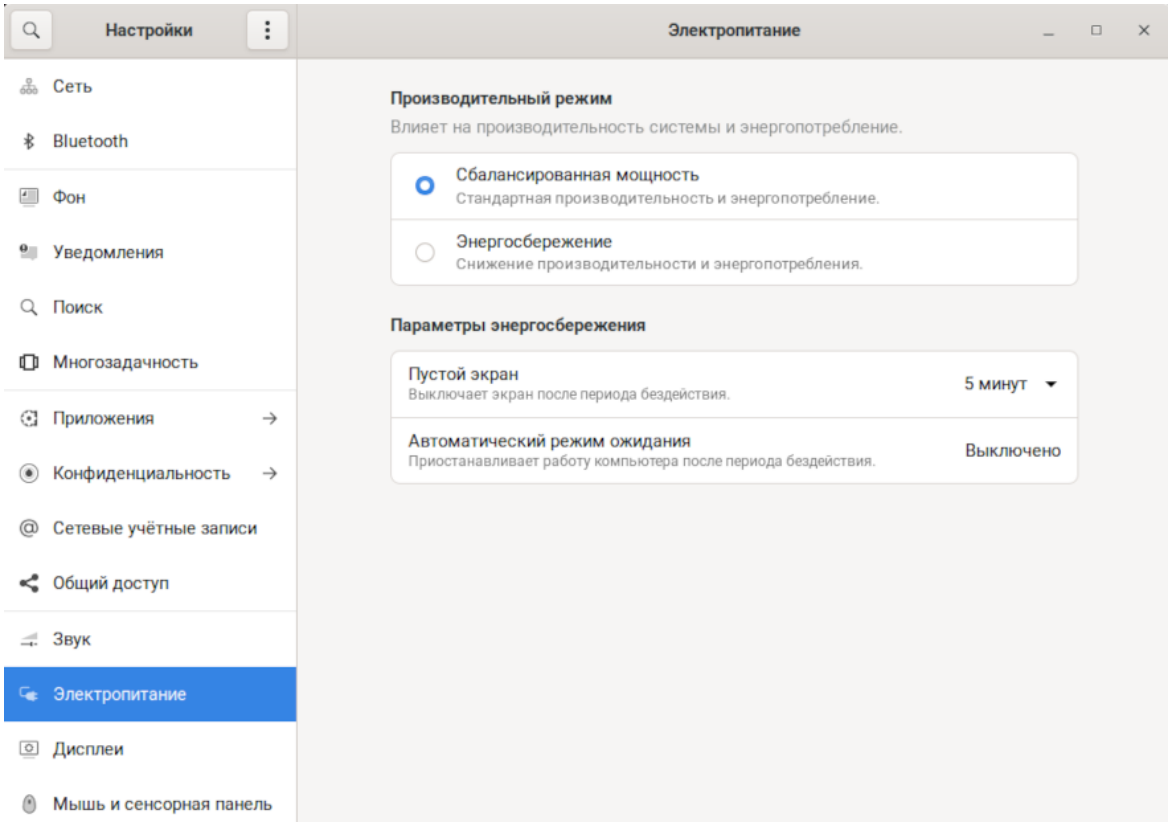

Рис. 46: Электропитание

3.19. Дисплеи

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

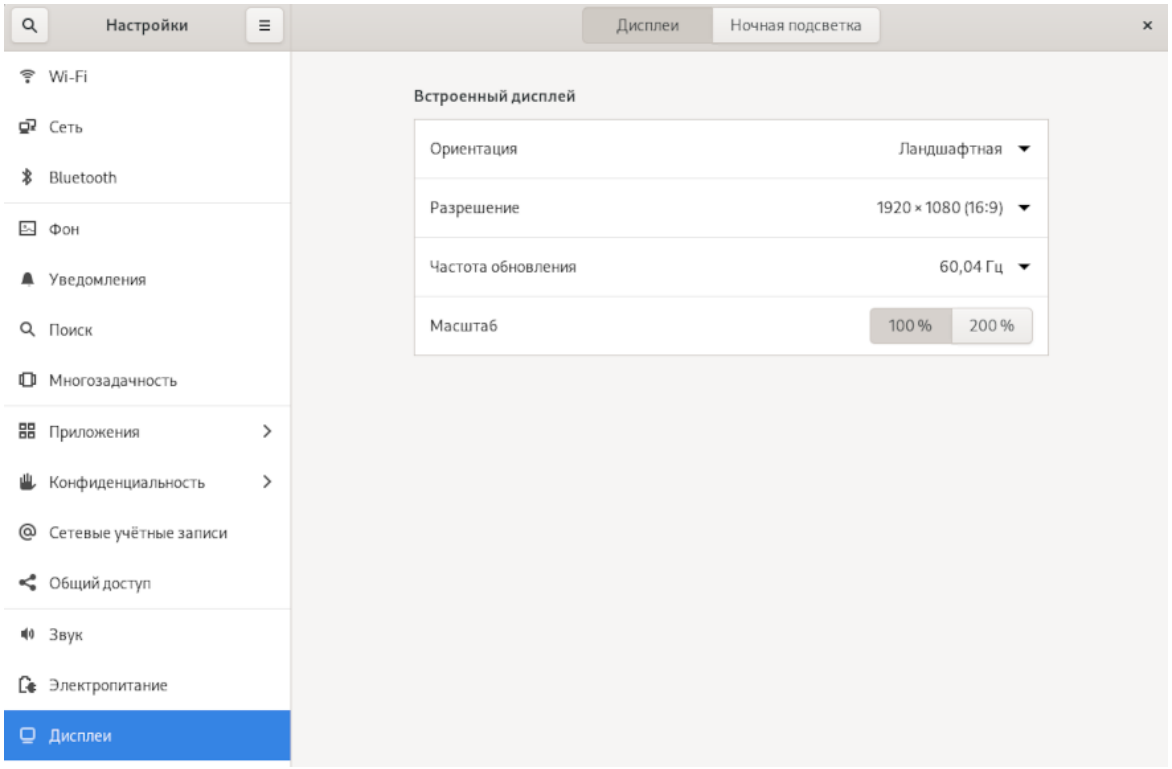

Рис. 47: Дисплеи

Ночная подсветка

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

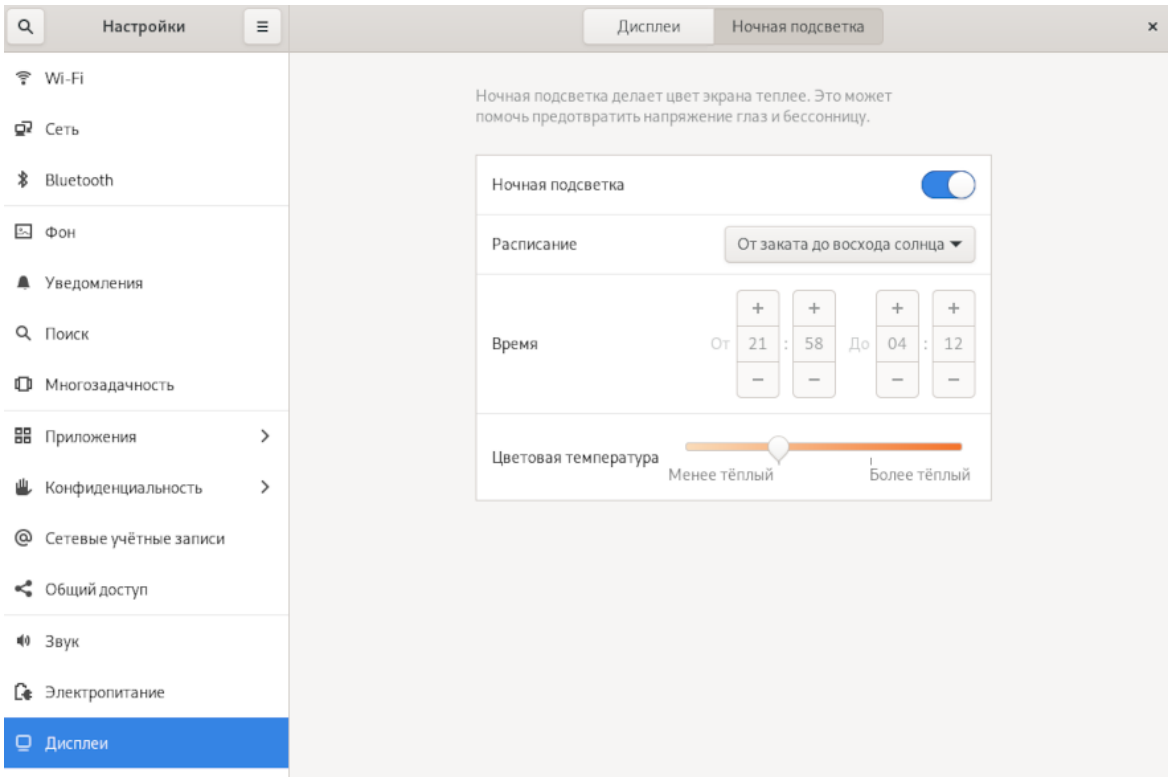

Рис. 48: Ночная подсветка

3.20. Мышь и сенсорная панель

Для просмотра и управления настройками мыши и сенсорной панели перейдите в «Настройки» → «Мышь и сенсорная панель». Нажмите на «Проверить параметры» для проверки работы мыши/сенсорной панели.

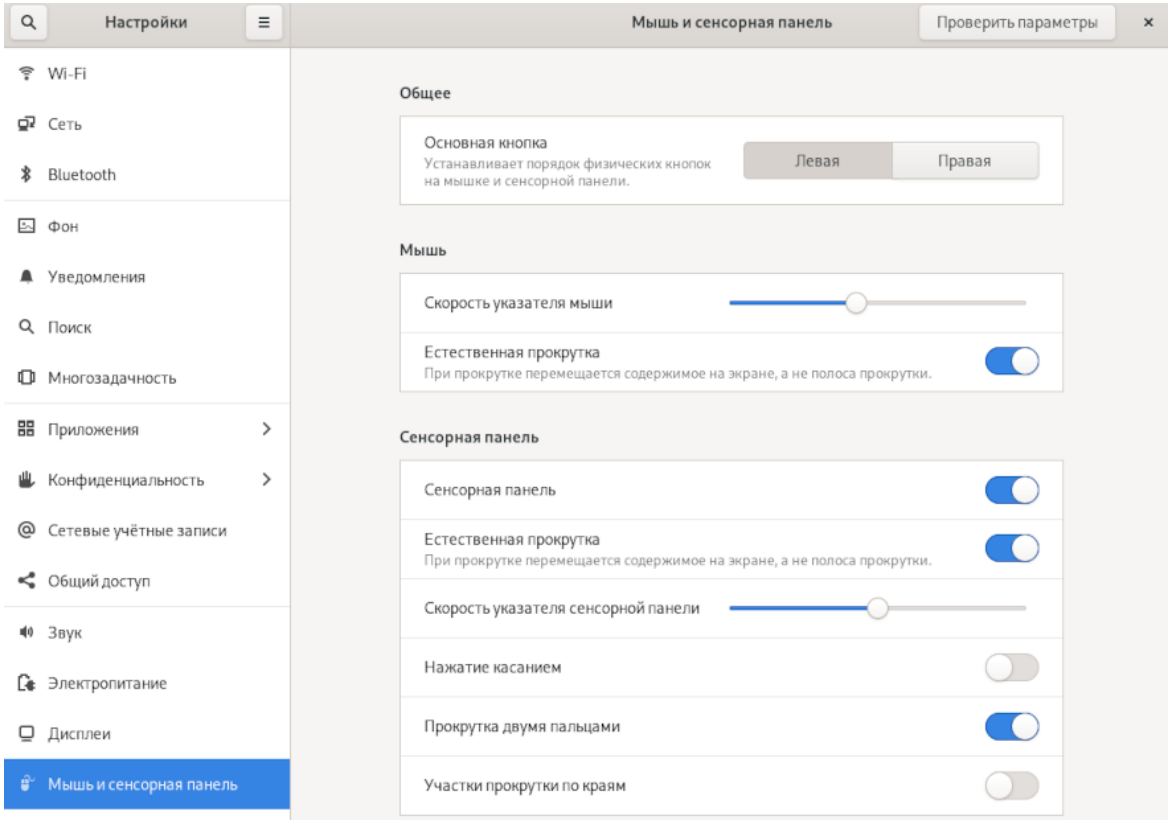

Рис. 49: Мышь и сенсорная панель

3.21. 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.

Ниже описан процесс настройки комбинации клавиш переключения языка ввода через приложение «Доп.настройки GNOME».

3.21.1. Приложение Доп.настройки GNOME

Приложение «Доп.настройки GNOME». позволяет визуально, легко и просто настроить параметры рабочего стола и управлять расширенными параметрами графической оболочки.

Запуск

Откройте меню «Приложения» и выберите приложение «Доп.настройки GNOME» (вы также можете воспользоваться поиском).

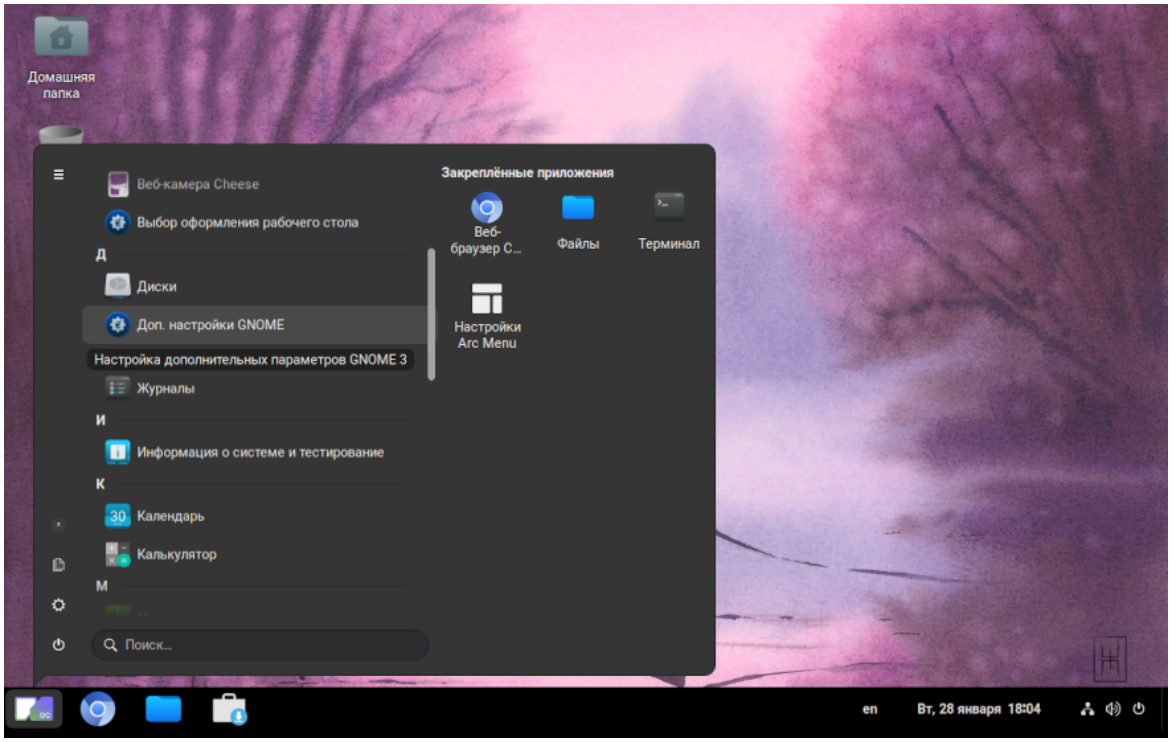

Рис. 50: Приложение «Доп.настройки GNOME»

При первом запуске приложение может выдать предупреждение.

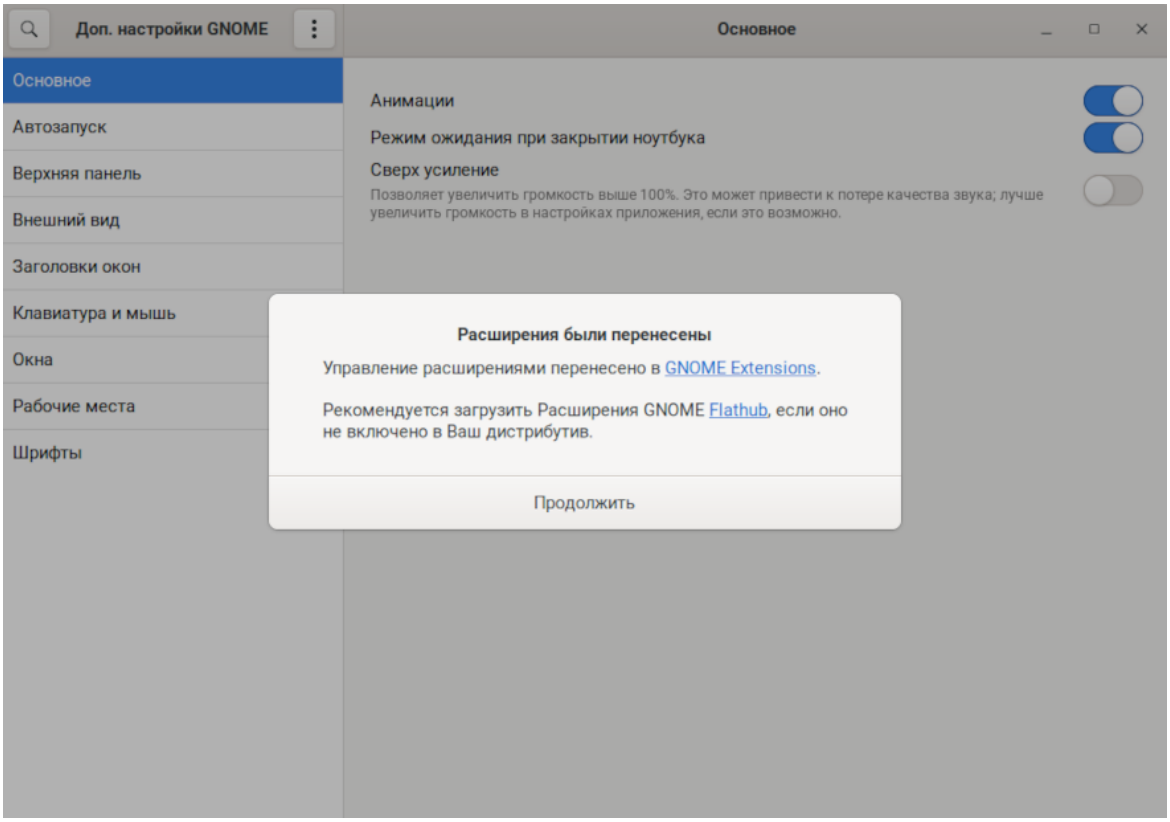

Рис. 51: Первый запуск «Доп.настройки GNOME»

Установка дополнительных пакетов или приложений не потребуется, просто нажмите «Продолжить» и приложение будет работать в обычном режиме.

Изменение клавиш переключения раскладки

Рассмотрим пример изменения клавиш переключения раскладки с помощью приложения «Доп.настройки GNOME».

1) Откройте приложение.
2) Перейдите во вкладку «Клавиатура и мышь».
3) Нажмите на кнопку «Дополнительные параметры раскладки».
4) Разверните список «Переключение на другую раскладку», выберите нужный вариант переключения.

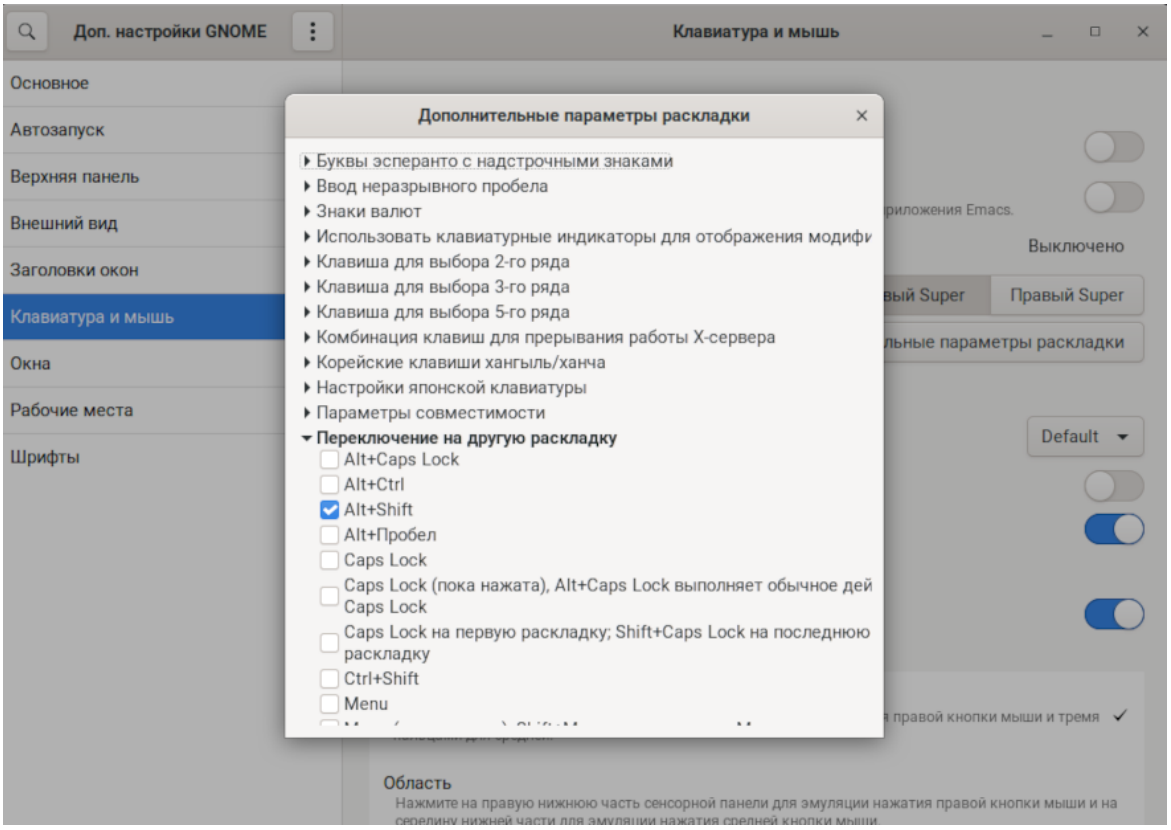

Рис. 52: Переключение на другую раскладку

5) Закройте окно «Дополнительные параметры раскладки». Теперь для переключения языка будет работать выбранная комбинация клавиш.

3.22. Принтеры

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

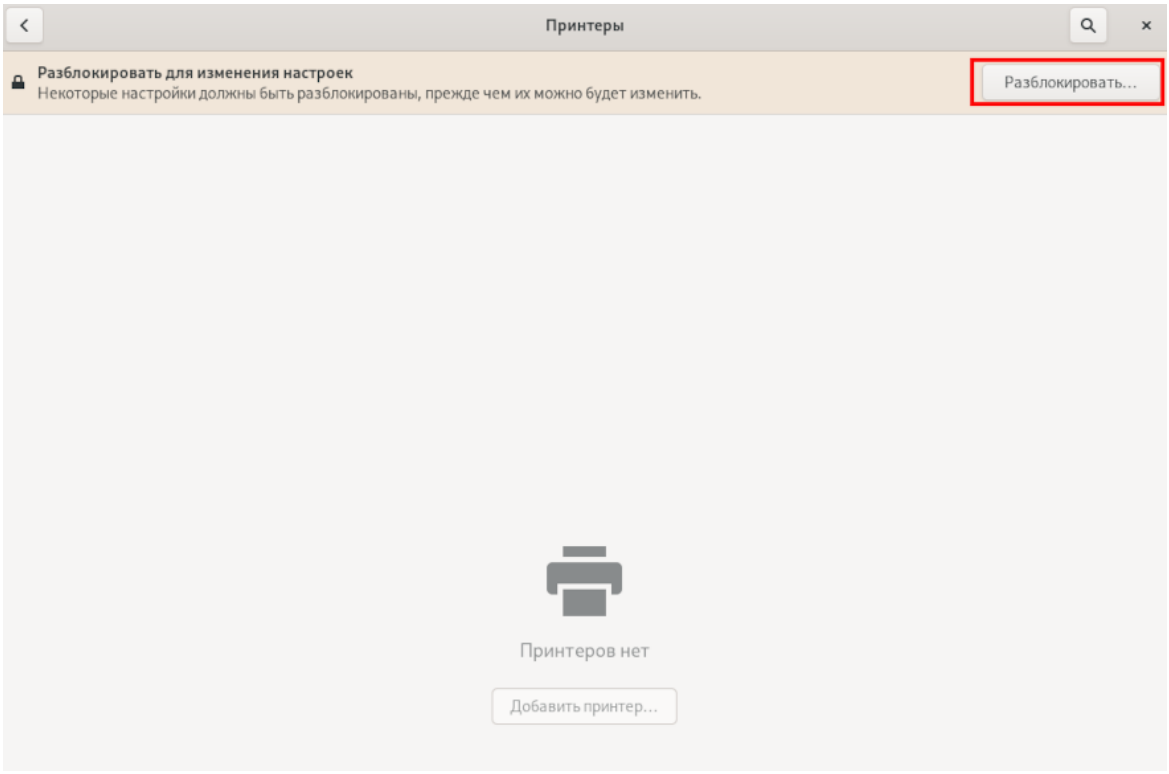

Рис. 53: Принтеры

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`.

3.23. Съёмный носитель

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

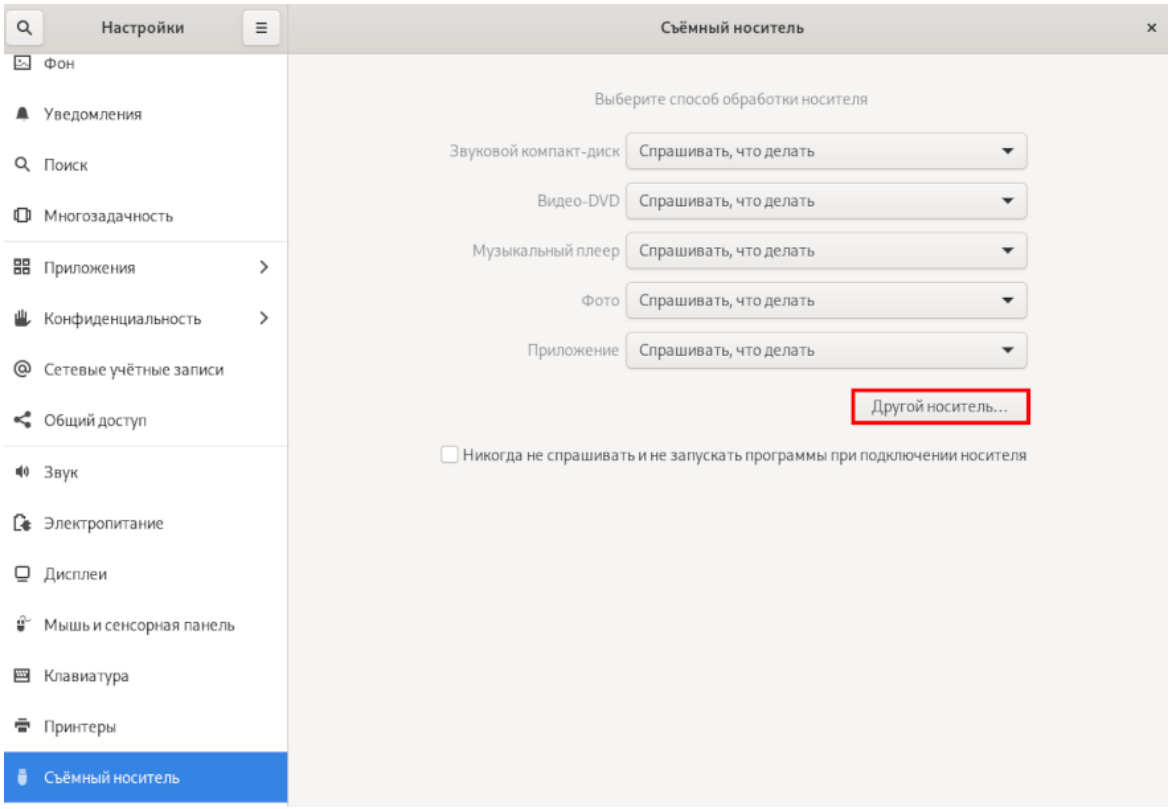

Рис. 54: Съёмный носитель

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

3.24. Цвет

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

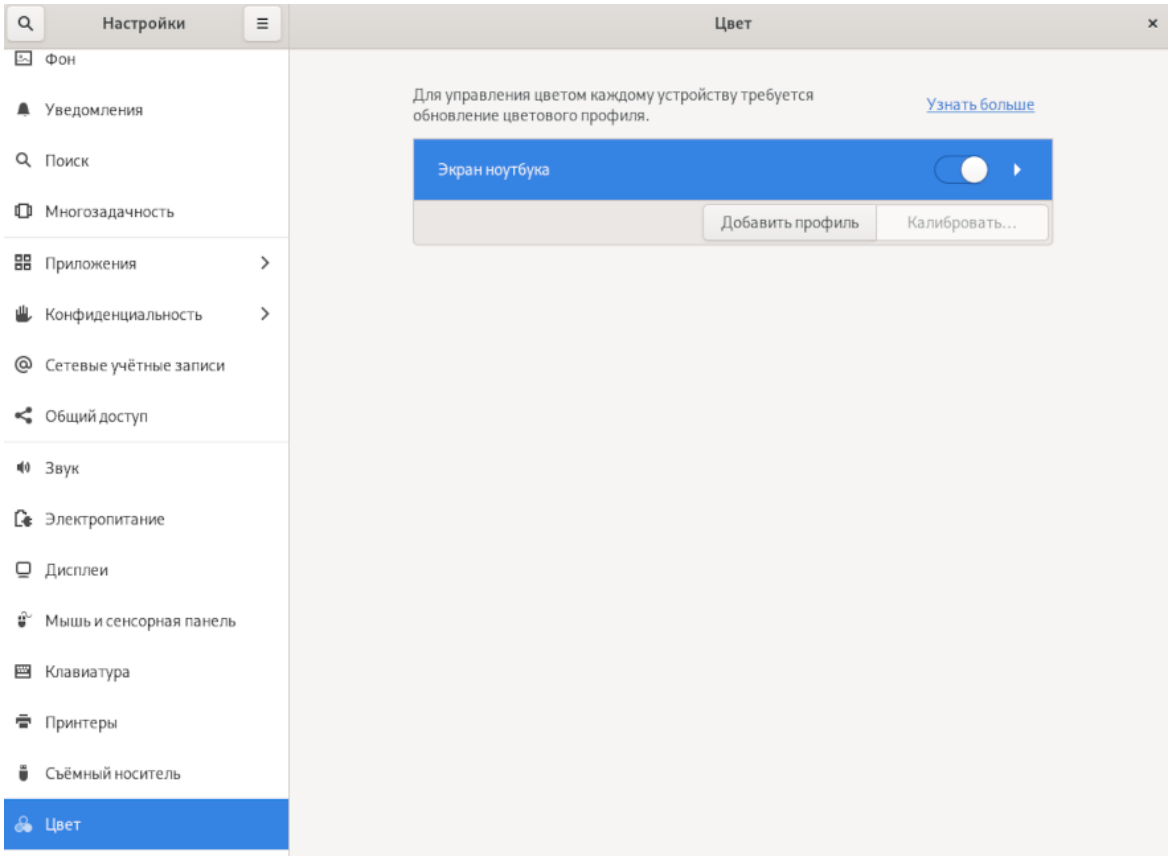

Рис. 55: Цвет

3.25. Регион и язык

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

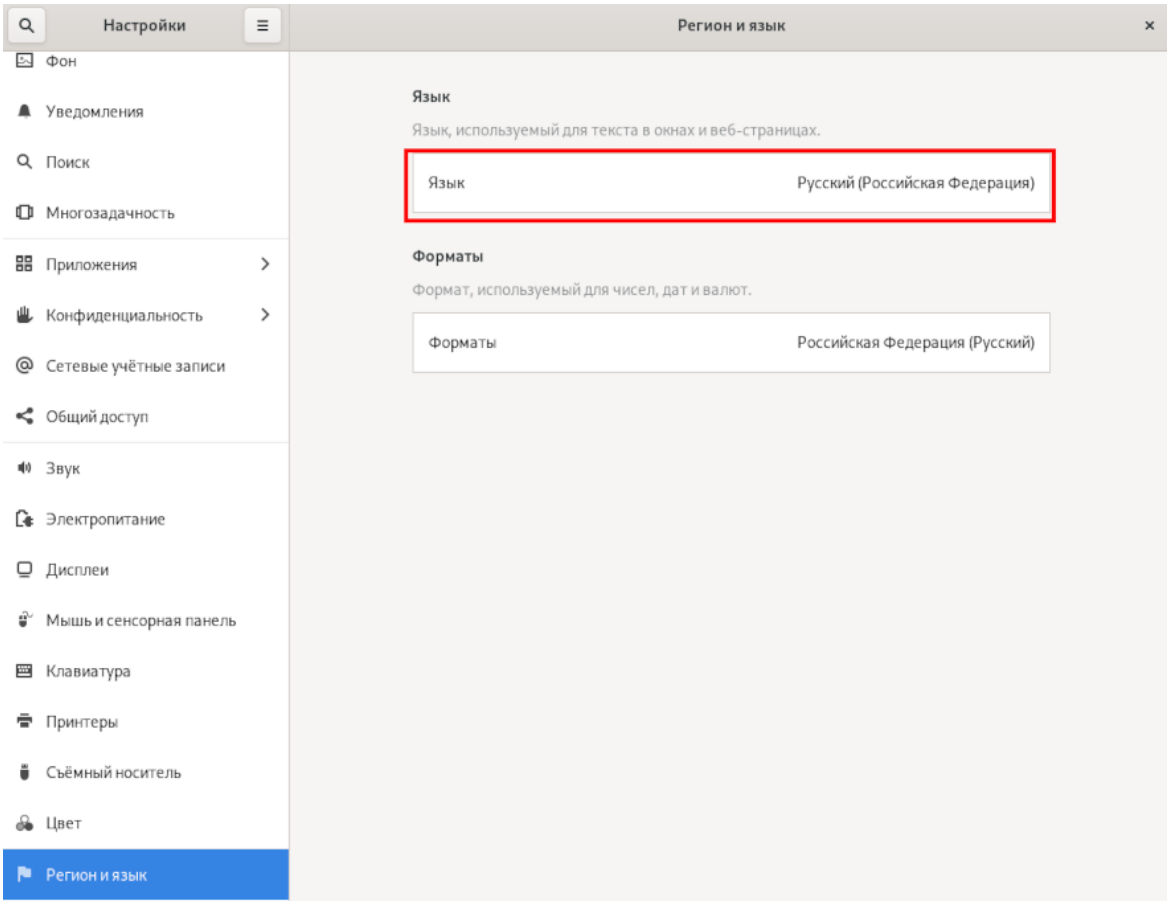

Рис. 56: Регион и язык

3.26. Специальные возможности

Для включения специальных возможностей перейдите в «Настройки» → «Специальные возможности».

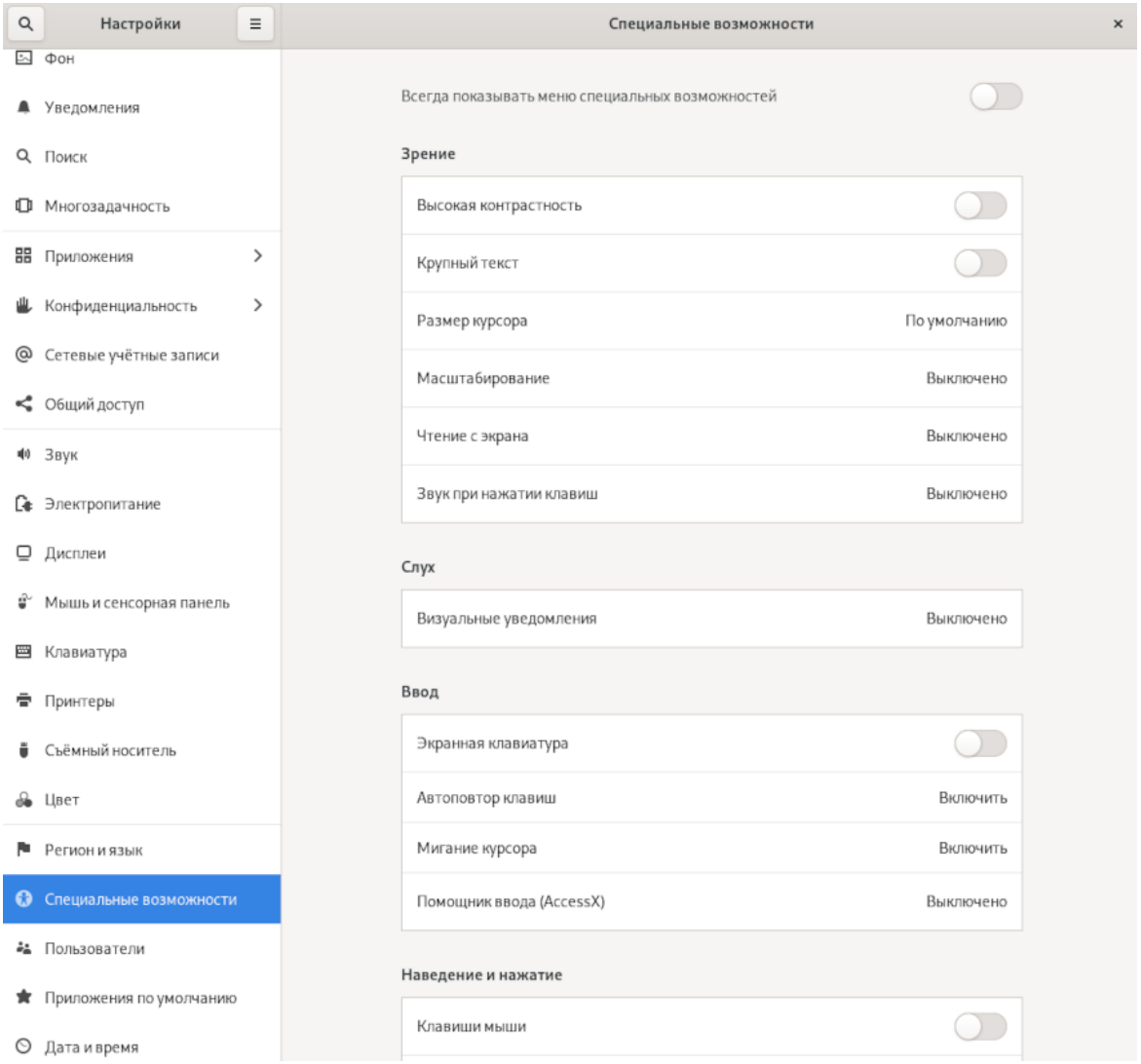

Рис. 57: Специальные возможности

3.27. Пользователи

Для изменения значений своего имени или пароля необходимо в системном меню выбрать «Настройки», в открывшемся окне выбрать «Пользователи».

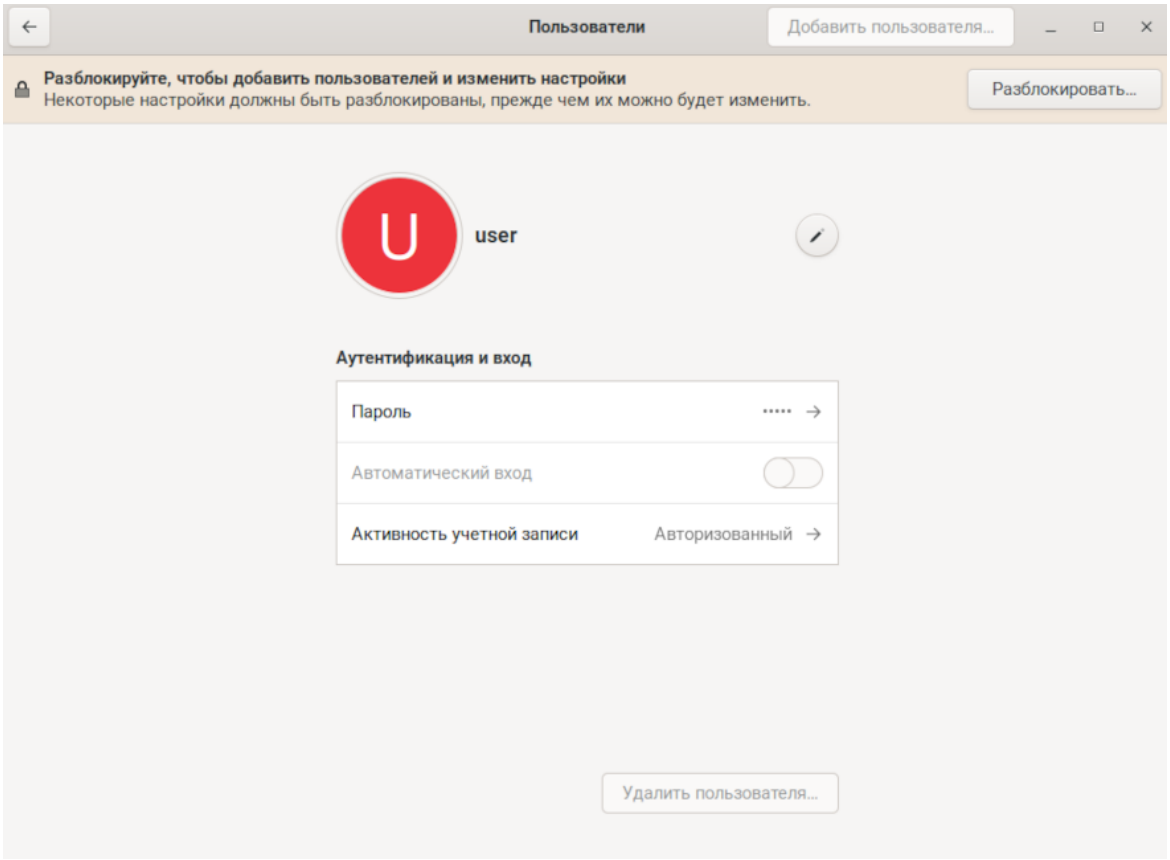

Рис. 58: Новое имя пользователя

Здесь можно задать новое значение своего имени пользователя. А также задать и подтвердить новое значение своего пароля, продемонстрировав предварительно знание текущего значения пароля.

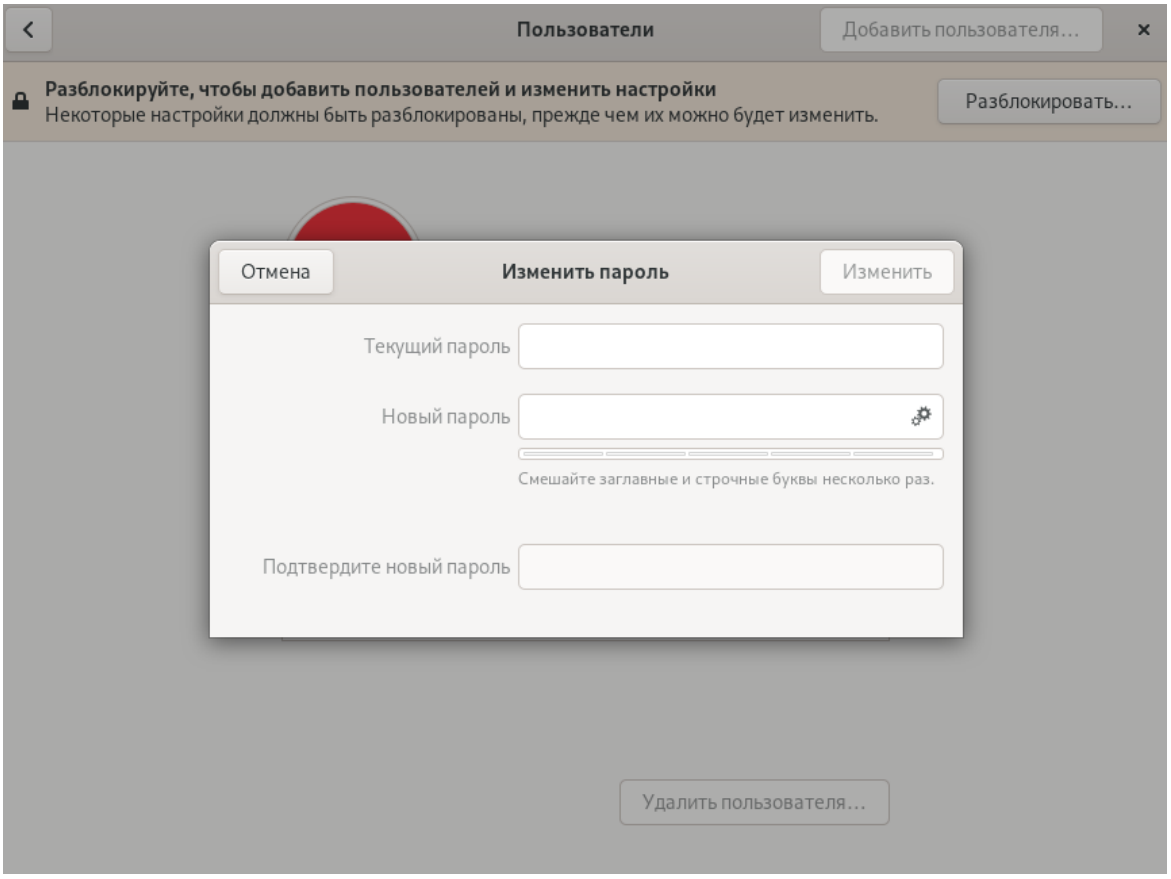

Рис. 59: Изменение пароля

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 на «Активность учётной записи». Появится журнал входа в систему с информацией о датах и времени начала и завершения сеансов работы.

3.28. Приложения по умолчанию

Для выбора приложений, которые открывают определённые типы файлов, перейдите в «Настройки» → «Приложения по умолчанию».

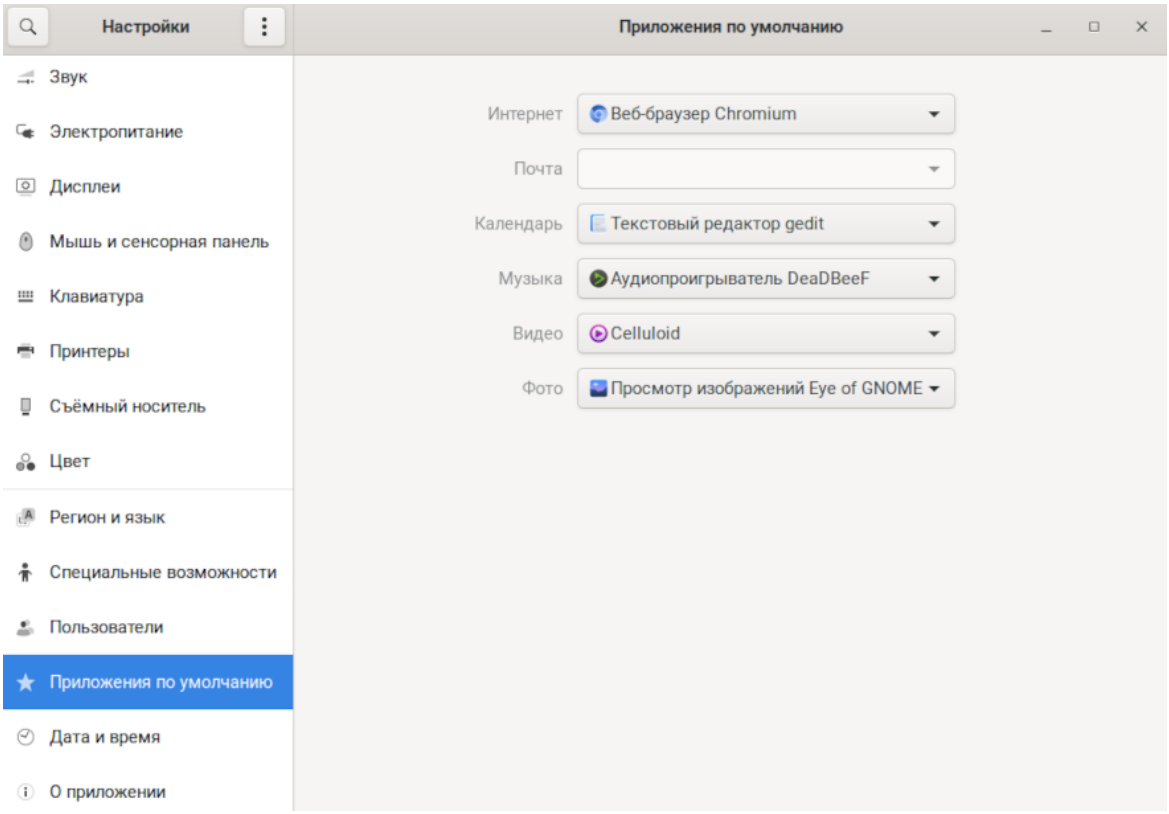

Рис. 60: Приложения по умолчанию

3.29. Дата и время

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

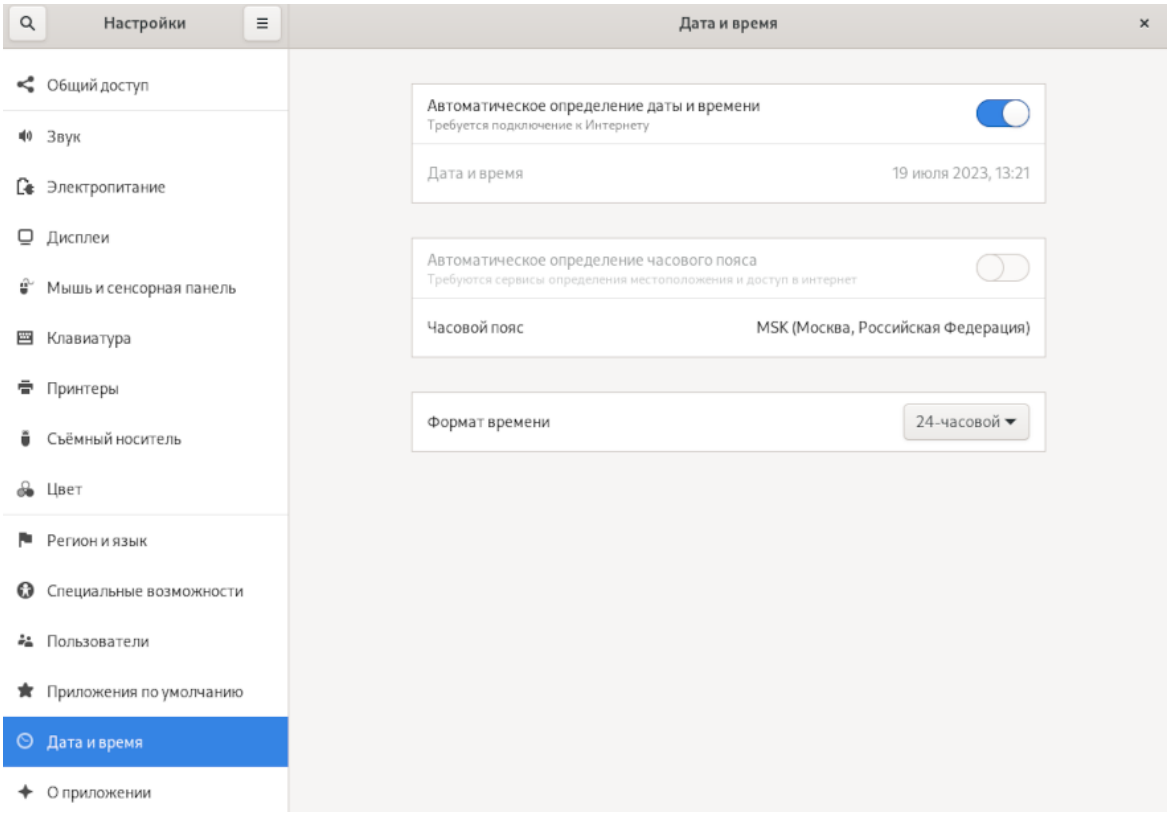

Рис. 61: Дата и время

3.30. О приложении

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

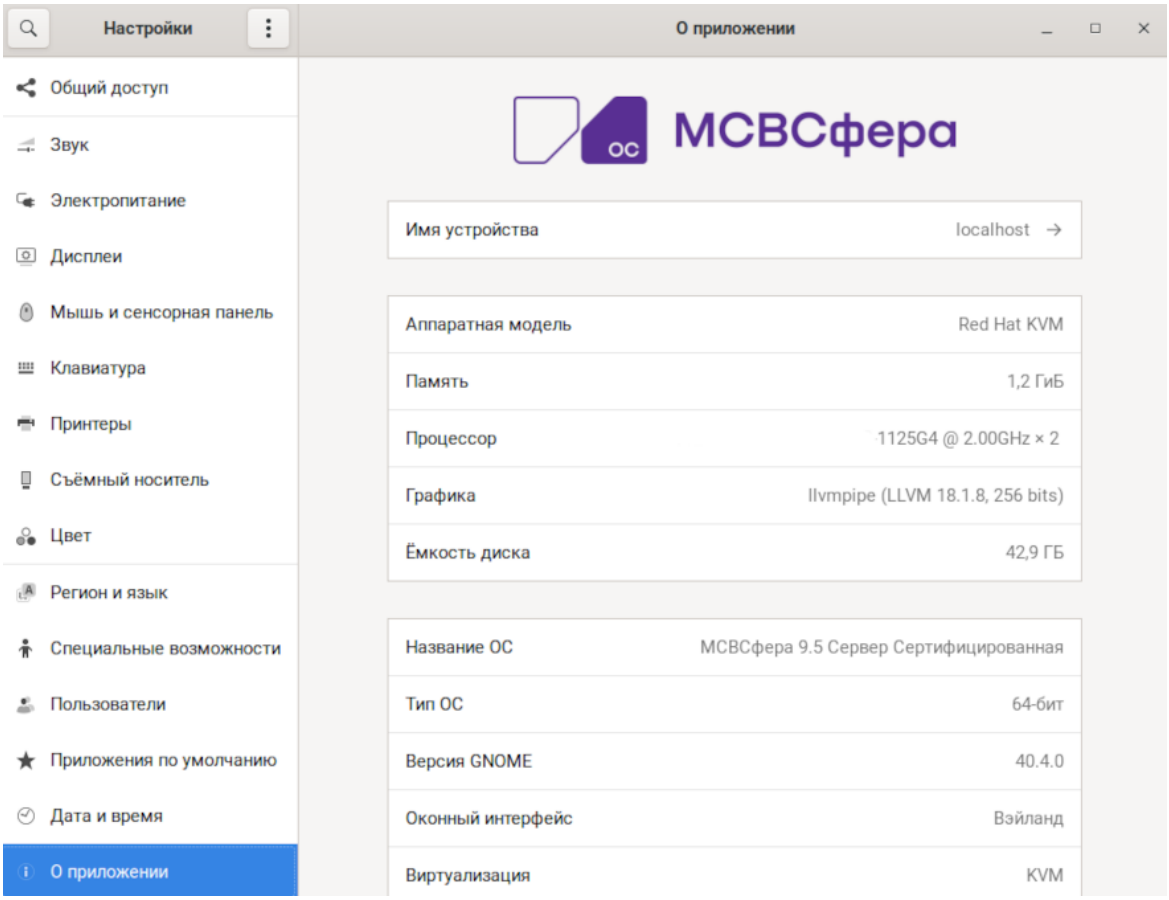

Рис. 62: О приложении

Для изменения имени устройства нажмите на «Имя устройства».

3.30.1. Изменение оконного интерфейса

По умолчанию в качестве оконного интерфейса используется Xorg (X11).

Если вы хотите использовать Wayland, то выполните следующие действия:

1) В файле `/etc/gdm/custom.conf` закомментируйте следующие строки:

```
WaylandEnable=false

DefaultSession=gnome-xorg.desktop
```

2) Перезапустите систему или выполните следующую команду:

```
$ sudo systemctl restart gdm
```

3) При логине в правом нижнем углу нажмите на значок шестерёнки и выберите сеанс «GNOME на Wayland».

Рис. 63: Сеанс GNOME на Wayland

3.30.2. Проверка и загрузка обновлений

Для проверки доступных обновлений нажмите на «Обновление ПО», вы будете перенаправлены в «*5. ЦЕНТР ПРИЛОЖЕНИЙ*».

3.31. Права доступа к папкам и файлам

Для просмотра и определения свойств папки и прав доступа к ней необходимо её выбрать, нажать правую кнопку мыши и в появившемся списке выбрать «Свойства», затем открыть вкладку «Права».

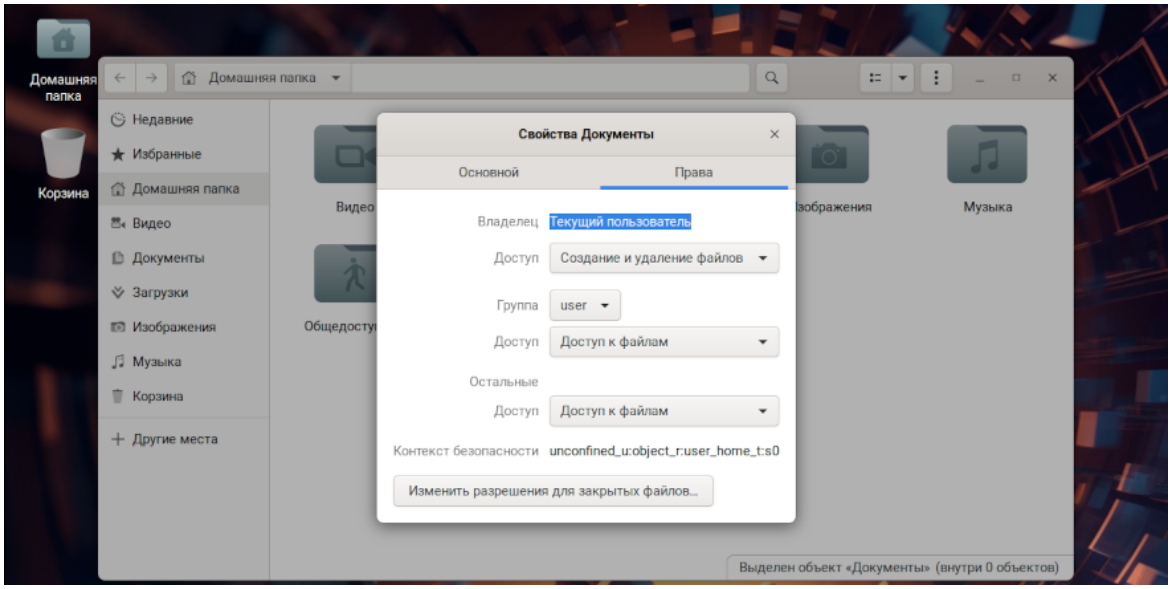

Рис. 64: Права доступа к папкам

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.

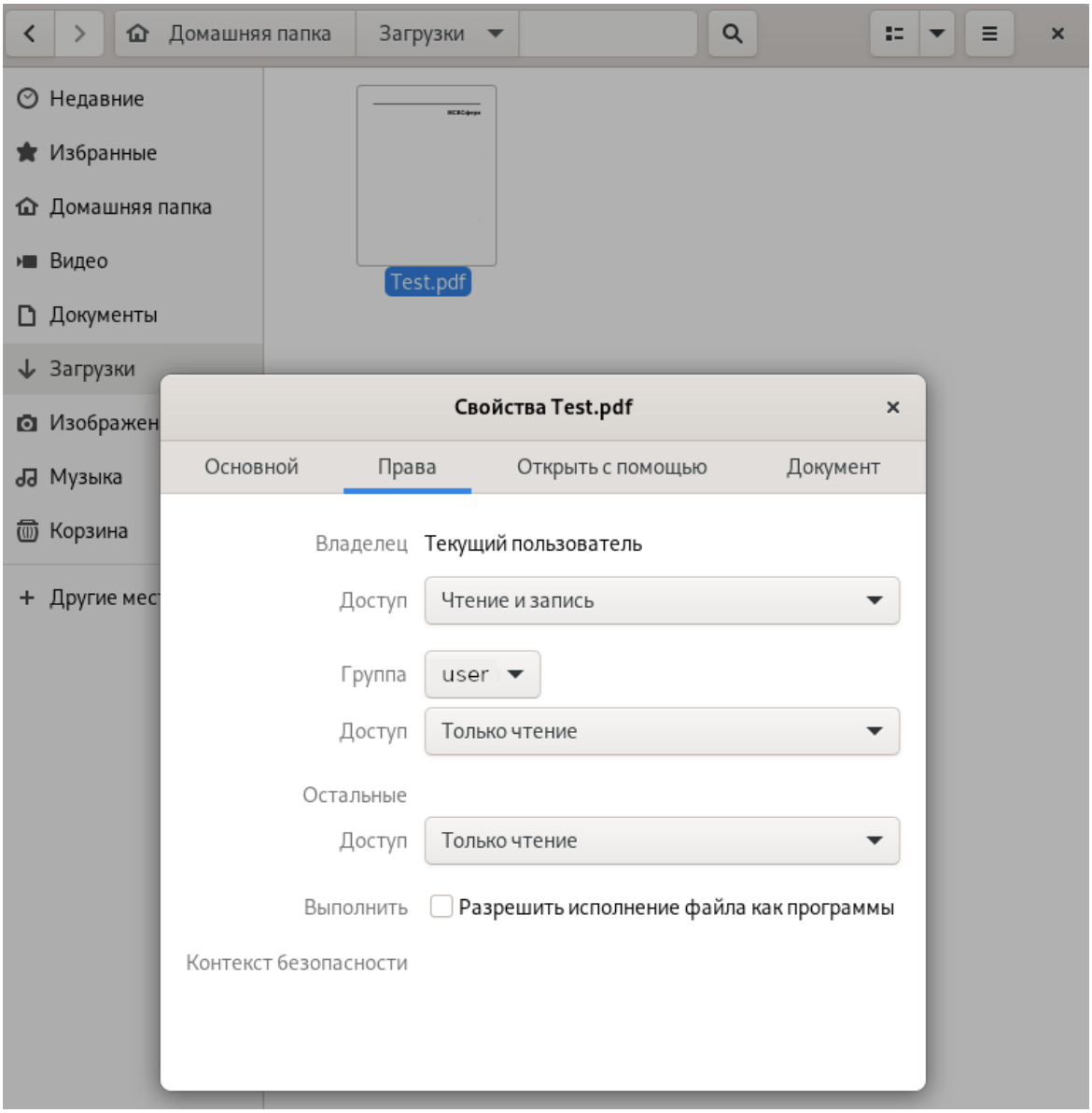

Рис. 65: Права доступа к файлам

4. ПРИЛОЖЕНИЯ

В меню «Приложения» добавляются все приложения, установленные на устройстве.

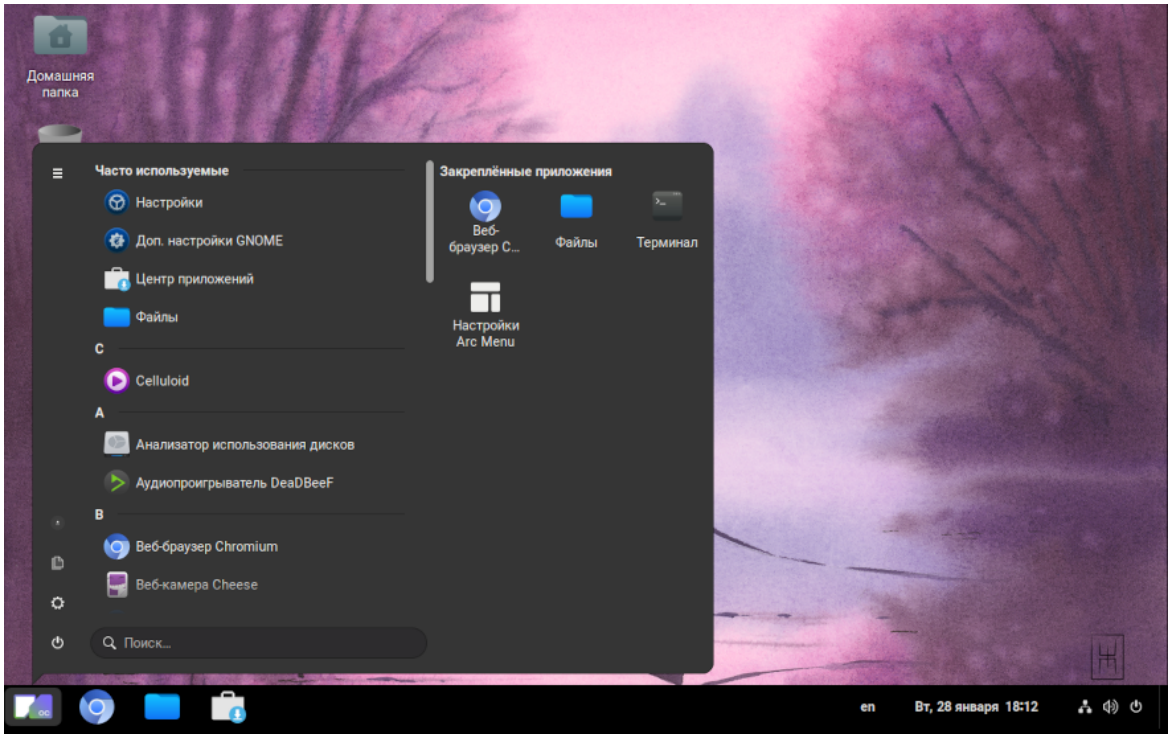

Рис. 66: Меню «Приложения»

Ниже показано как добавить приложение в «Избранное».

4.1. Добавление в «Избранное»

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

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

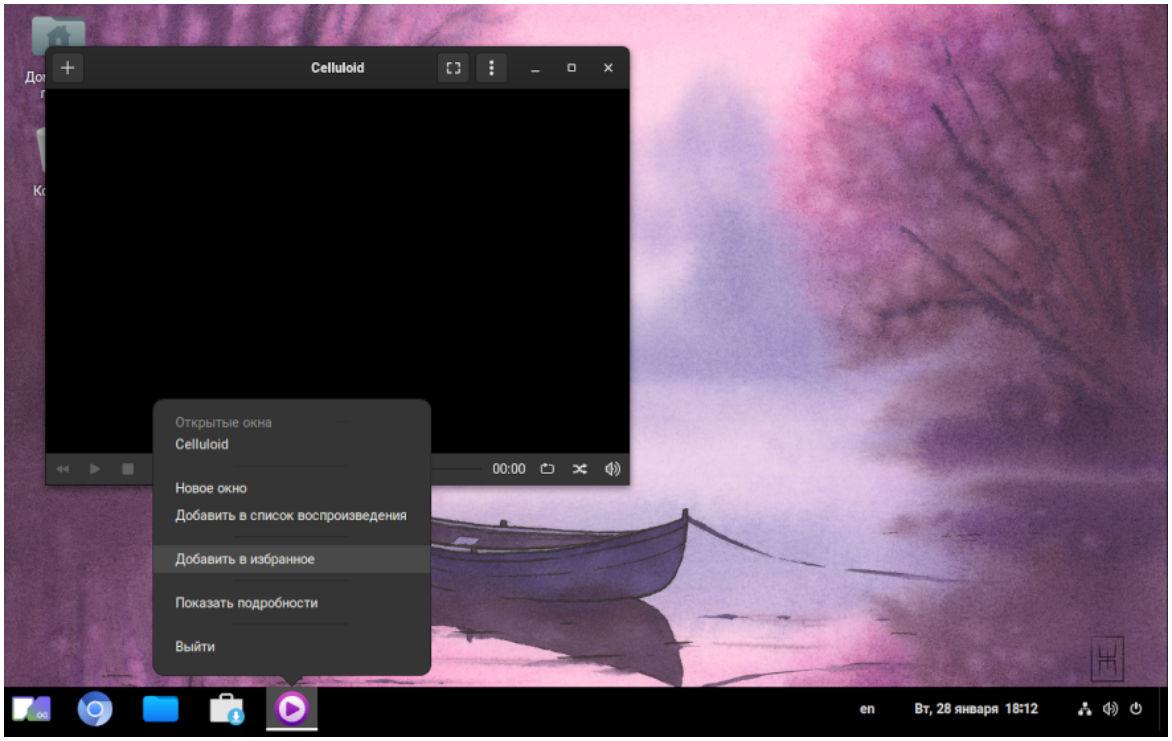

Рис. 67: Добавить в «Избранное»

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

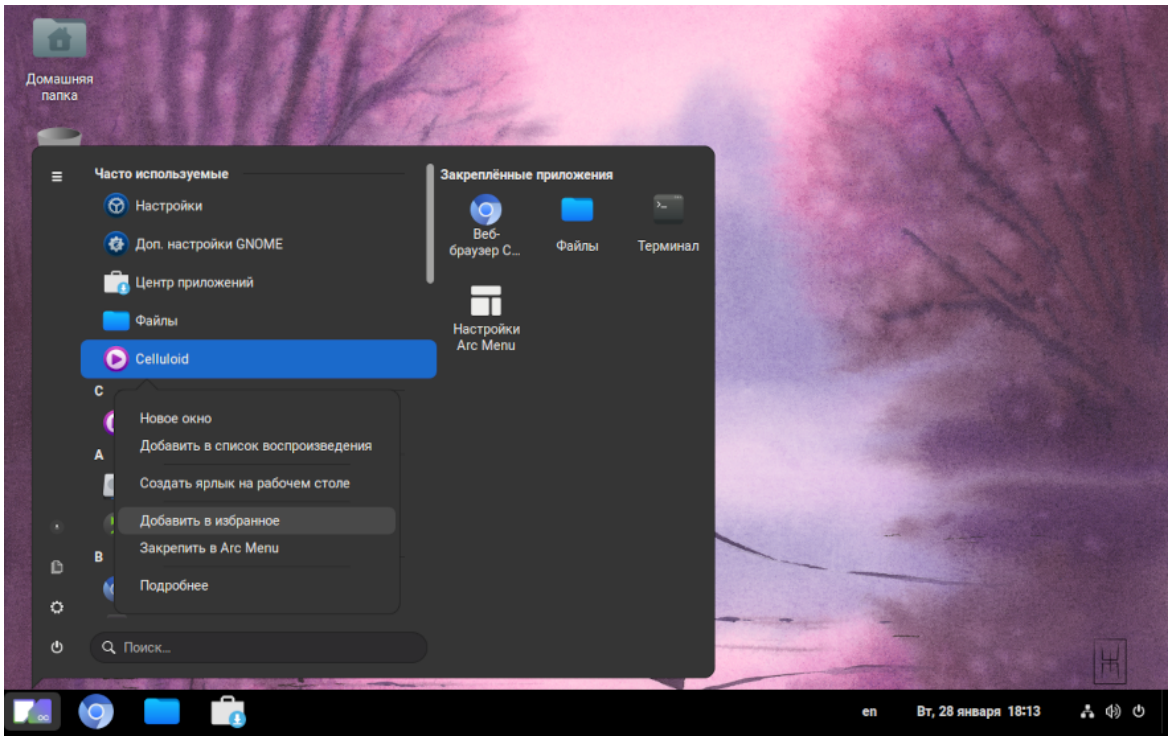

Рис. 68: Добавить в «Избранное»

4.2. Добавление в ArcMenu

Вы также можете закрепить приложение в ArcMenu, в этом случае при открытии меню «Приложения» закреплённые приложения отображаются в правой части меню.

Чтобы закрепить или открепить приложение из ArcMenu, нажмите на значок приложения в списке задач или в меню, а затем выберите «Закрепить в ArcMenu»/ «Открепить из ArcMenu».

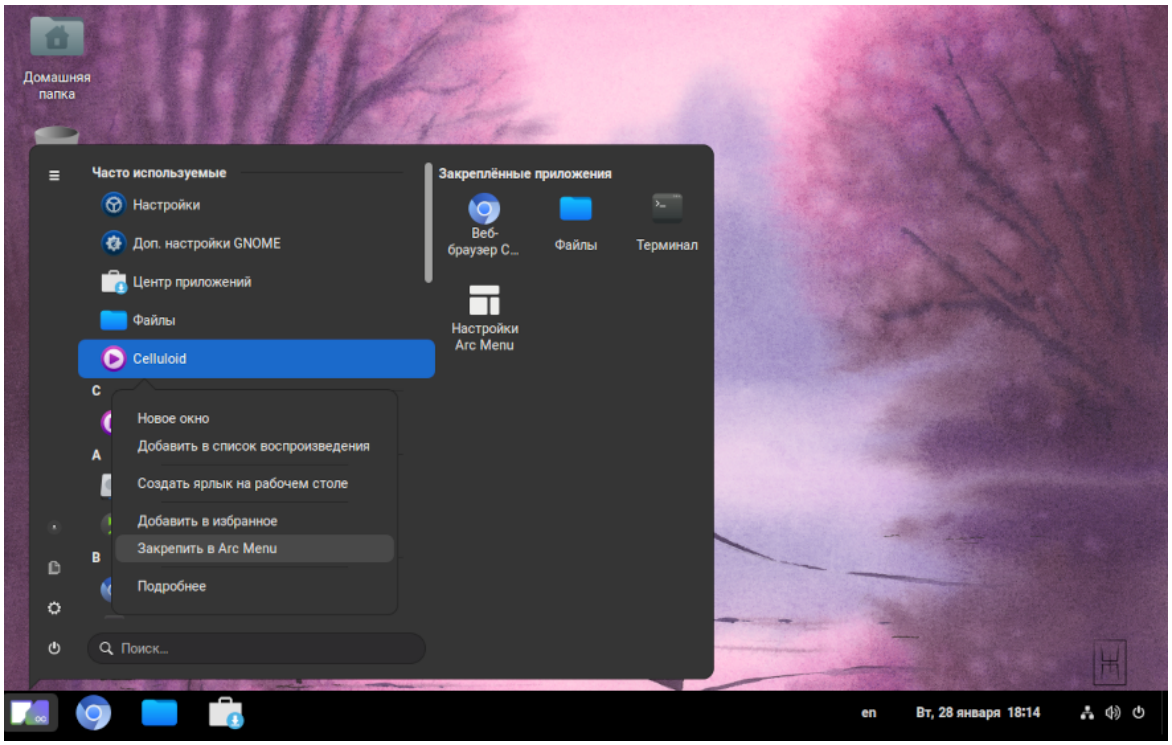

Рис. 69: Закрепить в ArcMenu

5. ЦЕНТР ПРИЛОЖЕНИЙ

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

Для запуска «Центра приложений» нажмите на его значок:

Рис. 70: Значок «Центр приложений»

5.1. Управление приложениями

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

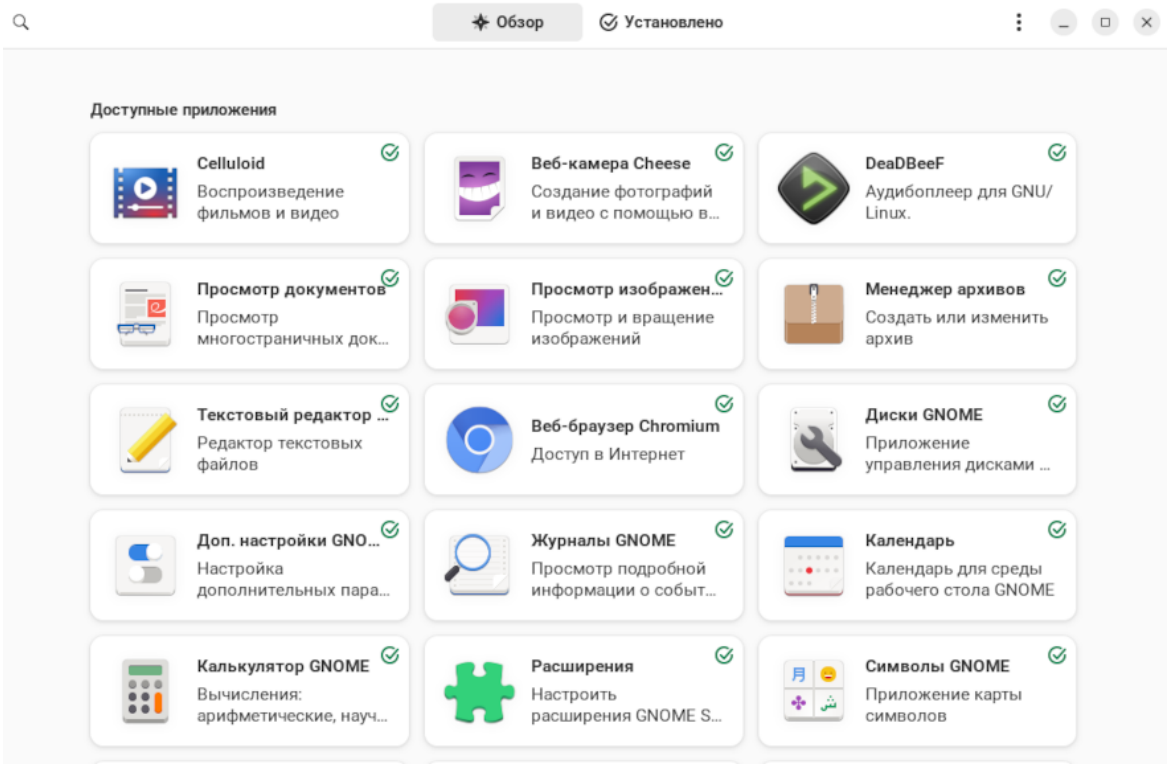

Рис. 71: Центр приложений

Для просмотра информации о приложении нажмите на него.

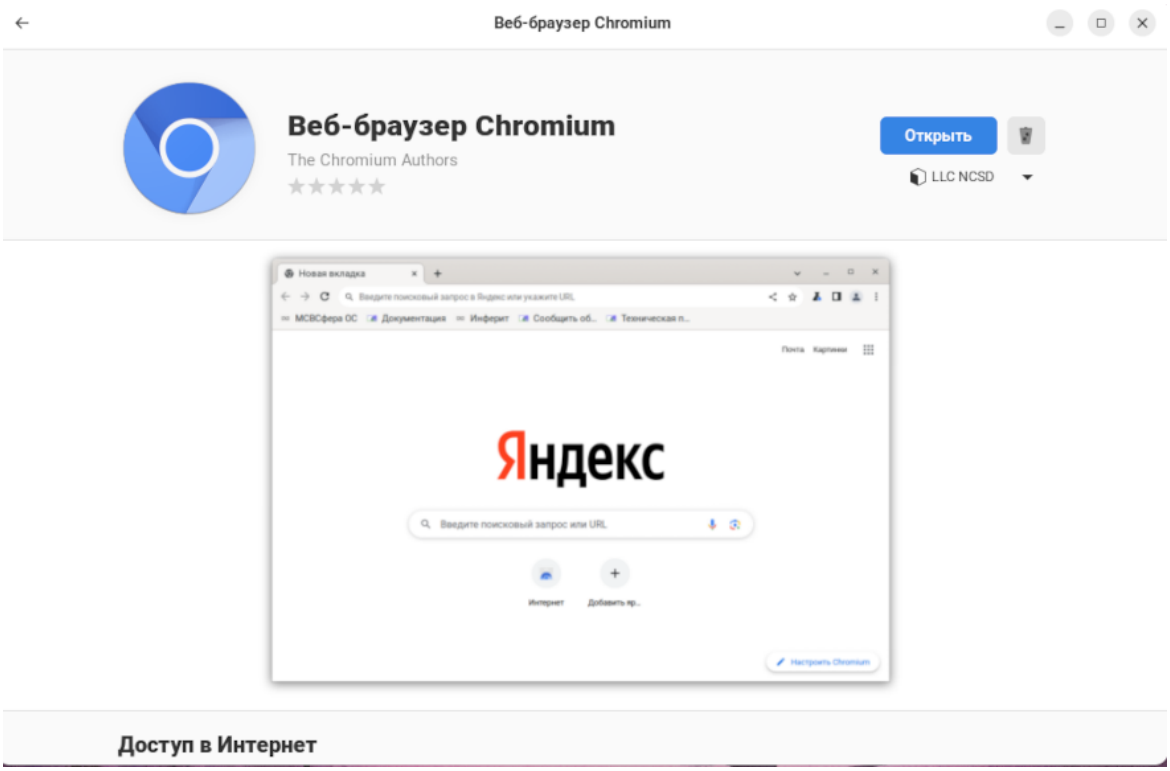

Рис. 72: Информация о приложении

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

5.1.1. Поиск приложения

Для поиска приложения нажмите на значок «Поиск», затем укажите название приложения или ключевые слова, описывающие, что должно делать приложение.

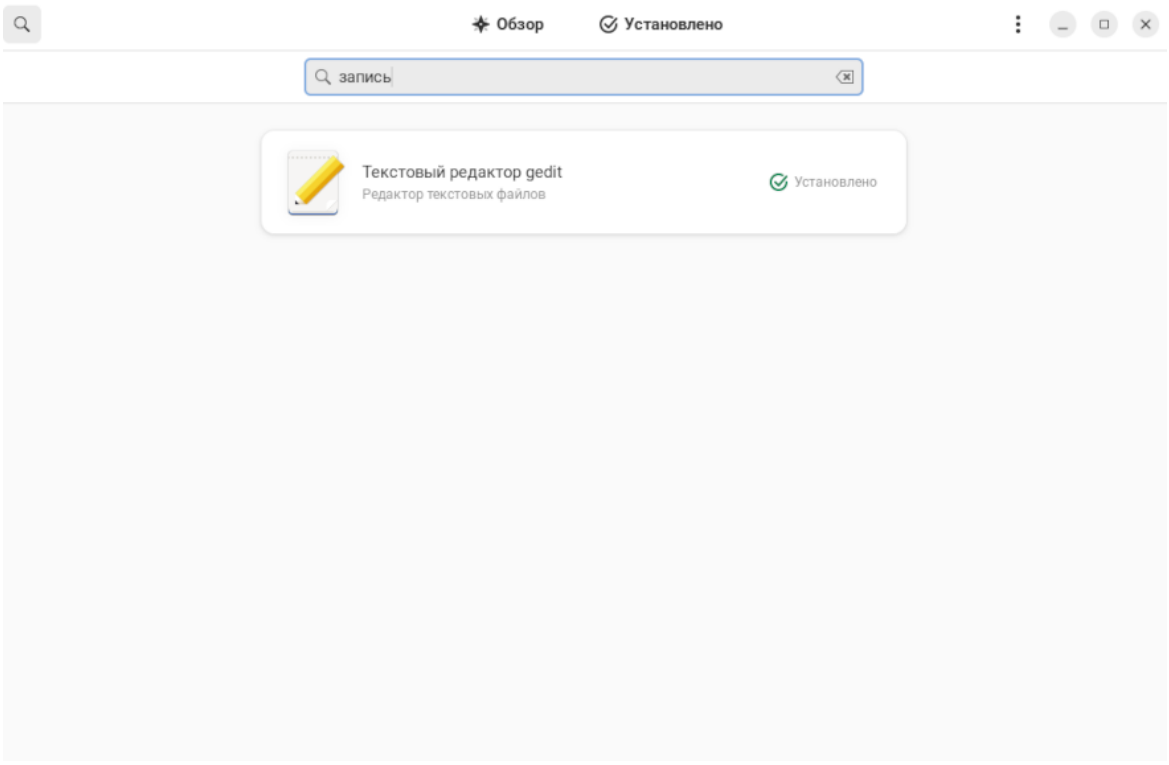

Рис. 73: Поиск приложения по ключевым словам

5.1.2. Просмотр списка установленных приложений

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

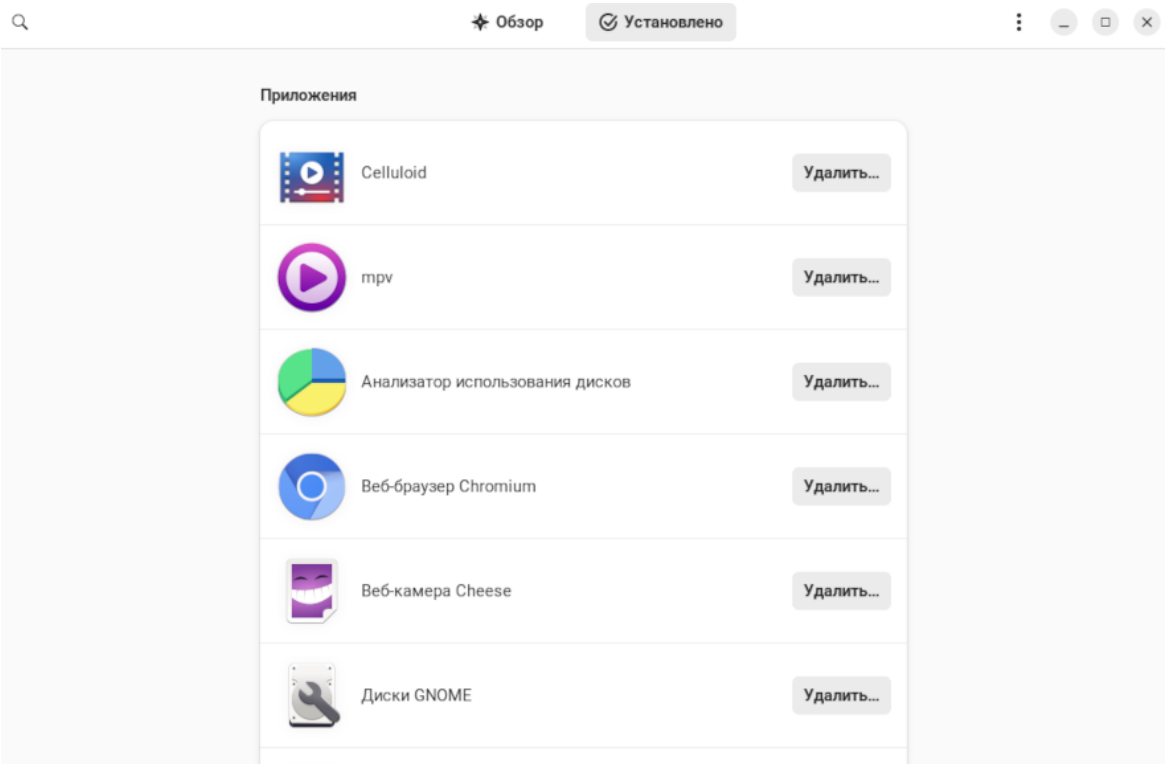

Рис. 74: Установленные приложения

5.2. 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 репозиториев.

5.2.1. Включение и выключение репозиториев

Для управления репозиториями перейдите в «Главное меню» (нажмите на значок «три точки») в правом верхнем углу, находясь в любой вкладке и выберите «Репозитории ПО».

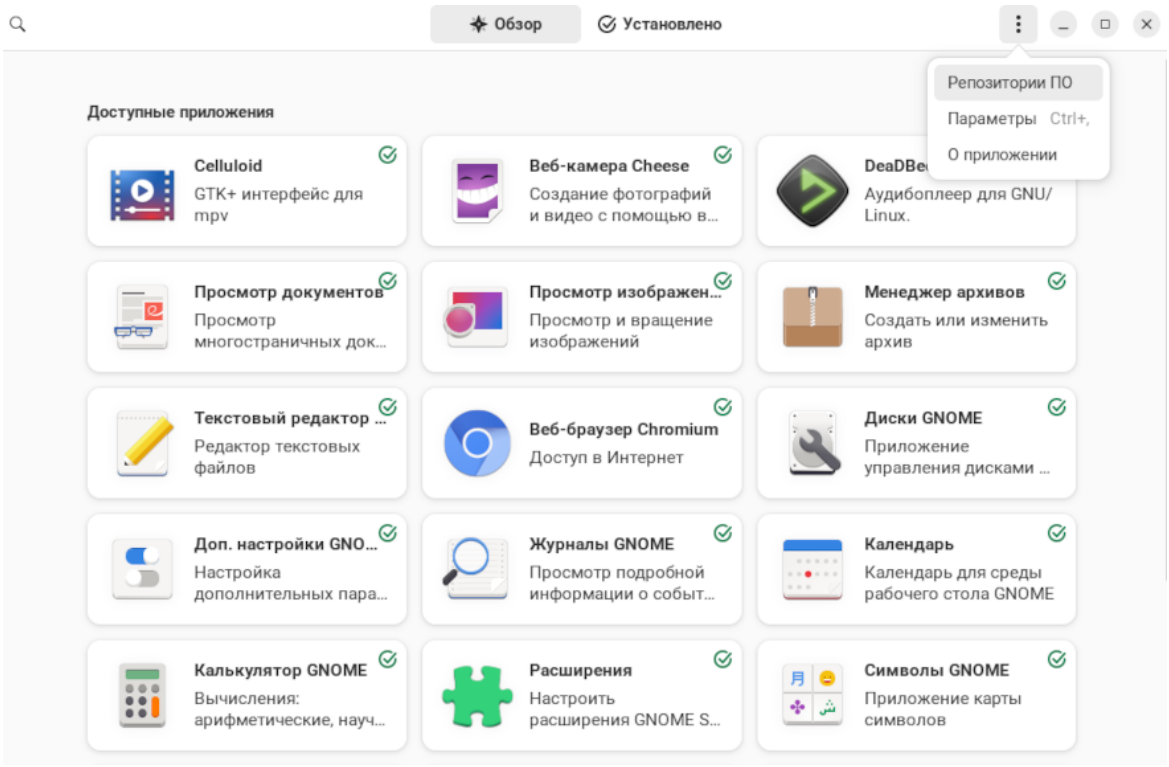

Рис. 75: «Репозитории ПО»

По умолчанию подключены только необходимые репозитории. Для включения репозитория передвиньте ползунок в активное состояние и выполните аутентификацию. Для отключения репозитория также необходимо выполнить аутентификацию.

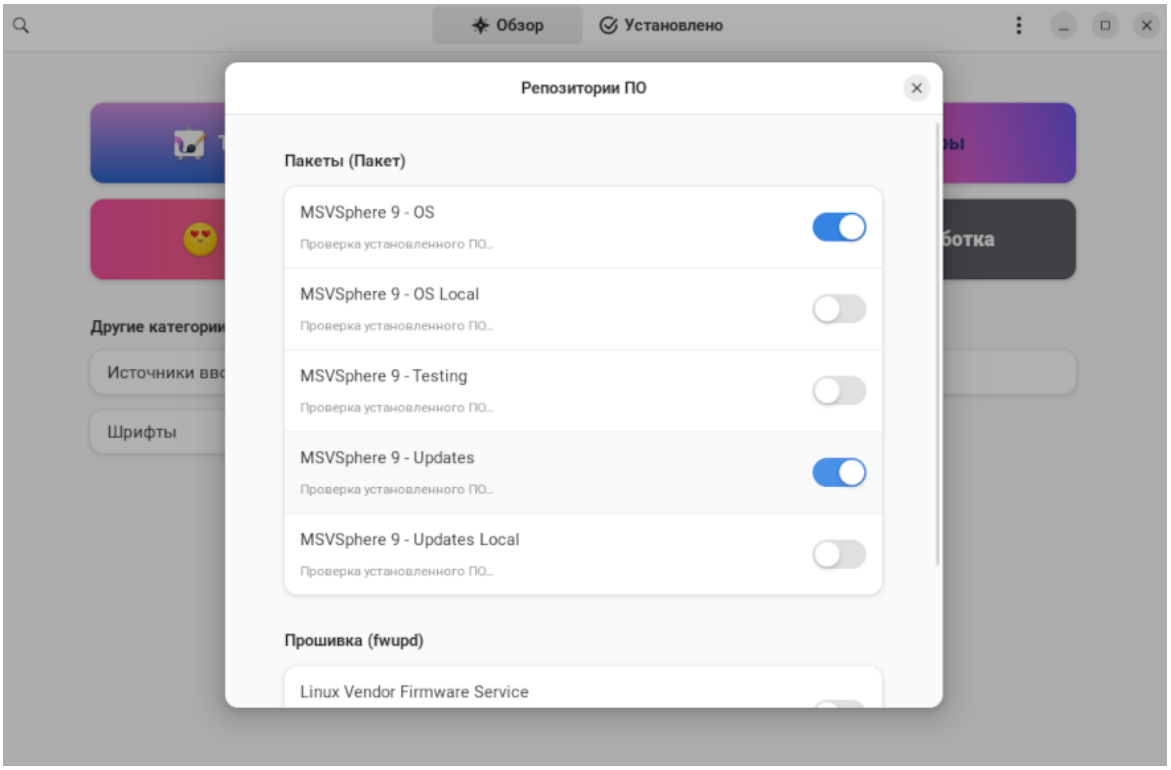

Рис. 76: «Репозитории ПО»

Примечание

Обратите внимание, что для включения обновлений, выпущенных для исправления уязвимостей или ошибок, должен быть включён репозиторий **Updates**. Для выполнения этих действий требуются права администратора!

5.2.2. Включение и выключение автоматических обновлений и уведомлений о новых версиях ПО

Для управления уведомлениями перейдите в «Главное меню» (нажмите на значок «три точки») в правом верхнем углу, находясь в любой вкладке, и выберите «Параметры».

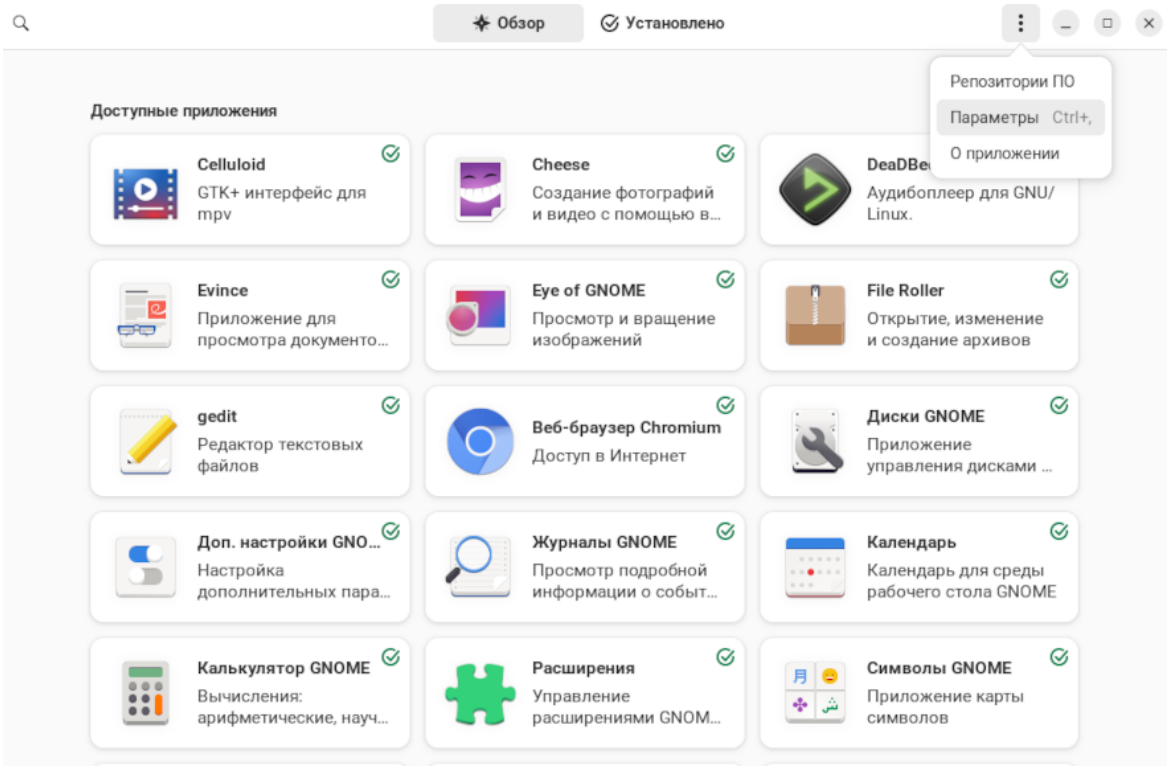

Рис. 77: Параметры обновлений

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

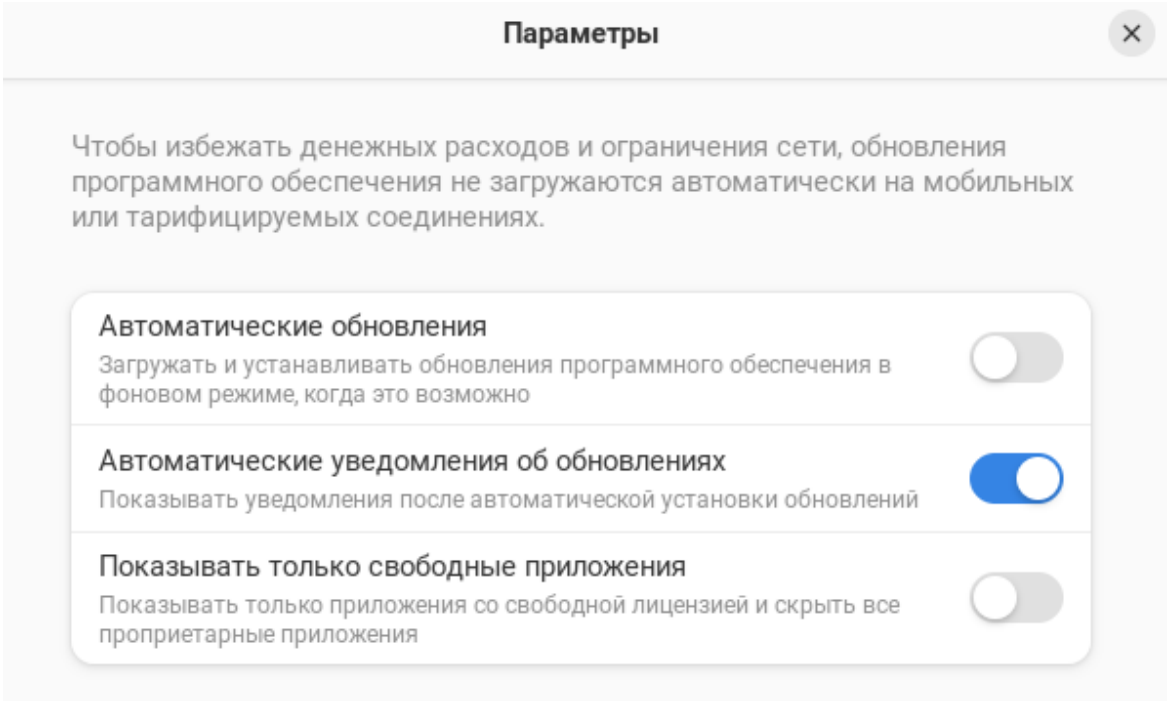

Рис. 78: Окно настройки параметров обновлений

6. РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ ПО КОНТЕЙНЕРИЗАЦИИ

6.1. Введение

Безопасность средства контейнеризации обеспечивается использованием программного комплекса для реализации настроек функций безопасности (далее – программный комплекс).

Пользователь системы работает с Docker в непривилегированном режиме (rootless), когда экземпляр Docker запускается в контексте текущего пользователя.

Пользователю запрещается устанавливать и использовать сторонние средства для создания и установки образов контейнеров в информационной системе.

6.2. Требования к авторизации пользователя

Для работы с Docker пользователь не должен иметь права доступа суперпользователя – root, и должен явно авторизоваться в системе (работать не через `sudo`).

Предупреждение

Работа через sudo – запрещена.

6.3. Настройка Docker

Для установки и настройки демона Docker выполните следующую команду:

```
$ dockerd-rootless-setuptool.sh install
```

После выполнения скрипта `dockerd-rootless-setuptool.sh` разработчики Docker рекомендуют пользователям выполнить самостоятельно дополнительную настройку – добавить в файл `~/.bashrc` следующие строки:

```
export PATH=/usr/bin:$PATH
export DOCKER_HOST=unix:///run/user/XXXX/docker.sock
```

Где `XXXX` – id пользователя.

Рекомендуется выполнить данные настройки. Для этого:

- откройте в редакторе файл `~/.bashrc`;
- скопируйте из вывода скрипта рекомендованные строки и вставьте их в

файл `~/.bashrc`;

- сохраните и закройте файл `~/.bashrc`.

После выполнения скрипта `dockerd-rootless-setuptool.sh` требуется перезагрузить компьютер.

6.4. Запрещённые параметры при запуске контейнера Docker

Запрещается при запуске контейнеров Docker использовать следующие параметры:

- `--net=host` – нарушение изоляции сетевого пространства;
- `--pid=host` – нарушение изоляции пространства PID;
- `--ipc=host` – нарушение изоляции пространства IPC;
- `--device` – нарушение изоляции устройств хоста и контейнера;
- `--userns=host` – нарушение изоляции пользовательских пространств имён.

При обнаружении того, что контейнер был запущен с использованием запрещённого параметра, исполнение запуска контейнера прерывается с выводом пользователю стандартного информационного сообщения ОС МСВСфера («Убито») и отправкой по электронной почте сообщений администратору и пользователю.

6.5. Обязательные параметры при запуске контейнера Docker

При запуске контейнеров Docker обязательно использовать следующие параметры:

- `--memory` – требование всегда запускать контейнеры с ограничением по памяти;
- `--read-only` – монтирование корневой файловой системы в режиме только для чтения. При необходимости нужно явно указывать каталоги, в которые разрешена запись. Для изоляции дискового пространства также можно использовать хранилища `volume`.

При обнаружении того, что контейнер был запущен без использования обязательного параметра, исполнение запуска контейнера прерывается с выводом пользователю стандартного информационного сообщения ОС МСВСфера («Убито») и отправкой по электронной почте сообщений администратору и пользователю.

6.6. Действия при создании или добавлении образа Docker

Образ, созданный пользователем (команда `docker build`) и прошедший проверку сканированием, перед использованием должен быть подписан ЭЦП.

7. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера страниц			Номера извещений	Подпись	Дата внесения изм.	Дата введения изм.