Код Безопасности

Средство защиты информации

# Secret Net LSP

## Руководство пользователя

RU.88338853.501410.017 92




| | |
|---|---|
| Почтовый адрес: | **105318, Россия, Москва, а/я 101<br>ООО "Код Безопасности"** |
| Телефон: | **8 495 982-30-20** |
| E-mail: | **info@securitycode.ru** |
| Web: | **http://www.securitycode.ru** |

# Оглавление

# Введение

Данное руководство предназначено для пользователей компьютеров, на которых функционирует изделие "Средство защиты информации Secret Net LSP" RU.88338853.501410.017 (далее — СЗИ, Secret Net LSP, система защиты).

## Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

**Исключения.** Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

## Другие источники информации

**Сайт в Интернете.** Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru).

**Учебные курсы.** Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training-courses/. Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

# Глава 1
# Общие сведения

## Что нужно знать

Средство защиты информации Secret Net LSP расширяет функциональные возможности ОС Linux по управлению доступом к ресурсам и правами пользователей.

Прежде чем приступить к работе на защищенном компьютере, рекомендуется ознакомиться с изложенными в этом документе базовыми понятиями и описанием порядка работы с Secret Net LSP.

Центральную роль в управлении системой защиты играет администратор. Администратор определяет права пользователя на доступ к ресурсам компьютера. Для того чтобы пользователь мог приступить к работе на компьютере, администратор должен зарегистрировать его в системе:

- присвоить условное имя, необходимое для идентификации пользователя;
- сообщить пароль, который необходим для аутентификации (подтверждения подлинности) пользователя. Для аутентификации могут использоваться аппаратные средства (персональные идентификаторы), на которых записана служебная информация для идентификации пользователя.

## Что необходимо иметь

Перед началом работы на защищенном компьютере необходимо:

1. Получить у администратора имя пользователя и пароль для входа в систему. Администратор также может выдать вам персональный идентификатор, который потребуется для входа в систему и входа в режиме усиленной аутентификации. Персональным идентификатором может быть Rutoken S, Rutoken S RF, Rutoken S micro, Rutoken ЭЦП и iButton.

| | |
|---|---|
| **Имя** | Для идентификации пользователя |
| **Пароль** | Для проверки подлинности пользователя |
| **Персональный идентификатор** | Для идентификации пользователя, хранения пароля и ключевой информации, необходимой для входа в систему, когда включен режим усиленной аутентификации |

2. Выяснить у администратора, какими правами и привилегиями вы сможете пользоваться при работе, а также какие ограничения действуют в Secret Net LSP в соответствии с настройками защитных механизмов.

## Что важно помнить

Во избежание затруднительных ситуаций следуйте двум общим рекомендациям:

1. Запомните свое имя в системе и пароль. Никому не передавайте персональный идентификатор, а пароль никому не сообщайте.
2. Во всех сложных ситуациях, которые вы сами не в состоянии разрешить, обращайтесь к администратору. Если имеющихся прав доступа к ресурсам недостаточно для эффективного выполнения должностных обязанностей, обращайтесь к администратору.

# О защитных механизмах

На компьютере, защищенном Secret Net LSP, действуют следующие защитные механизмы:

- механизмы защиты входа в систему;
- механизм разграничения доступа к объектам файловой системы;
- механизм разграничения доступа к устройствам;
- механизм контроля целостности;
- механизм затирания остаточной информации;
- механизм регистрации событий.

## Механизмы защиты входа в систему

Механизмы предназначены для предотвращения доступа посторонних лиц к защищенному компьютеру и включают в себя механизмы идентификации и аутентификации.

Идентификация и аутентификация выполняются при входе пользователя в систему, при смене пользователем пароля и при запуске механизма повышения полномочий (запуске приложений с привилегиями другого пользователя).

Для усиления защиты входа могут использоваться персональные идентификаторы — устройства, предназначенные для хранения информации, необходимой для идентификации и аутентификации пользователя.

В системе Secret Net LSP может применяться режим, когда ввод идентификационных и/или аутентификационных данных должен осуществляться только путем предъявления персонального идентификатора пользователя.

Кроме того, в Secret Net LSP может быть установлен режим усиленной аутентификации, когда по запросу системы пользователь должен предъявить идентификатор с хранящейся в нем ключевой информацией.

Персональные идентификаторы выдаются пользователям администратором.

## Механизм разграничения доступа к объектам файловой системы

Доступ пользователя к объектам файловой системы (каталогам и файлам) осуществляется на основе прав, предоставленных ему администратором.

Администратор определяет, кто из пользователей может получить доступ к ресурсу и какой тип доступа ему может быть предоставлен.

- Используются следующие типы прав доступа:
- на открытие объекта на чтение;
- на открытие объекта на запись;
- на исполнение объекта. Для каталогов — право на чтение содержимого каталога;
- запрет на удаление файла в каталоге для не владельцев;
- на исполнение файла от имени его владельца;
- на исполнение файла от имени группы владельца. Для каталогов — наследование группы для объектов в каталоге.

При создании нового ресурса файловой системы (каталога, файла) пользователь, создавший ресурс, автоматически становится его владельцем. При этом ресурс будет принадлежать группе создавшего его пользователя.

Пользователь может при необходимости изменить установленные по умолчанию права доступа к ресурсу, владельцем которого он является.

## Механизм разграничения доступа к устройствам

В целях предотвращения несанкционированной утечки информации с защищаемого компьютера в Secret Net LSP используется механизм разграничения доступа пользователей и групп к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам.

Пользователи могут подключать и работать только с теми устройствами, которые зарегистрированы в системе, и выполнять только те операции, которые заданы правами доступа к данному устройству.

Регистрацию устройств и назначение прав доступа к ним выполняет администратор.

Подключение устройств контролируется системой Secret Net LSP и регистрируется в журналах.

## Механизм контроля целостности

При загрузке операционной системы контролируется целостность объектов файловой системы (файлов и каталогов), поставленных на контроль администратором.

В Secret Net LSP предусмотрена блокировка входа пользователей в систему при нарушении целостности объектов, поставленных на контроль. Снять блокировку может только администратор.

## Механизм затирания остаточной информации

Механизм предназначен для предотвращения доступа к остаточной информации в освобождаемых блоках оперативной памяти и запоминающих устройств (жестких дисков, внешних запоминающих устройств).

Действие механизма заключается в очистке (обезличивании) освобождаемых областей памяти путем выполнения в них однократной (или многократной) произвольной записи.

Предусмотрены два режима затирания на жестких дисках и внешних запоминающих устройствах: синхронный и асинхронный.

В **синхронном** режиме затирание остаточной информации выполняется автоматически при удалении файлов.

В **асинхронном** режиме предусмотрено отложенное затирание удаляемых файлов: файлы перемещаются в специальный каталог ("Корзина") для дальнейшей очистки сервисом затирания.

Асинхронный режим может быть назначен отдельным разделам жесткого диска и/или запоминающего устройства (например, USB-флеш-накопителя).

Независимо от состояния механизма затирания (включен/выключен) и режима его работы пользователь может принудительно вручную выполнять безопасное удаление файлов на жестких дисках и внешних носителях с помощью утилиты **secrm**, вызываемой из контекстного меню файлового менеджера.

## Механизм регистрации событий

В процессе работы Secret Net LSP события, происходящие на компьютере и связанные с безопасностью системы, регистрируются в подсистемах, входящих в состав СЗИ, обрабатываются и сохраняются в файловой базе данных. На основании сведений, хранящихся в файловой базе данных, формируется "Журнал событий", включающий в себя системный журнал и журнал аудита.

Содержимое журналов позволяет администратору контролировать работу защитных механизмов и проводить аудит действий пользователей.

## Что нужно знать и иметь перед началом работы

Перед началом работы в системе администратор должен предоставить пользователям все необходимые права для выполнения должностных обязанностей и проинформировать о предоставленных правах, разъяснить особенности работы в рамках действующих защитных механизмов.

Если для входа в систему используется персональный идентификатор, необходимо получить его у администратора и ознакомиться с порядком его применения.

# Глава 2
# Вход в систему

## Варианты входа в систему

Общий порядок идентификации и аутентификации при входе в систему зависит от способа ввода идентификационных данных. Предусмотрен ввод данных (имени пользователя и пароля) с клавиатуры и/или считывание с персонального идентификатора пользователя. В обоих случаях может быть установлено дополнительное требование усиленной аутентификации, когда пользователь должен предъявить ключ, хранящийся в его персональном идентификаторе.

Режим входа задается администратором.

Ввод данных для идентификации и аутентификации может осуществляться одним из трех способов:

| **Для идентификации** |
|---|
| Имя пользователя вводится с клавиатуры |
| Имя пользователя вводится при предъявлении его персонального идентификатора |
| Имя пользователя может вводиться с клавиатуры или при предъявлении персонального идентификатора. Задается по умолчанию после установки Secret Net LSP |
| **Для аутентификации** |
| Аутентификация выполняется по паролю, хранящемуся в идентификаторе или введенному с клавиатуры. Задается по умолчанию после установки Secret Net LSP |
| Аутентификация выполняется по паролю, введенному с клавиатуры, и ключу, хранящемуся в идентификаторе |
| Аутентификация выполняется по паролю и ключу, хранящимся в идентификаторе |

Для всех пользователей компьютера устанавливается единый режим входа.

Если применяются средства аппаратной поддержки системы защиты, администратор выдает каждому пользователю персональный идентификатор (USB-ключ Rutoken или идентификатор iButton). При необходимости компьютер оснащается дополнительным устройством для считывания информации, содержащейся в персональном идентификаторе.

В зависимости от типа применяемого средства "Предъявить" персональный идентификатор означает привести его в соприкосновение со считывающим устройством (для iButton) или вставить в разъем USB-порта (для USB-ключей Rutoken S/S RF/S micro/ЭЦП).

Для доступа к памяти USB-ключа необходимо указывать специальный пароль — PIN-код. По умолчанию USB-ключ защищен стандартным PIN-кодом, который задан производителем устройства. Если стандартный PIN-код не изменен, система Secret Net LSP автоматически осуществляет доступ к памяти идентификатора при его предъявлении. В том случае, если администратор сменил стандартный PIN-код на другой (нестандартный), при каждом предъявлении идентификатора система выводит запрос на ввод PIN-кода. Администратор обязан сообщить вам нестандартный PIN-код при передаче идентификатора.

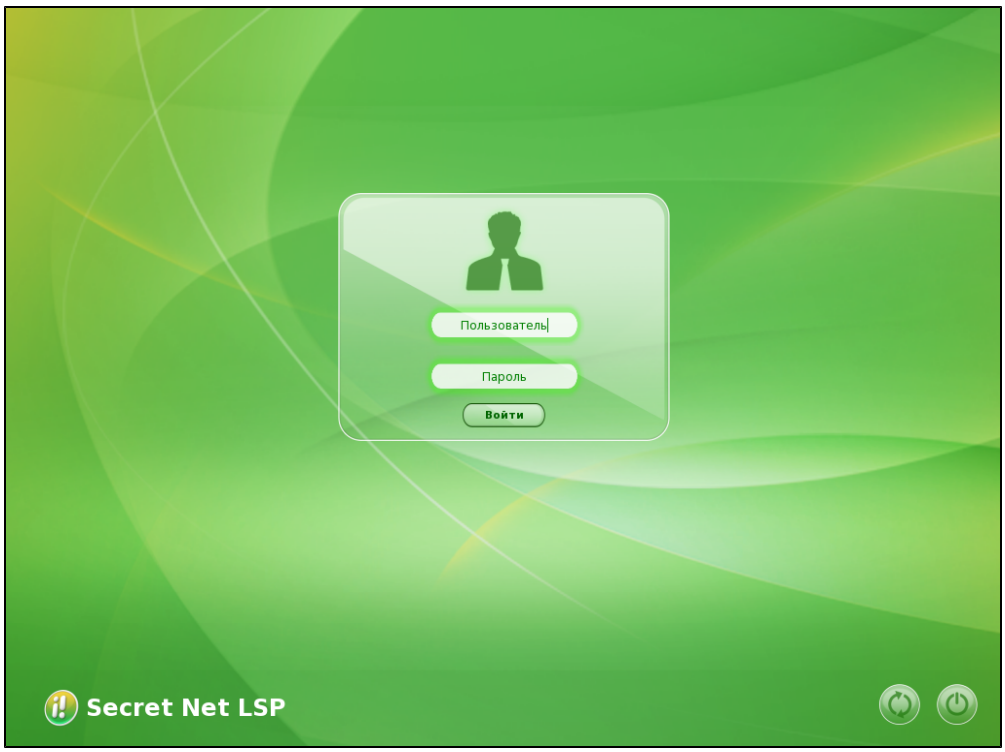
Не забывайте PIN-код, его утрата делает невозможным дальнейшее использование USB-ключа.

# Приглашение на вход в систему

Чтобы начать сеанс работы на компьютере, пользователь должен пройти процедуру входа в систему. При этом указываются учетные данные пользователя, необходимые для его идентификации. После ввода учетных данных система аутентифицирует пользователя, и при успешном завершении аутентификации пользователю предоставляется возможность работы в системе.

Процедура входа начинается при появлении на экране приглашения на вход в систему. В зависимости от действующих механизмов защиты и ограничений, установленных администратором, действия пользователя при входе в систему могут различаться.

Ниже на рисунке приведено окно приглашения на вход в систему:




В центре окна приглашения расположены поля для ввода имени и пароля пользователя и кнопка "Войти".

В правом нижнем углу окна приветствия расположены кнопки:

| | |
|---|---|
|  | Перезагрузка |
|  | Выключение |

В левом нижнем углу расположен логотип СЗИ Secret Net LSP.

## Стандартный вход

При стандартном режиме входа порядок действий пользователя совпадает с принятым в ОС Linux.

**Для входа в стандартном режиме:**

1. При появлении экрана приветствия (приглашение на вход в систему) введите имя и пароль пользователя.

В целях безопасности символы пароля не отображаются в явном виде в строке ввода. Помните, что при вводе пароля различаются строчные и заглавные буквы, кириллица и латиница. Если при вводе имени или пароля была неправильно нажата какая-либо клавиша, удалите ошибочно набранные символы в строке ввода с помощью клавиши <Backspace> или <Delete> и заново повторите ввод символов.

2. Нажмите кнопку "Войти".

   Если учетные данные введены правильно, будет выполнен вход в систему.

## Вход по идентификатору

При использовании для входа в систему персонального идентификатора система автоматически определяет имя пользователя, которому присвоен идентификатор.

**Для входа по идентификатору:**

1. При появлении экрана приветствия (приглашение на вход в систему) предъявите свой персональный идентификатор.

   Если в качестве идентификатора используется USB-ключ, который защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК".

2. Реакция системы защиты зависит от информации о пароле пользователя, содержащейся в персональном идентификаторе, и наличия закрытого ключа (если установлен режим усиленной аутентификации). Возможны следующие варианты:
   - идентификатор содержит актуальный пароль пользователя;
   - в идентификаторе не записан пароль или идентификатор содержит другой пароль, не совпадающий с паролем пользователя (например, из-за того, что срок действия пароля истек и он был заменен, но не записан в персональный идентификатор);
   - в идентификаторе отсутствует ключ или записанный в идентификаторе ключ не соответствует открытому ключу пользователя.

   **Если в идентификаторе содержится актуальный пароль**, то после успешной проверки прав пользователя выполняется вход в систему без запроса пароля.

   **Если в идентификаторе нет пароля или содержится другой пароль**, появится сообщение об ошибке входа в систему.

   **Если в идентификатре отсутствует ключ или он не соответствует открытому ключу пользователя**, появится сообщение об ошибке аутентификации.

   При появлении сообщения об ошибке вход в систему пользователю будет запрещен. В этом случае обратитесь к администратору.

## Смешанный вход

**Для входа в систему:**

- Введите имя и пароль с клавиатуры и нажмите кнопку "Войти" или предъявите персональный идентификатор, хранящий пароль.

## Как действовать в проблемных ситуациях

При нарушении правил входа система защиты прерывает процедуру входа.

Ниже приведены сообщения системы защиты и ОС при неверных действиях пользователя или сбоях системы при входе. Там же указаны причины их появления и рекомендуемые действия пользователя.

**Неправильное имя пользователя**
**Неправильное имя пользователя или пароль**

**Причина.** Указанное имя пользователя отсутствует в базе данных системы или введен неправильный пароль.

**Действия пользователя.** Проверьте состояние переключателя регистра (верхний/нижний) и переключателя раскладки (рус/лат).

Если допущена ошибка при вводе, повторите ввод имени и пароля.

Если вы забыли свой пароль, обратитесь за помощью к администратору.

**Пароль в идентификаторе не совпадает с текущим.**

**Причина.** В персональном идентификаторе записан пароль, отличный от имеющегося в системе.

**Действия пользователя.** Для смены пароля обратитесь к администратору.

**Идентификатор с серийным номером < > не привязан ни к одной учетной записи.**

**Причина.** При входе в систему предъявлен идентификатор, не принадлежащий входящему пользователю или не содержащий нужной информации.

**Действия пользователя.** Повторите процедуру входа, предъявив нужный идентификатор.

**Истек срок действия пароля.**

**Причина.** При входе в систему указан пароль, срок действия которого истек. Вход в систему невозможен.

**Действия пользователя.** Для смены пароля обратитесь к администратору.

**Неправильный ПИН-код.**

**Причина.** Введен неправильный PIN-код персонального идентификатора.

**Действия пользователя.** Введите правильный ПИН-код, полученный от администратора.

**Не удалось считать сведения с идентификатора с серийным номером < >.**

**Причина.** Возможно, идентификатор испорчен или чтение данных из идентификатора было выполнено с ошибкой.

**Действия пользователя.** Добейтесь правильного контакта персонального идентификатора со считывающим устройством.

Если ошибка устойчиво повторяется, обратитесь за помощью к администратору.

**Закрытый ключ не соответствует открытому, ошибка аутентификации.**

**Причина.** Повреждена ключевая информация в идентификаторе.

**Действия пользователя.** Для замены ключа обратитесь к администратору.

**Ошибка при работе со считывателем.**

**Причина.** Аппаратная или программная ошибка при работе считывателя.

**Действия пользователя.** Перезагрузите компьютер и повторите вход в систему. Если ошибка повторяется, обратитесь к администратору.

**Аутентификация без персонального идентификатора запрещена политикой безопасности.**

**Причина.** Была предпринята попытка ввода идентификационных данных с клавиатуры при установленном режиме входа по идентификатору.

**Действия пользователя.** Для ввода идентификационных данных предъявите персональный идентификатор.

**Идентификатор с серийным номером < >не обнаружен.**

**Причина.** При смене пользователем пароля, хранящегося в персональном идентификаторе, последний не был предъявлен для записи нового пароля.

**Действия пользователя.** Повторно смените пароль и во время процедуры его смены предъявите идентификатор.

**Не удалось сменить пароль на идентификаторе с серийным номером < >.**

**Причина.** Произошла аппаратная или программная ошибка при записи пароля в идентификатор.

**Действия пользователя.** Повторите процедуру смены пароля. Если сменить пароль в идентификаторе не удается, обратитесь к администратору.

## Смена пароля

Пользователь может сменить свой пароль после истечения срока, запрещающего смену пароля. Смена пароля осуществляется пользователем после входа в систему. Процедура смены пароля выполняется в режиме командной строки.

Если срок действия пароля истек, пользователю будет предложено сменить пароль при входе в систему.

Если пользователь не сменил устаревший пароль в течение определенного времени, учетная запись пользователя будет заблокирована и он не сможет войти в систему. В этом случае необходимо обратиться к администратору.

**Для смены пароля после входа в систему:**

1. Запустите командную оболочку и введите команду passwd.

   Появится запрос на ввод текущего пароля.
2. Введите пароль.

   Появится запрос на ввод нового пароля.
3. Введите новый пароль.

   При вводе пароля осуществляется проверка его качества. Пароль должен содержать не менее 6 буквенно-цифровых символов и удовлетворять требованиям сложности.

   Появится запрос на повторный ввод нового пароля.
4. Введите повторно новый пароль.

   Появится сообщение об успешном обновлении пароля.

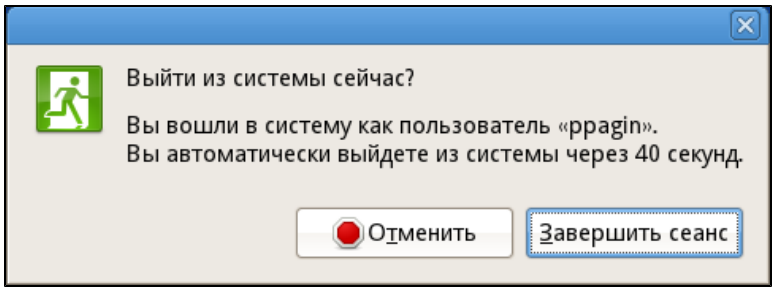
## Выход из системы

Выход из системы (завершение сеанса) выполняется с помощью команд окружения рабочего стола (в зависимости от используемой ОС).

**Для выхода из системы:**

1. Выберите в меню "Система" команду "Завершить сеанс пользователя".

   Появится следующее окно:




2. Нажмите кнопку "Завершить сеанс".

   Будет выполнен выход пользователя из системы и на экране появится окно приветствия СЗИ Secret Net LSP.

## Перезагрузка и выключение

**Для перезагрузки или выключения:**

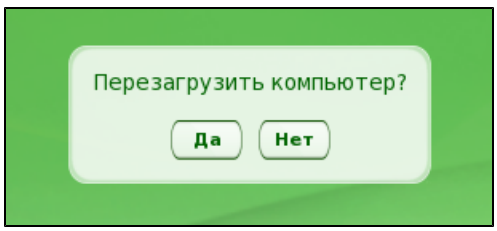
1. Выйдите из системы.

   На экране появится окно приветствия.

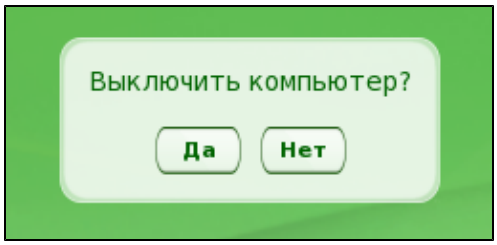
2. В окне приветствия в правом нижнем углу нажмите кнопку:

| | |
|---|---|
|  | - для перезагрузки системы |
|  | - для выключения компьютера |

   - Если была нажата кнопка перезагрузки системы, в окне приветствия появится предупреждение:




   - Если была нажата кнопка выключения компьютера, в окне приветствия появится предупреждение:




3. Нажмите кнопку "Да".

   Начнется перезагрузка системы или выключение компьютера.

# Глава 3
# Работа в условиях действия защитных механизмов

## Разграничение прав доступа

При создании нового ресурса файловой системы (каталога, файла) пользователь, создавший ресурс, автоматически становится его владельцем. При этом в зависимости от типа ресурса (каталога или файла) к нему по умолчанию устанавливаются классические права доступа UNIX и расширенные права доступа ACL для владельца, группы владельца и остальных.

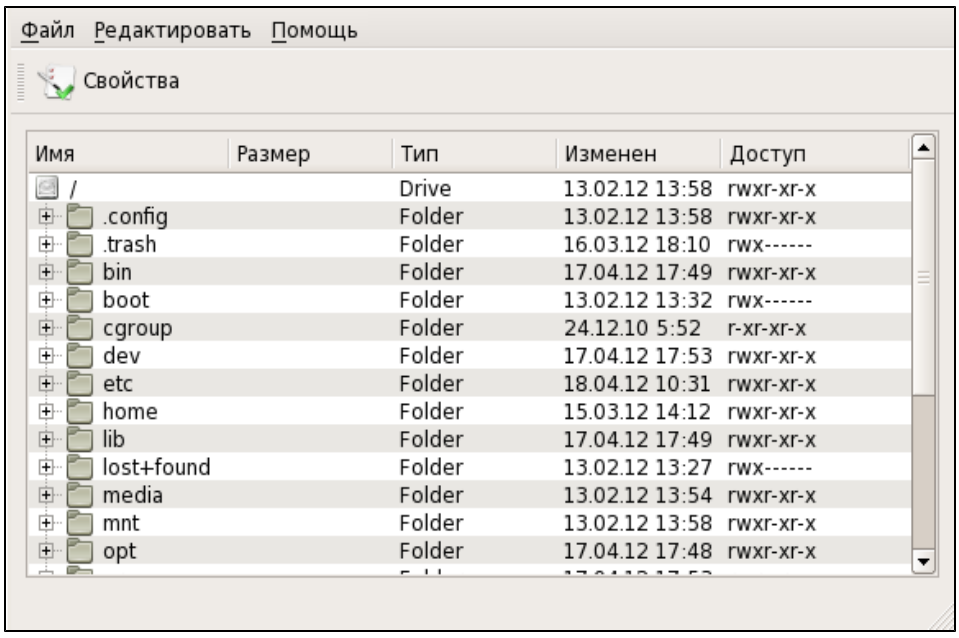
Пользователь-владелец может при необходимости изменить установленные по умолчанию права доступа.

Просмотр и изменение прав доступа к ресурсам осуществляются с помощью утилиты управления правами доступа.

**Для запуска утилиты управления правами доступа:**

1. Запустите файловый менеджер.
2. Выберите объект, вызовите контекстное меню и выберите пункт "Контроль доступа".

   Запустится утилита управления и на экране появится окно "Управление правами доступа":




   В окне представлено содержимое корневого каталога файловой системы и приведены права доступа UNIX к каталогам. Права доступа отображаются строкой следующего формата:

| Владелец | Группа | Остальные |
|---|---|---|
| rwx | rwx | rwx |

   В таблице: r — чтение, w — запись, x — выполнение.
3. Для просмотра прав доступа к вложенным папкам и файлам раскройте соответствующую папку.

   Более подробно права доступа к каталогам и файлам описаны ниже.

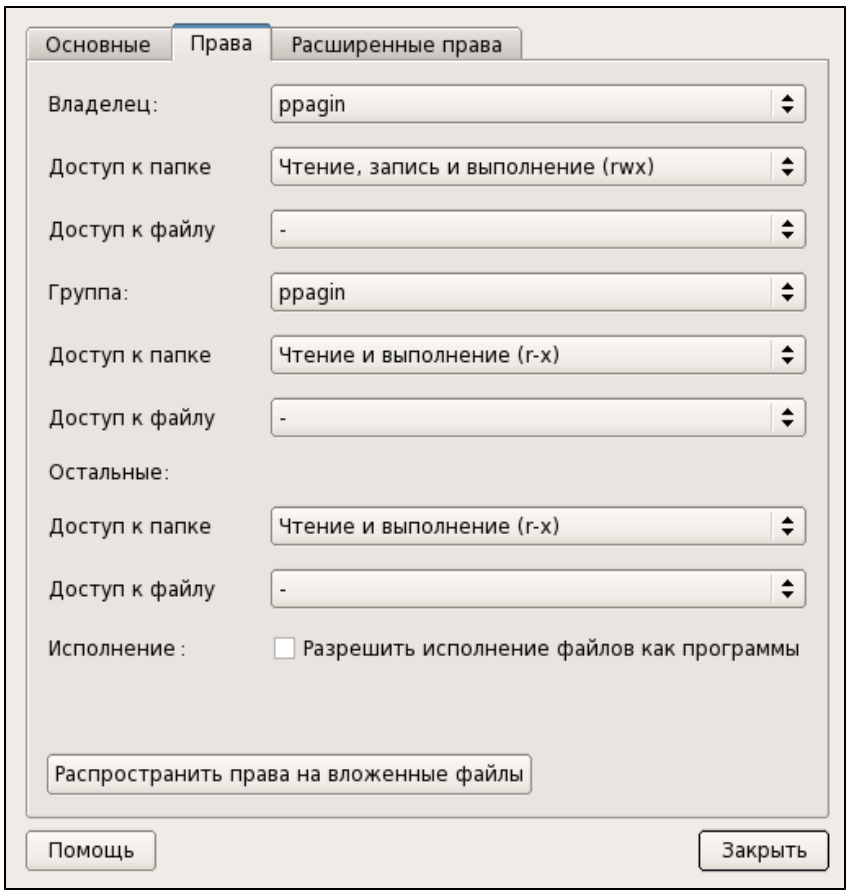
## Права доступа к каталогам и файлам

**Для просмотра и изменения прав доступа к каталогу:**

1. Запустите утилиту просмотра прав (см. выше), выберите нужный ресурс (каталог или файл) и нажмите кнопку "Свойства" на панели инструментов (или вызовите контекстное меню выбранного ресурса и выберите команду "Свойства").

   Откроется окно свойств данного ресурса.

2. Перейдите на вкладку "Права":




   На вкладке представлены права UNIX, установленные для владельца, группы владельца и остальных.

3. При необходимости измените права доступа.

   Для каталога:

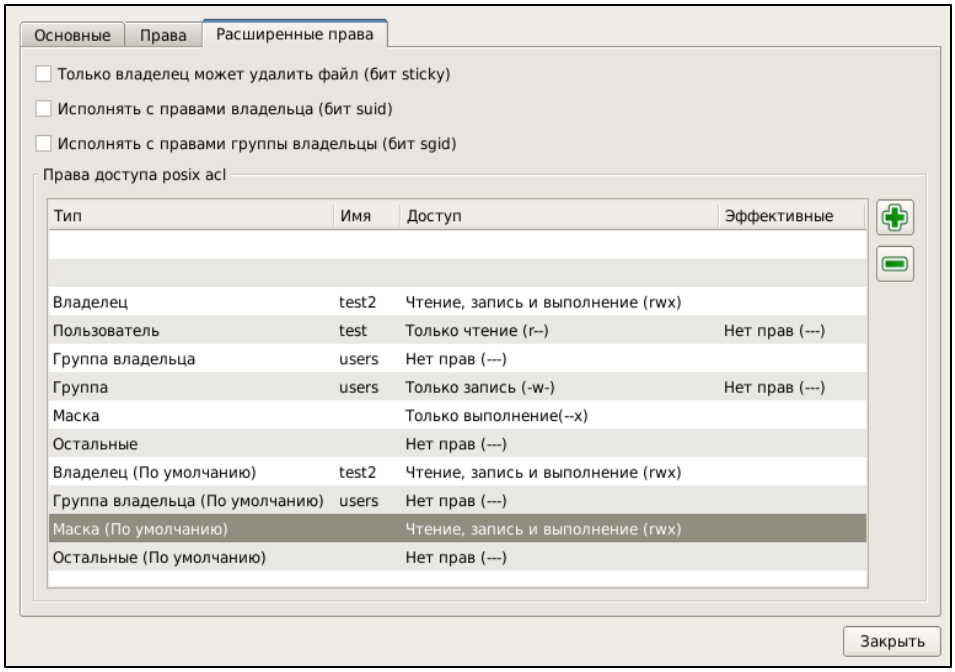
| Поле | Описание |
|---|---|
| Владелец | Владелец ресурса. Изменить значение может только владелец ресурса или пользователь с правами root |
| Доступ к папке | Для каталогов. Выберите из раскрывающегося списка права доступа к папке |
| Доступ к файлу | Для каталогов. Выберите из раскрывающегося списка права доступа к файлам в папке:<br>• Нет доступа;<br>• Запись;<br>• Чтение;<br>• Чтение и запись;<br>• Не определено (-) |
| Группа | Для каталогов. Группа владельца. Изменить нельзя |

| Поле | Описание |
|---|---|
| Доступ к папке | Для каталогов. Выберите из раскрывающегося списка права доступа группы владельца к папке |
| Доступ к файлу | Для каталогов. Выберите из раскрывающегося списка права доступа группы владельца к файлам в папке:<br>• Нет доступа;<br>• Запись;<br>• Чтение;<br>• Чтение и запись;<br>• Не определено (-) |
| Доступ к папке (остальные) | Для каталогов. Выберите из раскрывающегося списка права доступа остальных к папке |
| Доступ к файлу | Для каталогов. Выберите из раскрывающегося списка права доступа остальных к файлам в папке:<br>• Нет доступа;<br>• Запись;<br>• Чтение;<br>• Чтение и запись;<br>• Не определено (-) |
| Разрешить исполнение файлов как программы | Установите отметку, если необходимо разрешить исполнение файлов в каталоге как программы |
| Распространить права на вложенные файлы | Установите отметку, если необходимо распространить права на вложенные файлы |

Для файла:

| Поле | Описание |
|---|---|
| Владелец | Владелец ресурса. Изменить значение может только владелец или пользователь с правами root |
| Права доступа | Выберите из раскрывающегося списка права доступа к файлу |
| Группа | Группа владельца. Изменить нельзя |
| Права доступа | Выберите из раскрывающегося списка права доступа группы владельца к файлу |
| Права доступа (остальные) | Выберите из раскрывающегося списка права доступа остальных к файлу |
| Разрешить исполнение файла как программы | Установите отметку, если необходимо разрешить исполнение файла как программы |

4. Для просмотра или изменения расширенных прав и прав POSIX ACL перейдите на вкладку "Расширенные права":




5. При необходимости установите нужные отметки в полях:

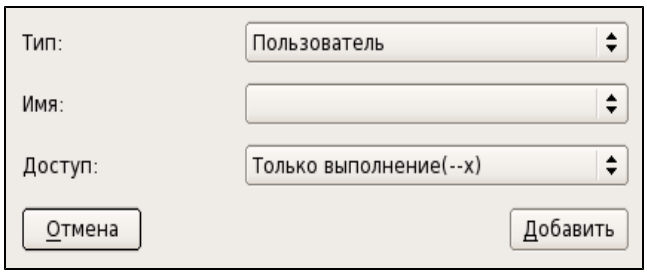
   Только владелец может удалить файл (бит sticky)

   Исполнять с правами владельца (бит suid)

   Исполнять с правами группы владельца (бит sgid)

6. Для добавления новой записи в список POSIX ACL нажмите кнопку , расположенную справа.

   Появится диалог "Добавить запись ACL":




7. В поле "Тип" выберите тип субъекта доступа. Доступные значения:

   Для каталога:

| Тип субъекта | Описание |
|---|---|
| Пользователь | Права устанавливаются для пользователя |
| Группа | Права устанавливаются для группы |
| Маска | Задает эффективное значение прав для пользователей и групп |
| По умолчанию для пользователя | Только для каталогов |
| По умолчанию для группы | Только для каталогов |
| Маска по умолчанию | Фильтр, определяющий максимально возможные права доступа |
| По умолчанию для остальных | Фильтр, определяющий максимально возможные права доступа по умолчанию |

Для файла:

| Тип субъекта | Описание |
|---|---|
| Пользователь | Права устанавливаются для пользователя |
| Группа | Права устанавливаются для группы |
| Маска | Задает эффективное значение прав для пользователей и групп |

8. Для выбранного типа субъекта доступа (кроме маски, маски по умолчанию и остальных) выберите в поле "Имя" имя пользователя или группы.
9. В поле "Доступ" выберите из раскрывающегося списка права доступа.
10. Нажмите кнопку "Добавить".

    В списке прав доступа POSIX ACL появится новая запись.
11. Добавьте все необходимые записи в список.

    Для удаления записи из списка выделите ее и нажмите кнопку , расположенную справа.

    Для удаления всех записей используйте команду контекстного меню.
12. После редактирования списка POSIX ACL нажмите кнопку "Закрыть".

# Безопасное удаление

В Secret Net LSP предусмотрено безопасное удаление файлов, которое может быть использовано для удаления, например, конфиденциальной информации. При безопасном удалении последующее восстановление удаленных файлов невозможно.

Режим безопасного удаления задается администратором. При этом в зависимости от установленного режима безопасное удаление может распространяться на отдельные каталоги или устройства.

Пользователь может независимо от установленного режима принудительно использовать безопасное удаление файлов с помощью ручного запуска утилиты **secrm**.

Утилита **secrm** не используется в сетевых файловых системах и в журналируемых файловых системах.

Утилита вызывается из контекстного меню файлового менеджера (например, Nautilus, Dolphin или Thunar).

## Безопасное удаление в режиме графического интерфейса

При удалении файлов в режиме графического интерфейса по умолчанию используются три прохода перезаписи с нулями в конце.

**Для безопасного удаления файла или каталога:**

1. В файловом менеджере выберите файл или каталог, предназначенный для удаления, вызовите контекстное меню и выберите команду "Безопасное удаление".

   Появится предупреждение о невозможности последующего восстановления данных после удаления.
2. Для удаления нажмите кнопку "OK" в окне предупреждения и дождитесь подтверждения об успешном завершении операции.
3. Нажмите кнопку "OK" в окне подтверждения.

# Работа с USB-устройствами

При разграничении доступа пользователей к USB-устройствам и шинам USB, SATA и IEEE 1394 предусмотрены три режима работы защитного механизма:

- отключено — действия пользователей с устройствами и шинами не контролируются;
- мягкий — действия пользователей регистрируются в журнале;
- жесткий — применяются все права доступа к шинам и устройствам, заданные администратором.

Режим работы механизма разграничения доступа к устройствам задается администратором.

При возникновении проблем, связанных с доступом к устройствам, обратитесь к администратору.