КОД безопасности

Средство защиты информации

Secret Net LSP

Руководство пользователя

RU.88338853.501410.017 92

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

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

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505- 30- 20 или 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 https://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 операционных систем (ОС) семейства 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. Персональными идентификаторами могут быть таблетки iButton, USB-ключи Rutoken, ESMART Token, JaCarta, vdToken 2.0, Guardant ID, смарт-карты JaCarta, ESMART Token.

Имя	Для идентификации пользователя
Пароль	Для проверки подлинности пользователя
Персональный идентификатор	Для идентификации пользователя, хранения пароля и ключевой информации

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 свой 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:

- защиты входа в систему;
- разграничения доступа к объектам файловой системы;
- разграничения доступа к устройствам;
- контроля целостности;
- замкнутой программной среды;
- персонального межсетевого экрана;
- затирания остаточной информации;
- регистрации событий.

Механизм защиты входа в систему

Механизм предназначены для предотвращения доступа посторонних лиц к защищенному компьютеру и включает в себя механизм 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 Secret Net LSP может применяться режим, когда ввод идентификационных или аутентификационных данных должен осуществляться только путем предъявления персонального идентификатора пользователя.

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 утечки информации с защищаемого компьютера в Secret Net LSP используется механизм разграничения доступа пользователей и групп к шинам USB, SATA, сетевым интерфейсам 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.

Назначение прав доступа к устройствам выполняет администратор.

Подключение устройств контролируется 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 замкнутой программной среды

При работе в условиях замкнутой программной среды администратором для каждого пользователя определяется перечень программ, разрешенных для запуска. При попытке запуска пользователем программ, не входящих в этот перечень, их запуск запрещается.

Если требуется расширить перечень разрешенных для запуска программ, необходимо обратиться к администратору безопасности, который обладает правом предоставлять пользователям доступ к ресурсам информационной системы.

Механизм персонального межсетевого экрана

Персональный межсетевой экран (ПМЭ) представляет собой автономный компонент средства защиты информации Secret Net LSP, предназначенный для защиты серверов и рабочих станций от несанкционированного доступа и разграничения сетевого доступа в информационных системах.
За счет работы модуля межсетевого экранирования механизм ПМЭ обеспечивает фильтрацию сетевого трафика для отправителей и получателей контролируемой информации в рамках всех операций ее передачи узлам информационной системы на сетевом, транспортном и прикладном уровнях, а также предоставляет возможность явно разрешать или запрещать информационный поток на основании установленных администратором правил фильтрации.

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 или запоминающего устройства (например, USB-флеш-накопителя).

Независимо от состояния механизма затирания (включен или выключен) и режима его работы пользователь может принудительно вручную выполнять безопасное удаление файлов на жестких дисках и внешних носителях с помощью утилиты **secrm**, запускаемой из командной строки.

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.

Лицензии на использование подсистем

Механизмы защиты системы Secret Net LSP доступны для использования при наличии соответствующих зарегистрированных лицензий. Лицензируются следующие механизмы:

- механизмы, входящие в базовую защиту (обязательная лицензия);
- дискреционное управление доступом;
- контроль устройств;
- замкнутая программная среда;
- персональный межсетевой экран.

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 или считывание из персонального идентификатора. Также может быть установлено дополнительное требование аутентификации, при котором необходимо предъявить приватный ключ, хранящийся в персональном идентификаторе пользователя.

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 определяется при предъявлении его персонального идентификатора
Имя пользователя может вводиться с клавиатуры или определяться при предъявлении персонального идентификатора

Метод аутентификаци зависит от наличия у пользователя записанного пароля и закрытого ключа в электронном идентификаторе. Режимы использования электронного идентификатора настраиваются администратором.

Для всех пользователей компьютера устанавливается единый режим входа.

Если применяются средства аппаратной поддержки системы защиты, администратор выдает каждому пользователю персональный идентификатор (USB-ключ, смарт-карту 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 (iButton, смарт-карта) или вставить в разъем USB-порта (USB-ключ).

Для доступа к памяти USB-ключа или смарт-карты необходимо указывать специальный пароль — PIN-код. По умолчанию устройство защищено стандартным PIN-кодом, который задан производителем устройства. Если стандартный PIN-код не изменен, 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 приведет к потере данных на USB-ключе или смарт-карте. Дальнейшее использование USB-ключа или смарт-карты будет возможным только после их форматирования.

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 используемой на компьютере ОС Linux и действующих механизмов защиты и ограничений, установленных администратором, внешний вид экрана с приглашением на вход в систему и действия пользователя при входе в систему могут различаться.

Примечание. Подробные сведения об экране с приглашением на вход в систему содержатся в сопроводительной документации к используемой на компьютере ОС Linux.

Стандартный вход

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

Для входа в стандартном режиме:

1. При появлении экрана с приглашением на вход в систему введите имя и пароль пользователя.

   Внимание! 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. Для завершения процедуры нажмите клавишу <Enter>.

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

Вход по идентификатору

При использовании для входа в систему персонального идентификатора автоматически определяется имя пользователя, которому принадлежит идентификатор.

Для входа по идентификатору:

1. При появлении экрана с приглашением на вход в систему предъявите свой персональный идентификатор.

   Если идентификатор (USB-ключ или смарт-карта) защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите кнопку "ОК" или клавишу <Enter>. Количество попыток неверного ввода PIN-кода ограничено и настраивается администратором. Превышение количества попыток приведет к блокировке идентификатора.

2. Реакция системы защиты зависит от информации о пароле пользователя, содержащейся в персональном идентификаторе, и наличия приватного ключа (если установлен соответствующий режим 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, появится сообщение об ошибке входа в систему.

Если идентификатор содержит другой пароль, появится сообщение об этом и будет предложено ввести верный пароль с возможностью перезаписи его на идентификаторе.

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

Если превышено количество попыток неверного ввода данных для входа в ОС, пользователь будет заблокирован. Количество попыток неверного ввода данных для входа в ОС задается администратором.

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 или предъявите персональный идентификатор, хранящий пароль.

Загрузка и вход в систему при использовании ПАК "Соболь"

На компьютере с программно-аппаратным комплексом (ПАК) "Соболь", который функционирует в режиме интеграции с Secret Net LSP, загрузка компьютера и вход пользователя в систему могут выполняться с использованием одного персонального идентификатора.

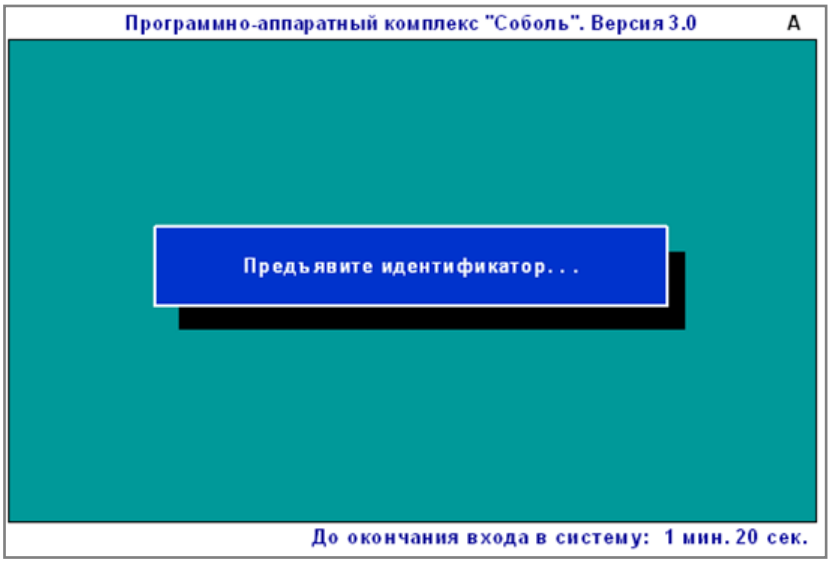
Secret Net LSP поддерживает интеграцию с ПАК "Соболь" версий 3.x и 4. Порядок загрузки компьютера и входа в систему для этих версий разный:

- для версий 3.x — см. ниже;
- для версии 4 — см. стр.**13**.

Для загрузки компьютера и входа в систему при использовании ПАК "Соболь" версий 3.x:

1. Включите питание компьютера.

   На экране появится запрос персонального идентификатора.



Пояснение.
- При включенном режиме автоматического входа в строке сообщений будет отсчитываться время в секундах, оставшееся до автоматического входа в ПАК "Соболь", после которого начнется загрузка ОС.
- Если включен режим ограничения времени, в строке сообщений будет отсчитываться время в минутах и секундах, оставшееся до предъявления идентификатора и ввода пароля. Если вы не успели за отведенное время выполнить эти действия, на экране появится сообщение "Время сеанса входа в систему истекло". Чтобы повторить попытку входа, нажмите <Enter>, а затем — любую клавишу.

2. Предъявите свой персональный идентификатор.

   Если в идентификаторе нет пароля или идентификатор содержит другой пароль (например, из-за того, что при смене пароля новый пароль не был записан в идентификатор), на экране появится диалог для ввода пароля.

3. Введите пароль для входа в ПАК "Соболь" и нажмите <Enter>.

   Если введенный пароль не соответствует предъявленному идентификатору, в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". Нажмите любую клавишу и снова предъявите идентификатор. Используйте выданный вам персональный идентификатор и не допускайте ошибок при вводе пароля.

Внимание! Учитывайте, что число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение в текущем сеансе входа, то при следующей попытке входа в строке сообщений появится сообщение "Ваш вход в систему запрещен: Вы превысили предел неудачных попыток входа", после чего компьютер будет заблокирован. В этом случае обратитесь за помощью к администратору.

   После успешного предъявления идентификатора (и ввода правильного пароля, если это необходимо) выполняется тестирование датчика случайных чисел. При обнаружении ошибок в строке сообщений появится сообщение об этом. Если после перезагрузки компьютера тестирование датчика случайных чисел вновь выполнено с ошибкой, обратитесь к администратору.

   Перед загрузкой операционной системы проводится контроль целостности файлов (если это предусмотрено).

   Если проверка завершена успешно, начнется загрузка операционной системы. При обнаружении ошибок на экране появятся сообщения об ошибках. Если в строке сообщений появилось сообщение "Компьютер заблокирован", выключите компьютер и обратитесь за помощью к администратору.

4. Далее на этапе загрузки ОС ваши действия зависят от того, какая информация о пароле содержится в персональном идентификаторе и какой режим входа используется в Secret Net LSP. Возможны следующие варианты:
   - Пароль, считанный из идентификатора при входе в ПАК "Соболь", является актуальным для ОС и в Secret Net LSP включен режим, разрешающий использовать идентификатор для входа в систему (см. стр.**10** и стр.**11**).

     В этом случае после успешной проверки прав пользователя будет выполнен вход в систему без запроса пароля.
   - В идентификаторе не записан пароль или идентификатор содержит другой пароль, который не является актуальным для ОС, или в Secret Net LSP включен режим, **не** допускающий вход в систему по идентификатору (см. стр.**10**).

     В таких случаях появится диалог для ввода учетных данных пользователя. Если идентификатор разрешено использовать для входа, в

диалоге будет отображаться имя пользователя — владельца предъявленного идентификатора.

Введите актуальный пароль (и имя пользователя, если требуется) и нажмите соответствующую кнопку (например, кнопку "Войти") или клавишу <Enter>.

Если введенный пароль правильный и хранение пароля в идентификаторе **не** предусмотрено, выполнится вход в систему.

Если введенный пароль правильный и актуальный пароль нужно записать в идентификатор — на экране появится запрос. В этом случае предъявите идентификатор для записи актуального пароля.

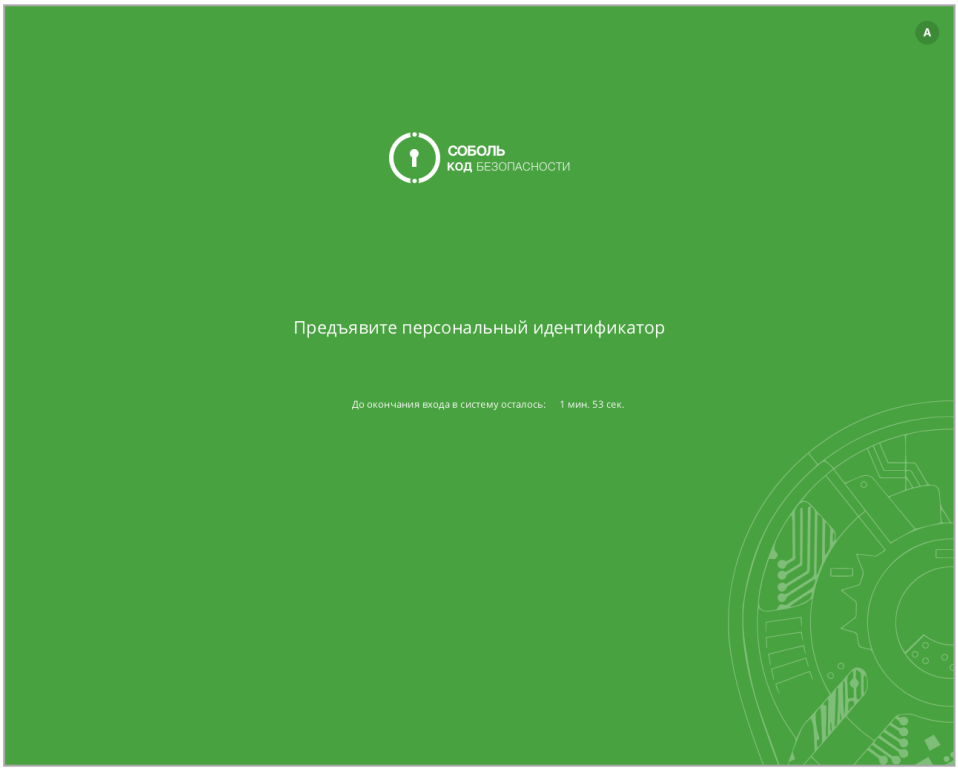
Для загрузки компьютера и входа в систему при использовании ПАК "Соболь" версии 4:

1. Включите питание компьютера.

   Начнется процедура тестирования датчика случайных чисел.

   Пояснение. Если при включении компьютера тестирование датчика случайных чисел не началось или появилось сообщение "Компьютер заблокирован", обратитесь к администратору.

   При успешном завершении тестирования на экране появится запрос персонального идентификатора.

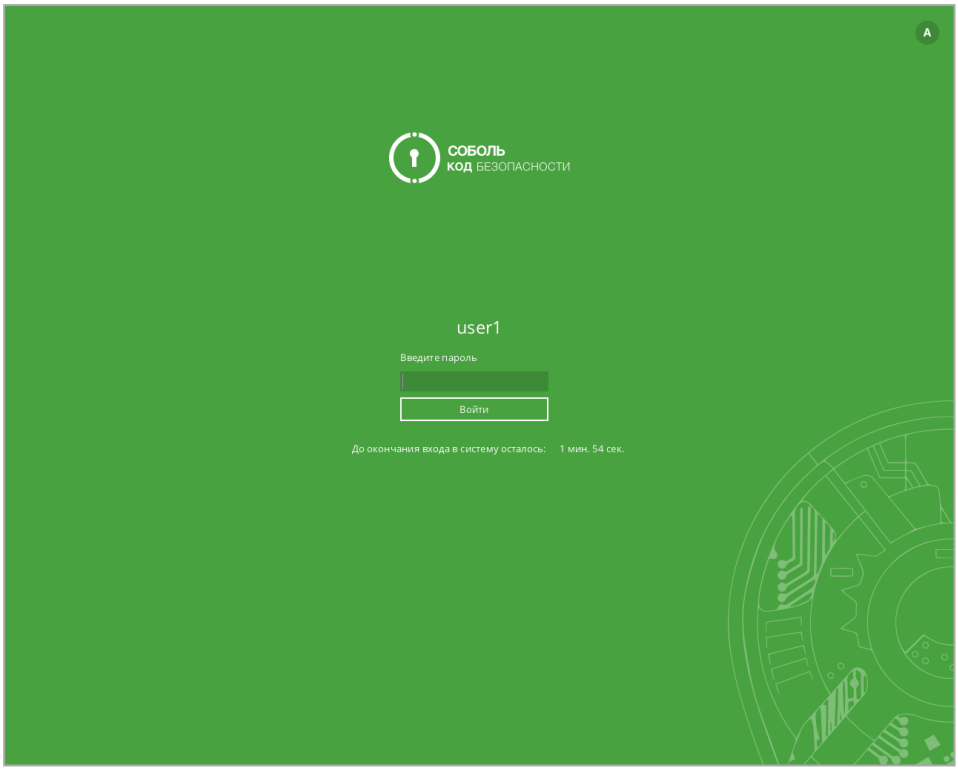


   Пояснение.
   - Счетчик времени, оставшегося до автоматической загрузки операционной системы, отображается, если в ПАК "Соболь" настроена автоматическая загрузка.
   - Счетчик времени, оставшегося для предъявления идентификатора и ввода пароля, отображается, если администратор активировал режим ограничения времени на вход в систему. Если вы не успели за отведенное время предъявить идентификатор и ввести пароль, компьютер будет заблокирован. Перезагрузите компьютер и повторите вход.

2. Предъявите выданный вам персональный идентификатор.

   Пояснение.
   - Если идентификатор уже предъявлен, ПАК "Соболь" автоматически считывает его.
   - Если одновременно предъявлено несколько идентификаторов, серийный номер первого из них отображается на экране. Для смены идентификатора нажмите <Esc>. Для выбора идентификатора с нужным серийным номером нажмите <Enter>.

Если в идентификаторе нет пароля или идентификатор содержит другой пароль (например, из-за того, что при смене пароля новый пароль не был записан в идентификатор), на экране появится диалог для ввода пароля.

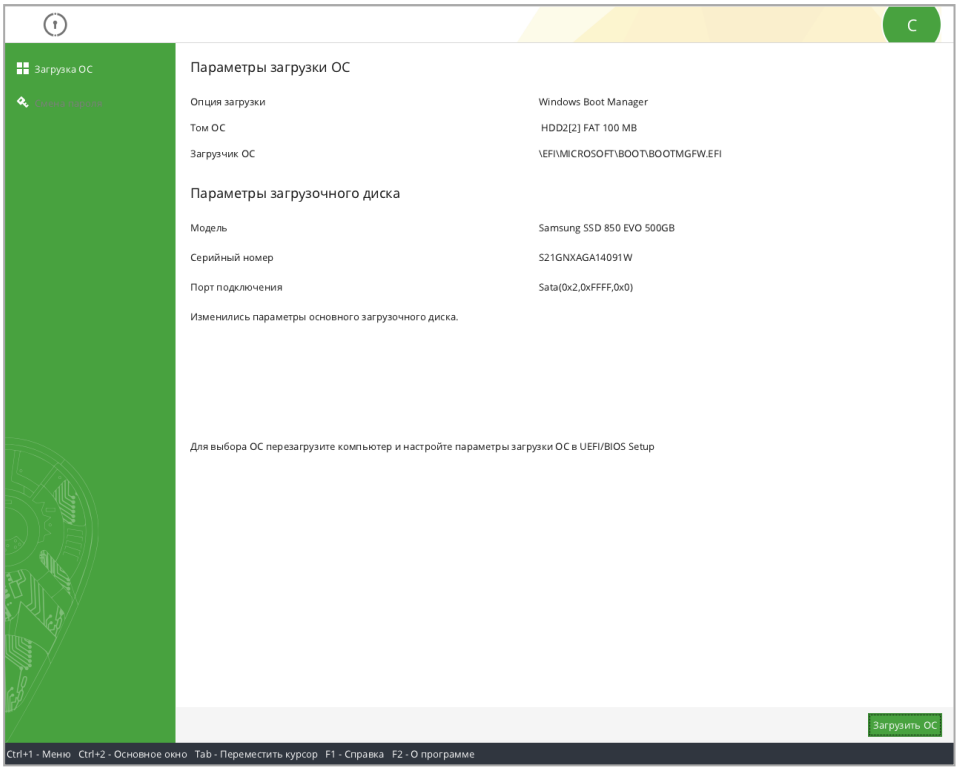


3. Введите пароль для входа в ПАК "Соболь" и нажмите <Enter>.

Если введенный пароль не соответствует предъявленному идентификатору, на экране появится сообщение "Неверный персональный идентификатор или пароль". Нажмите любую клавишу и снова предъявите идентификатор. Используйте выданный вам персональный идентификатор и не допускайте ошибок при вводе пароля.

Внимание! Число неудачных попыток входа может быть ограничено администратором. Если вы превысили это ограничение, то при следующей попытке входа на экране появится сообщение о блокировке компьютера. В этом случае обратитесь к администратору.

После успешного ввода учетных данных появится окно "Загрузка ОС".



4. Нажмите кнопку "Загрузить ОС" или клавишу <Enter>.

   Будет выполнен контроль целостности файлов (если это предусмотрено).

   Если проверка завершена успешно, начнется загрузка операционной системы. При обнаружении ошибок на экране появятся сообщения об ошибках. Если на экране появилось сообщение "Компьютер заблокирован", выключите компьютер и обратитесь за помощью к администратору.

5. Далее на этапе загрузки ОС ваши действия зависят от того, какая информация о пароле содержится в персональном идентификаторе и какой режим входа используется в Secret Net LSP. Возможны следующие варианты:

   - Пароль, считанный из идентификатора при входе в ПАК "Соболь", является актуальным для ОС и в Secret Net LSP включен режим, разрешающий использовать идентификатор для входа в систему (см. стр.**10** и стр.**11**).

     В этом случае после успешной проверки прав пользователя будет выполнен вход в систему без запроса пароля.

   - В идентификаторе не записан пароль или идентификатор содержит другой пароль, который не является актуальным для ОС, или в Secret Net LSP включен режим, **не** допускающий вход в систему по идентификатору (см. стр.**10**).

     В таких случаях появится диалог для ввода учетных данных пользователя. Если идентификатор разрешено использовать для входа, в диалоге будет отображаться имя пользователя — владельца предъявленного идентификатора.

     Введите актуальный пароль (и имя пользователя, если требуется) и нажмите соответствующую кнопку (например, кнопку "Войти") или клавишу <Enter>.

     Если введенный пароль правильный и хранение пароля в идентификаторе **не** предусмотрено, выполнится вход в систему.

     Если введенный пароль правильный и актуальный пароль нужно записать в идентификатор — на экране появится запрос. В этом случае предъявите идентификатор для записи актуального пароля.

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 PIN-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.

При наличии у пользователя персональных идентификаторов, в которых хранится пароль, их необходимо будет предъявить для записи нового пароля.

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 программу эмулятора терминала, введите команду passwd и нажмите <Enter>.

   Появится запрос на ввод текущего пароля.
2. Введите пароль и нажмите <Enter>.

   Появится запрос на ввод нового пароля.
3. Введите новый пароль и нажмите <Enter>.

   Совет. При вводе пароля осуществляется его проверка. Учитывайте следующие требования:
   - длина пароля в символах не должна быть меньше минимально допустимой длины пароля, заданной администратором, и пароль должен соответствовать требованиям сложности;
   - если имеется персональный идентификатор, используемый для входа в ПАК "Соболь", пароль не должен содержать символы кириллицы. Иначе вход в ПАК "Соболь" станет невозможен.

   Появится запрос на повторный ввод нового пароля.
4. Введите повторно новый пароль и нажмите <Enter>.

   Если пароль хранится в персональном идентификаторе, на экране появится запрос на предъявление идентификатора для записи нового пароля.
5. Предъявите персональный идентификатор, номер которого указан в сообщении, и нажмите любую клавишу.

Если идентификатор (USB-ключ или смарт-карта) защищен нестандартным PIN-кодом, на экране появится запрос. Введите PIN-код и нажмите <Enter>.

6. При наличии у вас нескольких идентификаторов повторите действие **5** для каждого из них.

   При успешном завершении процедуры смены пароля появится сообщение об успешном обновлении пароля.

Временная блокировка компьютера

Функция временной блокировки компьютера позволяет предотвратить его несанкционированное использование на время вашего отсутствия. Временная блокировка выполняется средствами используемой на компьютере ОС Linux.

В Secret Net LSP дополнительно имеется возможность временной блокировки компьютера при изъятии персонального идентификатора пользователя, предъявленного при входе в систему. Такая блокировка будет выполняться, если администратор безопасности включил для компьютера соответствующий режим.

Для временной блокировки с помощью идентификатора:

- Извлеките из считывающего устройства персональный идентификатор, который был предъявлен при входе в систему.

  Компьютер перейдет в режим временной блокировки.

Для разблокирования компьютера с помощью идентификатора:

1. Предъявите тот же персональный идентификатор и при необходимости для продолжения нажмите нужную кнопку, например, "Разблокировать".

   Если нужные данные при входе считываются из идентификатора (см. стр.**9**), идентификатор содержит ваш текущий пароль и ввод PIN-кода не требуется, компьютер будет разблокирован.

   Во всех остальных случаях на экране будут появляться запросы для ввода нужных данных (PIN-код, пароль).

2. Введите запрашиваемые данные так, как это выполняется при входе в систему (см. стр.**10**).

   После успешного ввода нужных данных компьютер будет разблокирован.

Выход из системы, перезагрузка и выключение

Выход из системы (завершение сеанса), перезагрузка и выключение компьютера выполняются средствами ОС.

Порядок выполнения этих операций зависит от используемой на компьютере ОС Linux и подробно рассматривается в сопроводительной документации к ней.

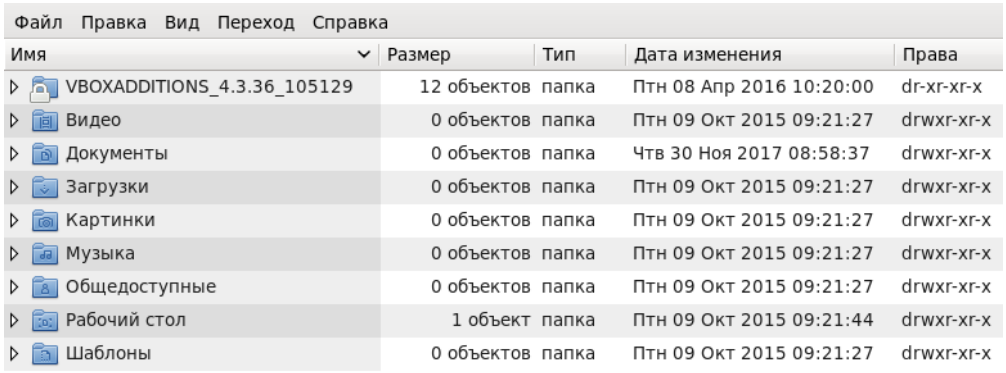
Глава 3
Работа в условиях действия защитных механизмов

Разграничение прав доступа

При создании нового ресурса файловой системы (каталога, файла) пользователь, создавший ресурс, автоматически становится его владельцем.

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

Просмотр и изменение прав доступа к ресурсам осуществляются с помощью файлового менеджера (например, Nautilus).



В окне представлено содержимое домашнего каталога пользователя 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.

Для просмотра прав доступа к вложенным папкам и файлам раскройте соответствующую папку.

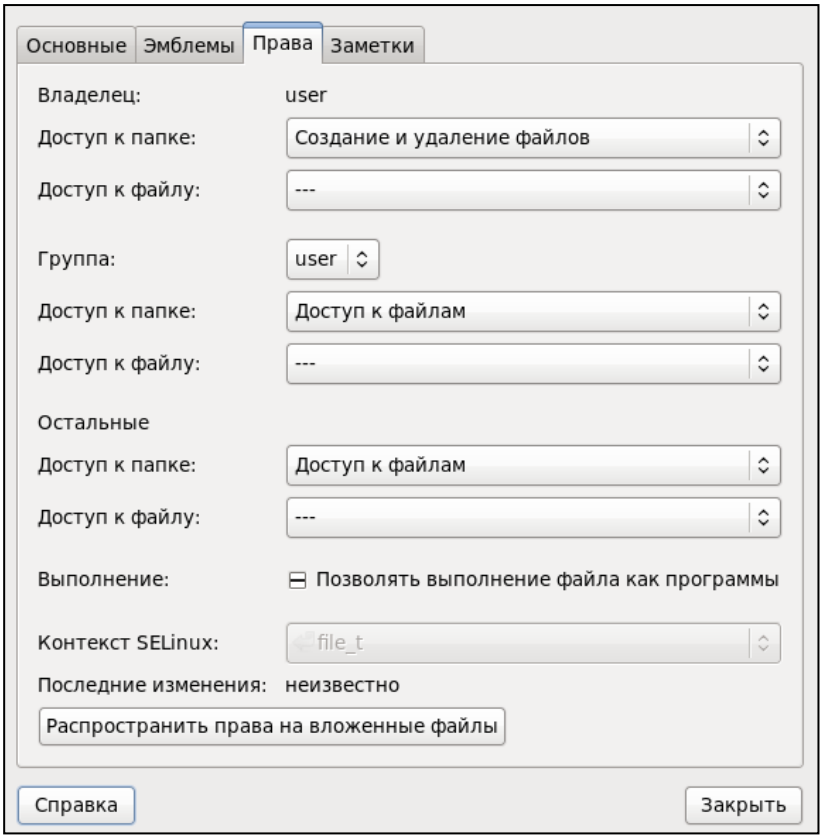
Более подробно права доступа к каталогам и файлам описаны ниже.

Права доступа к каталогам и файлам

Для просмотра и изменения прав доступа к каталогу:

1. Запустите файловый менеджер (например, Nautilus), вызовите контекстное меню нужного ресурса (каталога или файла) 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: • Нет доступа; • Запись; • Чтение; • Чтение и запись; • Не определено (-)
Группа	Для каталогов. Группа владельца. Изменить нельзя
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: • Нет доступа; • Запись; • Чтение; • Чтение и запись; • Не определено (-)
Доступ к папке (остальные)	Для каталогов. Выберите из раскрывающегося списка права доступа остальных к папке

Поле	Описание
Доступ к файлу	Для каталогов. Выберите из раскрывающегося списка права доступа остальных к файлам в папке: • Нет доступа; • Запись; • Чтение; • Чтение и запись; • 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. Завершив редактирование, нажмите кнопку "Закрыть".

Контроль целостности

При нарушении целостности объектов, поставленных на контроль, предусмотрена блокировка рабочей станции, если установлено правило КЦ. Также возможно последующее восстановление данных, установленное правилом при настройке механизма КЦ администратором. Снять блокировку может только администратор.

Персональный межсетевой экран

При нарушении правил персонального межсетевого экрана может вывестись всплывающее уведомление, если администратор настроил вывод сообщений.

Пример всплывающего уведомления:

Triggering a firewall rule #2: DROP UDP. ГГГГ-ММ-ДД ЧЧ:ММ:СС.

Замкнутая программная среда

Некоторые ресурсы могут быть недоступны из-за нехватки прав по ЗПС. При попытке доступа к ресурсу без определенных прав доступа, появляется уведомление о недоступности ресурса.

Пример уведомления:

"Отказано в доступе" ("недостаточно прав").

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 утилиты **secrm**.

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

Утилита запускается из командной строки.

Для безопасного удаления файла или каталога:

1. Запустите эмулятор терминала и выполните команду:

   ```
   secrm <имя файла/каталога>
   ```

2. Нажмите кнопку "Да" в окне подтверждения и дождитесь сообщения об успешном завершении операции.
3. Нажмите кнопку "OK" в окне сообщения.

Работа с USB-устройствами

При разграничении доступа пользователей к USB-устройствам и шинам USB, SATA и сетевым интерфейсам предусмотрены два режима работы защитного механизма:

- отключено — действия пользователей с устройствами и шинами не контролируются;
- включено — применяются все права доступа к устройствам, заданные администратором.

Режим работы механизма разграничения доступа к устройствам задается администратором.

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