



Код безопасности

Средство защиты информации
Secret Net LSP



Руководство администратора

RU.88338853.501410.017 91



Код Безопасности

© Компания "Код Безопасности", 2016. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

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

Оглавление

Введение	6
Общие сведения	7
Назначение	7
Основные функции	7
Защитные механизмы	7
Механизм защиты входа в систему	7
Механизм разграничения доступа и защиты ресурсов	9
Механизм разграничения доступа к устройствам	10
Механизм контроля целостности	11
Механизм регистрации событий	13
Механизм затирания остаточной информации	13
Архитектура	14
Подсистема локального управления	14
Подсистема идентификации и аутентификации	16
Подсистема разграничения доступа	16
Подсистема разграничения доступа к устройствам	17
Подсистема контроля целостности и восстановления	18
Подсистема очистки памяти	19
Подсистема ведения журналов	20
Подсистема аудита	20
Функции администратора	21
Требования к аппаратным и программным средствам	22
Установка, удаление и обновление	23
Установка	23
Удаление	25
Обновление	26
Первая загрузка	27
Инструментальные средства администратора	27
Описание панели безопасности	27
Начало работы	30
Настройки по умолчанию	30
Просмотр журналов	33
Смена паролей пользователей	34
Смена паролей средствами панели управления	34
Управление пользователями	36
Просмотр списка пользователей	36
Просмотр списка групп пользователей	37
Добавление и удаление пользователей	39
Изменение атрибутов пользователя	40
Добавление и удаление групп пользователей	42
Изменение атрибутов группы	42
Включение и исключение пользователей из группы	43
Изменение паролей и атрибутов паролей пользователей	43
Блокировка и разблокировка учетной записи пользователя	43
Защита входа в систему	44
Настройка и контроль параметров паролей по умолчанию	44
Включение и выключение режима усиленной аутентификации	44
Настройка блокировки входа при нарушении целостности	45
Блокировка учетных записей пользователей	45
Персональные идентификаторы	45
Просмотр сведений об идентификаторах пользователя	46
Инициализация идентификатора	48
Присвоение идентификатора	48
Отмена присвоения идентификатора	50

Запись пароля в идентификатор	50
Проверка принадлежности идентификатора	50
Блокировка идентификатора	51
Управление режимом входа в систему	51
Управление режимом аутентификации	52
Управление доступом к объектам файловой системы	53
Включение и выключение	53
Просмотр прав доступа к объектам	53
Изменение прав доступа UNIX	55
Редактирование списка POSIX ACL	56
Разграничение доступа к устройствам	58
Список устройств	58
Регистрация устройства и назначение прав доступа	61
Отмена регистрации устройства	63
Сохранение настроек прав доступа в файл	63
Управление режимом работы подсистемы	64
Аудит событий	64
Контроль целостности	65
Постановка ресурсов на контроль	66
Снятие ресурса с контроля	67
Изменение реакции СЗИ на нарушение целостности	68
Разблокирование входа в систему	68
Аудит контроля целостности	68
Затирание остаточной информации	69
Включение и отключение механизма затирания	69
Изменение режима затирания остаточной информации	70
Ручной запуск утилиты безопасного удаления	70
Запуск утилиты <code>secrm</code> в режиме графического интерфейса	70
Запуск утилиты <code>shred</code> в режиме командной строки	71
Настройка удаленного управления	72
Аудит	75
Системный журнал	75
Контроль печати	78
Журнал аудита	78
Настройка аудита	81
Аудит объектов	82
Аудит сети	86
Просмотр правил аудита	87
Приложение	88
Утилиты Secret Net LSP	88
Настройка параметров политик	88
Управление персональными идентификаторами	88
Безопасное удаление	90
Разграничение доступа к устройствам	91
Контроль целостности	92
Правила аудита	93
Управление режимом аутентификации	94
Настройка удаленного управления	94
Резервное копирование настроек Secret Net LSP	95
Экспорт и импорт настроек Secret Net LSP	95
Перенос конфигурации Secret Net LSP предыдущих версий на Secret Net LSP 1.5	96
Работа с журналами	97
События, регистрируемые в системном журнале	97
Уровни важности событий	97
Группы сообщений	98
Типы сообщений	98

События, регистрируемые в журнале аудита	101
Типы сообщений	101
Управление режимами работы модулей ядра	101
Информация о работе подсистем	101
Управление режимами работы	102
Функциональный контроль	103
Замена серийного номера демонстрационной версии	103
Обновление операционной системы	105

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net LSP" RU.88338853.501410.017 (далее — СЗИ, Secret Net LSP, система защиты). В руководстве содержатся сведения, необходимые для установки, настройки и управления Secret Net LSP.

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

Назначение

Программный продукт Secret Net LSP (номер текущей версии — 1.5) предназначен для защиты от НСД к информационным ресурсам компьютеров, функционирующих под управлением следующих дистрибутивов Linux:

- ALT Linux 7.0.5 Centaurus;
- CentOS 7.1/6.5;
- ContinentOS 4.2;
- Debian 8.0/7.6;
- Red Hat Enterprise Linux 7.2/7.0/6.5/6.3/5.8/5.5/5.2.

Основные функции

Secret Net LSP реализует следующие основные функции:

- контроль входа пользователей в систему, в том числе с использованием аппаратных средств защиты;
- разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера;
- разграничение доступа пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам;
- уничтожение (затирание) содержимого файлов при их удалении;
- очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств);
- контроль целостности ключевых компонентов Secret Net LSP и объектов файловой системы;
- регистрация событий безопасности в журналах;
- контроль действий пользователей, связанных с доступом к файлам, устройствам и узлам вычислительной сети;
- проведение аудита действий субъектов (пользователей, процессов) с объектами файловой системы и аудита сетевых соединений.

Защитные механизмы

Защитные механизмы — это программные и аппаратные средства, предназначенные для реализации защитных функций системы Secret Net LSP. Краткое описание защитных механизмов, используемых в системе защиты, приведено в последующих подразделах.

Механизм защиты входа в систему

Защита от несанкционированного входа предназначена для предотвращения доступа посторонних лиц к защищенному компьютеру и включает в себя:

- программные и аппаратные средства идентификации и аутентификации;
- функции блокировки входа в систему и учетных записей пользователей.

Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователя выполняется при каждом входе в систему. При загрузке компьютера проверяются имя пользователя и его пароль.

В механизме парольной аутентификации предусмотрен контроль качества задаваемого пароля при его изменении пользователем.

Кроме входа в систему, механизм идентификации и аутентификации используется в следующих случаях:

- при смене пользователем пароля;
- при запуске механизма повышения полномочий (запуске приложений с привилегиями другого пользователя).

События, связанные с процедурами идентификации и аутентификации, регистрируются в журнале.

Для обеспечения дополнительной защиты входа в Secret Net LSP применяются средства аппаратной поддержки, в которых используются персональные идентификаторы. Персональный идентификатор — это отдельное устройство, входящее в комплект аппаратного средства и предназначеннное для хранения информации, необходимой для идентификации и аутентификации пользователя.

В Secret Net LSP используются персональные идентификаторы Rutoken S, Rutoken S RF, Rutoken S micro, Rutoken ЭЦП, Rutoken ЭЦП Flash и iButton. Для работы с идентификаторами iButton используется программно-аппаратный комплекс (ПАК) "Соболь" версии 3.0.

Режимы входа

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

Режим входа задается параметрами политики "Параметры аутентификации": "Метод идентификации" и "Метод аутентификации".

Параметр "Метод идентификации" задает способ ввода данных для идентификации и может принимать 3 значения:

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

Параметр "Метод аутентификации" задает способ ввода данных для аутентификации и может принимать 3 значения:

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

Управление режимом входа осуществляется администратором изменением перечисленных выше параметров на странице "Настройка политик".

Блокировка входа в систему

Механизм предназначен для предотвращения несанкционированного входа в систему. В этом режиме вход пользователей в систему блокируется. Вход разрешен только администратору с правами root.

К блокировке приводят следующие ситуации:

- нарушение функциональной целостности системы Secret Net LSP;
- нарушение целостности контролируемых объектов.

Проверка целостности компонентов Secret Net LSP и объектов файловой системы выполняется при загрузке операционной системы (ОС). В случае нарушения целостности контролируемых объектов вход в систему блокируется для всех пользователей. Разблокирование входа может выполнить только администратор.

Блокировка учетных записей

Для защиты входа в систему в Secret Net LSP используется механизм блокировки учетной записи пользователя. Предусмотрены принудительная блокировка администратором и автоматическая блокировка учетной записи пользователя в случае истечения срока действия пароля.

Механизм разграничения доступа и защиты ресурсов

Механизм дискреционного разграничения доступа используется для контроля и управления правами доступа пользователей и групп к объектам файловой системы — файлам и каталогам. При этом предусмотрено управление как классическими правами UNIX, так и списками контроля доступа POSIX ACL.

Права доступа UNIX

Для всех объектов файловой системы устанавливаются права доступа владельца, группы владельца и остальных субъектов. Владельцем объекта может быть любой пользователь системы. Группой может быть любая группа системы.

Объект одновременно может принадлежать только одному владельцу и группе.

При установке СЗИ Secret Net LSP права доступа изначально устанавливаются в соответствии с правами, определенными в ОС.

В механизме используются следующие типы прав доступа:

- r — право на открытие объекта на чтение;
- w — право на открытие объекта на запись;
- x — право на исполнение объекта (для каталогов — право на чтение содержимого каталога);
- t — sticky бит, для каталогов налагает запрет на удаление файла в каталоге для не владельцев;
- SUID — право на исполнение файла от имени его владельца;
- SGID — право на исполнение файла от имени группы владельца; для каталогов — наследование группы для объектов в каталоге.

Изменение прав доступа объекта разрешено только его владельцу или администратору.

При создании объекта без указания прав доступа на него устанавливаются права, вычисляемые на основании значения маски для текущей сессии.

При создании объекта его владельцем становится субъект, создавший данный объект. Объект будет также принадлежать группе создавшего его субъекта.

Правом смены владельца объекта обладает только администратор.

Изменение группы владельца объекта разрешается только владельцу данного объекта.

Списки контроля доступа POSIX ACL

Изначально для каждого объекта файловой системы автоматически назначается список POSIX ACL, соответствующий значениям стандартных прав доступа. Права доступа устанавливаются для трех категорий объектов:

- владельца;
- группы владельца;
- остальных.

Администратор может для каждого объекта добавить в список дополнительные права доступа: пользователей (пользователь выбирается из общего списка зарегистрированных пользователей системы) и групп (группа выбирается из общего списка зарегистрированных групп). Для каждого пользователя (группы) с установленными для них правами в список POSIX ACL может быть добавлена только одна запись.

При добавлении в список дополнительных прав автоматически добавляется маска. По умолчанию значение маски равно максимальному доступу (rwx) среди всех дополнительных пользователей и групп. Маска применяется к правам доступа именованных групп и группы владельца по правилу логического умножения. В результате определяются эффективные права доступа.

Для каталогов в списке POSIX ACL могут быть заданы права доступа по умолчанию для владельца, группы владельца и остальных, которые будут распространяться на создаваемые внутри каталога файлы и подкаталоги. При добавлении таких прав для них в список автоматически добавляется наследуемая маска.

Списки POSIX ACL преобладают над UNIX-правами доступа, т.е. при принятии решения подсистемой разграничения доступа о разрешении или запрещении доступа субъекта к объекту при однозначном определении прав доступа POSIX ACL (для данной пары субъект—объект) UNIX-права игнорируются.

В случае возникновения конфликтов прав доступа для пар субъект1—объект и субъект2—объект приоритет имеет запрещающее правило.

Изменение списка POSIX ACL объекта возможно, только если субъект является владельцем объекта, для которого производится изменение списка.

Механизм разграничения доступа к устройствам

Механизм используется для разграничения доступа пользователей и групп к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам в целях предотвращения несанкционированной утечки информации с защищаемого компьютера.



В текущей версии Secret Net LSP действие механизма распространяется только на физические устройства. Контроль доступа к виртуальным устройствам (например, LVM, программный RAID) не поддерживается.

Предоставление доступа осуществляется на основе матрицы доступа, описывающей права доступа пользователей и групп к зарегистрированным в системе устройствам.

Матрица доступа формируется администратором. Для формирования матрицы администратор должен выполнить следующее:

- составить список контролируемых USB-устройств;
- для каждого контролируемого устройства задать права доступа пользователей и групп.

Каждое контролируемое устройство однозначно идентифицируется по следующим параметрам:

- VendorID;
- DeviceID;
- серийный номер.

Значения вышеперечисленных параметров считаются автоматически при регистрации устройства. Дополнительно администратор для каждого устройства может задать условную символьную метку для его идентификации.

Права доступа к устройству задаются при его добавлении в список (регистрации устройства). При этом субъектами доступа могут быть:

- пользователи;
- группы;
- ВСЕ.

Назначаемые права доступа:

- на чтение;
- на чтение и запись;
- нет доступа.

Права доступа к устройству могут наследоваться от прав, установленных для шины.

Если пользователь входит в несколько групп, для каждой из таких групп вычисляются эффективные права доступа к устройству: производится логическое умножение прав доступа к устройству для групп, членами которых является пользователь. При этом разрешающие права имеют приоритет над запрещающими.

Механизм контроля целостности

Механизм контроля целостности (КЦ) предназначен для слежения за неизменностью содержимого ресурсов компьютера. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля при обнаружении несоответствия текущих и эталонных значений система оповещает администратора о нарушении целостности ресурсов и выполняет заданное при настройке действие, например, блокирует вход пользователя в систему.

Контроль проводится в автоматическом режиме при загрузке операционной системы. Также администратор может вручную запустить проверку целостности защищаемых ресурсов, используя средства панели безопасности.

Объекты и параметры контроля

Объектами контроля целостности в СЗИ Secret Net LSP являются:

- компоненты установленного ПО СЗИ (файлы и каталоги);
- ресурсы файловой системы компьютера, поставленные на контроль администратором (файлы и каталоги).



Постановка компонентов ПО СЗИ на контроль и сам контроль осуществляются автоматически без участия администратора. При этом вся настройка механизма контроля целостности (внесение в базу данных информации о контролируемых объектах, расчет контрольных сумм, реакция системы на нарушение целостности объектов, перечень регистрируемых событий) выполняется в процессе установки ПО СЗИ на компьютер.

Ресурсы файловой системы ставятся на контроль администратором вручную. При этом задаются список контролируемых объектов и реакция СЗИ на факты нарушения целостности защищаемых объектов.

Контроль файлов ведется по каждому из следующих параметров:

- права доступа (в том числе ACL);
- расширенные атрибуты (xattr);
- пользователь (владелец);
- группа;
- размер файла;
- время и дата последней модификации;

- контрольная сумма содержимого файла по алгоритму MD5.

Контроль каталогов ведется по каждому из следующих параметров:

- права доступа (в том числе ACL);
- расширенные атрибуты (xattr);
- индексный дескриптор каталога;
- пользователь (владелец);
- группа;
- время и дата последней модификации;
- создание объектов в каталоге;
- удаление объектов в каталоге.

Методы контроля

В качестве проверяющих методов используется метод подсчета и проверки контрольных сумм по алгоритму MD5.

Факт нарушения контроля целостности для каждого объекта фиксируется индивидуально. Объект признается целостным, когда каждый из фиксируемых параметров соответствует значениям из базы данных контроля целостности.

Регистрация событий

События, связанные с работой механизма контроля целостности (в том числе — с действиями администратора), регистрируются в "Журнале событий".

Полный перечень регистрируемых событий приведен в Приложении.

Реакция СЗИ на нарушение целостности объектов

В механизме контроля целостности в качестве реакции СЗИ на нарушение целостности объектов предусмотрены следующие варианты:

- не предпринимать никаких действий, только регистрация изменений;
- восстанавливать объект из эталонного значения;
- блокировать вход пользователей в систему;
- восстановить объект из эталонного значения и блокировать вход в систему.

Восстановление объекта из эталонного значения осуществляется только при одновременном выполнении трех условий:

- для объекта определено восстановление в настройках подсистемы контроля целостности;
- для объекта обнаружено нарушение целостности;
- существует эталонная копия объекта, сохраненная при его постановке на контроль.

При восстановлении объекта восстанавливается и каталог, в котором содержался данный объект.

Настройка механизма

Настройка контроля целостности компонентов СЗИ, поставленных на контроль при установке системы защиты, не требуется.

Для настройки контроля целостности объектов, поставленных на контроль вручную администратором, необходимо выполнить следующее:

- задать список объектов, подлежащих контролю;
- для каждого объекта задать реакцию СЗИ на нарушение его целостности.

Механизм регистрации событий

В процессе работы Secret Net LSP события, происходящие на компьютере, и события, связанные с безопасностью системы, регистрируются в подсистеме журнализации, входящей в состав СЗИ. События 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.

В системном журнале содержатся сведения обо всех событиях, зарегистрированных подсистемами, входящими в состав СЗИ.

В журнале аудита содержатся сведения, необходимые администратору для контроля действий субъектов (пользователей и процессов) и действий с защищаемыми объектами.

Механизм используется подсистемами ведения журналов и аудита.

Механизм затирания остаточной информации

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

Действие механизма заключается в очистке освобождаемых областей памяти путем выполнения в них однократной произвольной записи.

Затирание областей оперативной памяти осуществляется в момент их освобождения. При этом предусмотрена возможность разбиения больших страниц (2 МБ, 4 МБ, 1 ГБ) на более мелкие непосредственно перед очисткой. Дополнительно выполняется затирание SWAP при выключении/перезагрузке операционной системы.

Затирание остаточной информации на файловой системе происходит при выполнении следующих операций с файлами:

- удаление (unlink);
- переименование в рамках перемещения (rename);
- модификация размера файла (truncate).

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

В **синхронном** режиме модуль ядра перехватывает запросы к файловым системам на освобождение блоков данных, осуществляет запись в них маскирующей информации и помечает их как свободные.

Этот режим является основным и применим ко всем операциям освобождения блоков данных на внешних носителях, за исключением случаев, если в конфигурационном файле явно указано использовать асинхронный режим.

В **асинхронном** режиме предусмотрено отложенное затирание удаляемых файлов. Модуль ядра перехватывает запросы к файловым системам на удаление файлов данных, перемещает их в специальные каталоги (корзины) для дальнейшей очистки сервисом затирания.

Асинхронный режим может быть назначен отдельным разделом жесткого диска (например, разделу с домашними каталогами пользователя). Использовать асинхронный режим при работе с внешними устройствами не рекомендуется.

По умолчанию после установки системы механизм затирания остаточной информации выключен. При необходимости администратор может вручную включить механизм затирания и задать асинхронный режим для всех объектов файловых систем или асинхронный режим для отдельных объектов (каталогов или внешних запоминающих устройств).

Независимо от состояния механизма затирания (включен/выключен) и режима его работы пользователь может принудительно вручную осуществлять затирание остаточной информации с помощью утилиты **shred**.

Архитектура

СЗИ Secret Net LSP имеет модульную архитектуру и включает в свой состав следующие основные подсистемы:

- Подсистема локального управления. Предназначена для управления подсистемами, входящими в состав СЗИ, и контроля их работоспособности.
- Подсистема идентификации и аутентификации. Управляет работой механизма защиты входа пользователей в систему.
- Подсистема разграничения доступа к файлам и каталогам. Реализует дисcretionaryную модель разграничения доступа субъектов (пользователей, процессов) к объектам файловой системы.
- Подсистема разграничения доступа к устройствам. Реализует discretionaryную модель разграничения доступа пользователей к USB-флеш-накопителям.
- Подсистема контроля целостности. Осуществляет контроль целостности программных компонентов комплекса средств защиты (КСЗ) и объектов файловой системы. Осуществляет тестирование работоспособности модулей всех КСЗ по требованию администратора и самотестирование до запуска компонентов СЗИ.
- Подсистема журналирования. Осуществляет сбор сведений о зарегистрированных в других подсистемах событиях и формирование системного журнала и журнала аудита.
- Подсистема аудита. Предназначена для работы с журналами и настройки регистрации событий и правил аудита.
- Подсистема очистки памяти. Осуществляет очистку затиранием выделенных или перераспределенных участков оперативной памяти и освобождаемых участков на жестких дисках или внешних устройствах.

Подсистема локального управления

Подсистема управления — ключевой компонент, предназначенный для управления подсистемами, входящими в состав СЗИ, и контроля их работоспособности.

В состав подсистемы входят:

- утилиты загрузки и инициализации;
- CLI-клиент управления;
- GUI-клиент управления (панель безопасности Secret Net LSP);
- плагины безопасности;
- CLI-утилиты.

Утилиты загрузки и инициализации

Встраиваются в систему инициализации ОС и выполняют следующие функции:

- загрузка модулей ядра и контроль их работы (если нет модуля контроля);
- загрузка сервисов СЗИ при старте ОС и контроль их работы при загрузке;
- внесение изменений в конфигурации подсистем СЗИ на основании запросов от подсистем СЗИ;
- трансляция запросов на выполнение тех или иных операций от GUI- и CLI-клиентов управления указанным подсистемам (сервисам, утилитам).

Работа утилит загрузки и инициализации осуществляется в фоновом режиме.

Клиенты управления

CLI-клиент представляет собой классическое консольное UNIX-приложение, позволяющее администратору управлять работой Secret Net LSP в режиме командной строки.

GUI-клиент — программа, позволяющая администратору управлять работой Secret Net LSP средствами графического интерфейса.

В общем случае клиентами выполняются следующие функции:

- Аутентификация администратора (средствами подсистемы идентификации и аутентификации).
- Конфигурирование СЗИ с трансляцией запросов службе ядра.
- Получение информации о текущем состоянии КСЗ.
- Регистрация событий, связанных с действиями администратора, и критических событий в работе клиента (используются средства подсистемы регистрации событий).
- Контроль доступа к устройствам.
- Экспорт журналов.
- Предоставление возможности работы с плагинами безопасности:
 - тестирование СЗИ;
 - управление пользователями и персональными идентификаторами;
 - управление контролем целостности и восстановлением;
 - контроль устройств.

Плагины безопасности

В состав подсистемы локального управления входят следующие плагины:

Плагин	Описание
Плагин управления контролем целостности и восстановлением	Запуск утилиты контроля целостности с требуемыми параметрами. Оповещение службы ядра о состоянии утилиты контроля целостности
Плагин управления аудитом	Внесение изменения в конфигурационный файл сервиса аудита. Получение информации о контролируемых объектах и состоянии сервиса аудита
Плагин управления доступом к объектам файловой системы	Просмотр и изменение классических прав доступа UNIX и прав доступа POSIX ACL для указанного объекта файловой системы
Плагин управления доступом к устройствам	Получение информации о запрашиваемом устройстве. Изменение прав доступа для указанного устройства
Плагин управления пользователями и группами	Получение списка пользователей или групп. Изменение свойств пользователя или группы. Изменение свойств пароля пользователя. Получение свойств пользователя или группы. Получение свойств пароля пользователя. Связывание идентификаторов с пользователями
Плагин управления политиками	Получение текущего состояния политик. Изменение конкретной политики
Плагин управления системными сервисами	Запуск/останов сервисов. Поддержание состояния сервисов, указанного в настройках
Плагин резервного копирования	Резервное копирование и восстановление настроек Secret Net LSP: данных о пользователях и группах, содержимого базы данных настроек Secret Net LSP, содержимого журналов
Плагин настройки удаленного управления	Настройка режима удаленного управления для подключения к серверу безопасности СЗИ Secret Net 7 (пакет обновления 4 и выше)

Подсистема идентификации и аутентификации

Подсистема предназначена для управления средствами защиты входа в систему, использующими механизмы идентификации и аутентификации пользователей и предоставляющими аутентифицированную сессию для работы в ОС.

Подсистема имеет плагинную архитектуру, позволяющую подключать различные методы идентификации и аутентификации, и базируется на использовании подключаемых аутентификационных модулей (PAM).

В Secret Net LSP используется аутентификация двух типов — локальная и доменная. Доменная аутентификация обеспечивает вход в систему от имени доменного пользователя и требует наличия в системе библиотеки pam_winbind.so, а также включения компьютера в домен. При локальной аутентификации вход в систему выполняется от имени локального пользователя.

Подсистема обеспечивает:

- Хранение информации, необходимой для использования сервиса идентификации и аутентификации, информации о сроках действия учетных записей пользователей.
- Кеширование (например, для случаев повышения полномочий).
- Предоставление графического и консольного интерфейсов для идентификации и аутентификации при входе пользователей в систему.
- Организацию сессии работы пользователя в случае успешного прохождения процедуры проверки подлинности.
- Предоставление возможности запуска приложений с привилегиями другого пользователя.
- Предоставление интерфейса для прохождения процедуры проверки подлинности.
- Регистрацию событий.
- Управление пользователями и группами (добавление, удаление, блокирование; задание, смена паролей с проверкой старого пароля, за исключением смены пароля администратором).
- Поддержку работы с персональными идентификаторами пользователей.
- Управление режимом входа в систему.

Подсистема разграничения доступа

Подсистема реализует дискреционную модель разграничения доступа и осуществляет контроль доступа к объектам файловой системы.

Средствами подсистемы администратор может изменять установленные по умолчанию права доступа UNIX, изменять и снимать списки POSIX ACL для объектов.

Взаимодействие подсистемы разграничения доступа с подсистемой аудита позволяет администратору осуществлять аудит событий, связанных с доступом к защищаемым объектам.

В работе подсистемы используется механизм дискреционного разграничения доступа, обеспечивающий управление классическими правами доступа UNIX и списками контроля доступа POSIX ACL.

В состав подсистемы входят следующие компоненты:

- механизмы разграничения прав доступа, реализованные в модуле ядра;
- CLI-утилита управления;
- GUI-утилита;
- GUI-плагин управления доступом;
- плагин сервиса управления.

Механизмы, реализованные в модуле ядра, выполняют следующие функции:

- обеспечивают взаимодействие с ядром ОС;
- перехватывают обращения к файловой системе;

- контролируют доступ субъектов к объектам на основании ACL из **xattrs** файловой системы.

CLI-утилита управления является приложением с классическим интерфейсом, предоставляющим администратору возможность выполнять все необходимые операции по управлению доступом средствами командной строки.

GUI-плагин является приложением с графическим интерфейсом.

GUI-утилита — приложение с графическим интерфейсом, предоставляющее пользователю возможность изменять права доступа к ресурсам, владельцем которых он является.

CLI-утилита управления и GUI-плагин предназначены для выполнения общих функций по управлению правами доступа:

- предоставляют информацию о правах доступа объектов файловой системы посредством чтения ACL из **xattrs** файловой системы;
- предоставляют возможность легитимного изменения правил разграничения доступа (метки в **xattrs** файловой системы);
- совместно с подсистемой аудита могут выполнять регистрацию действий по изменению правил разграничения доступа.

Подсистема разграничения доступа к устройствам

Подсистема предназначена для контроля и управления правами доступа пользователей и групп к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам.

В состав подсистемы входят:

- механизмы разграничения доступа, реализованные в модуле ядра;
- приложение — обработчик событий;
- конфигурационный компонент.

Загружаемый модуль ядра

Предназначен для выполнения следующих функций:

- встраивание в подсистему **kobject** и модификация механизмов работы ядра, связанных с отправкой событий **uevent**;
- встраивание в подсистему **vfs** и модификация механизмов работы ядра, связанных с контролем доступа субъектов (процессов) к объектам файловой системы;
- создание и поддержка интерфейсов взаимодействия с приложением пользователя для поддержки задания параметров работы, а также отображения статистики;
- регистрация событий.

Приложение — обработчик событий

Приложение выполняет следующие функции:

- обработка **uevent** событий ядра;
- выполнение специфичных для целевого устройства/подсистемы действий, связанных со сбором и получением дополнительной информации (например, серийного номера);
- выполнение специфичных для целевого устройства/подсистемы действий, связанных с оценкой необходимости запрета дальнейшего распространения данного события подписчикам (например, **udev**);
- внесение изменений в параметры, управляющие функционированием модуля ядра, если это необходимо.

Конфигурационный компонент

Компонент предназначен для управления параметрами работы подсистемы и включает в себя:

- модуль сервиса управления;

- модуль подсистемы локального управления;
- набор утилит, выполняющих базовые операции конфигурирования с использованием командного интерфейса (работа с БД, отображение информации, взаимодействие с модулем ядра и пр.).

Модуль сервиса управления представляет собой центральный элемент конфигурационного компонента и является связующим звеном между подсистемой локального управления и утилитами выполнения базовых операций конфигурирования.

Модуль подсистемы локального управления предоставляет графический интерфейс настройки параметров работы механизма разграничения доступа к устройствам.

Набор утилит включает в себя все необходимое для осуществления полноценной конфигурации, а также командную утилиту управления.

Режимы работы подсистемы

Предусмотрены три режима работы подсистемы:

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

Режим работы подсистемы задается администратором настройкой политики.

Регистрация событий

По умолчанию регистрация событий, связанных с доступом к устройствам, отключена. При необходимости администратор может включить регистрацию событий или ограничить ее только событиями с неуспешным результатом доступа.

Для каждого события, регистрируемого в журнале аудита, приводится следующая информация:

- дата и время события;
- VendorID;
- DeviceID;
- серийный номер устройства (если есть);
- метка, присвоенная устройству при его регистрации;
- результат операции подключения/отключения устройства.

Настройка регистрации событий осуществляется с помощью политики "Параметры управления устройствами".



Факт осуществления пользователем чтения или записи на устройство в журнале не регистрируется.

Подсистема контроля целостности и восстановления

Подсистема обеспечивает работу механизмов контроля целостности и предназначена для выполнения следующих функций:

- расчет контрольных сумм для файлов и каталогов, поставленных на контроль;
- проверка целостности защищаемых ресурсов;
- обновление контрольных сумм;
- анализ результатов проверки контролируемых ресурсов;
- восстановление поврежденных файлов и каталогов;
- создание хранилища для файлов и каталогов, указанных в списке восстановления;
- регистрация событий, связанных с работой механизма контроля целостности.

В состав подсистемы входят следующие компоненты:

- GUI-плагин клиента локального управления — GUI-приложение управления контролем целостности и восстановлением. Обеспечивает управление настройками подсистемы контроля целостности и восстановления средствами графического интерфейса.
- CLI-плагин клиента локального управления — CLI-приложение управления контролем целостности и восстановлением. Обеспечивает управление настройками подсистемы контроля целостности и восстановления в классическом UNIX-CLI-интерфейсе, а также запускает проверку целостности по требованию администратора.
- Системная утилита контроля целостности и восстановления. Ведет базу контроля целостности, производит проверку целостности объектов на контроле, производит восстановление объектов из эталонов при указании соответствующих настроек. Утилита используется внутри модулей Secret Net LSP и не должна запускаться администратором.
- Плагин подсистемы управления. Запускает утилиту контроля целостности и восстановления для проверки целостности стоящих на контроле файлов.

Подсистема очистки памяти

Подсистема предназначена для управления механизмом затирания остаточной информации и обеспечивает выполнение следующих функций:

- затирание освобождаемых страниц оперативной памяти;
- затирание освобождаемых блоков на файловой системе;
- безопасное удаление информации на жестких дисках и внешних носителях;
- затирание SWAP;
- включение/выключение механизма затирания на жестких дисках и внешних носителях и управление режимом его работы (синхронный/асинхронный).



Затирание освобождаемых блоков поддерживается на следующих файловых системах: EXT2, EXT3, EXT4 и VFAT.

В состав подсистемы входят:

- модуль ядра очистки оперативной памяти и затирания остаточной файловой информации;
- сервис очистки SWAP;
- CLI- и GUI-приложения для безопасного удаления на жестких дисках и внешних носителях;
- сервис асинхронного затирания остаточной информации на жестких дисках и внешних носителях.

Модули ядра перехватывают запросы на освобождение областей оперативной памяти и файловых систем соответственно и производят их затирание.

Загрузка модулей ядра осуществляется утилитами начальной инициализации при загрузке ОС и при программном останове ОС соответственно.

Сервис очистки SWAP выполняет очистку остаточной информации в разделе подкачки при выключении/перезагрузке операционной системы.

CLI- и GUI-приложения для безопасного удаления выполняют многократную перезапись содержимого файла маскирующей последовательностью перед его удалением на жестких дисках и внешних устройствах. При удалении каталога происходит рекурсивное безопасное удаление хранящихся в нем файлов. Количество проходов перезаписи содержимого удаляемых файлов задается в конфигурационном файле.

Для безопасного удаления информации на жестких дисках и внешних носителях независимо от установленного режима работы подсистемы применяются утилиты **shred** и **secrm**.

Подсистема ведения журналов

Подсистема предназначена для формирования журнала аудита и системного журнала и предоставления администратору инструментальных средств для работы с ними.

Подсистемой выполняются следующие функции:

- сбор сведений от других подсистем о зарегистрированных в них событиях;
- первичная обработка событий и хранение их в базе данных;
- формирование и отображение журнала аудита и системного журнала в табличном виде.

Подсистема предоставляет администратору следующие возможности:

- создание и хранение настраиваемых по различным критериям фильтров для формирования отчетов;
- контекстный поиск в журналах по названиям событий;
- поиск в журналах по временному интервалу;
- постраничный вывод содержимого журналов;
- сортировка отображаемой в журналах информации;
- сохранение отчетов в файл;
- интерактивный мониторинг событий.

Доступ к журналам предоставляется только администратору на основании интеграции с подсистемой идентификации и аутентификации.

Подсистема ведения журналов базируется на механизме регистрации событий и работает совместно с подсистемой аудита.

В состав подсистемы входят:

- сервис сбора и хранения журналов от всех подсистем СЗИ;
- GUI- плагин подсистемы локального управления с графическим интерфейсом, обеспечивающий работу с журналами;
- компоненты подсистемы контроля работоспособности, реализующие проверку запуска и работоспособности подсистемы ведения журналов.

Подсистема аудита

Подсистема предназначена для слежения за действиями субъектов (пользователей, процессов) и действиями с защищаемыми объектами (файлами, каталогами, сетевыми соединениями, USB-устройствами).

Слежение основано на задании правил аудита для объектов и привязки этих правил к субъектам (пользователям и группам).

Под правилом аудита понимается определенный набор операций, выполняемых с объектами, и привязка этих операций к субъектам (пользователям и группам).

К операциям, выполняемым с объектами, относятся:

- запрос сведений о файле/каталоге;
- изменение атрибутов файла/каталога;
- переименование файла/каталога;
- удаление файла/каталога;
- создание файла/каталога;
- запуск программы;
- чтение файла/каталога;
- открытие файла/каталога на запись.

Для ведения аудита сетевой активности пользователей и групп используются правила, включающие в себя следующие операции:

- создание сокета;
- прием/передача датаграмм;

- установление сетевого соединения.

Подсистема аудита предоставляет администратору возможность добавлять в систему новые правила, удалять их и редактировать.

На основании заданных администратором правил средствами подсистемы ведения журналов формируется журнал аудита.

В состав подсистемы аудита входят:

- GUI-плагин подсистемы локального управления — приложение с графическим интерфейсом для управления правилами слежения за объектами и субъектами системы;
- CLI-приложение с классическим UNIX-интерфейсом для управления правилами слежения за объектами и субъектами системы из командной строки;
- модуль ядра аудита, реализующий все необходимые функции для обеспечения сервиса аудита;
- сервис аудита;
- плагины подсистемы контроля работоспособности, реализующие проверку запуска и работоспособности сервиса аудита.

Функции администратора

Функциональные возможности системы позволяют администратору решать следующие задачи:

- управлять пользователями и группами;
- контролировать вход пользователей в систему;
- разграничивать доступ пользователей к информационным ресурсам на основе принципа дискреционного разграничения доступа;
- контролировать целостность ресурсов;
- контролировать вывод информации на печать;
- надежно скрывать информацию, содержащуюся в удаленных файлах, предотвращая ее восстановление;
- управлять доступом пользователей к USB-устройствам;
- осуществлять контроль действий пользователей в системе.

В процессе эксплуатации СЗИ Secret Net LSP основными функциями администратора являются:

- установка и обновление программного обеспечения СЗИ;
- настройка механизмов защиты, гарантирующая требуемый уровень безопасности ресурсов компьютеров;
- контроль действий пользователей, связанных с нарушением информационной безопасности;
- контроль работоспособности СЗИ и ее восстановление в аварийных ситуациях.

Требования к аппаратным и программным средствам

Secret Net LSP (номер текущей версии — 1.5) устанавливается на компьютеры, удовлетворяющие приведенным в следующей таблице системным требованиям.

Операционная система	<ul style="list-style-type: none"> • ALT Linux 7.0.5 Centaurus x86/x64 (версия ядра 3.14.41-std-def-alt1); • CentOS 7.1 x64 (версия ядра 3.10.0-229, 3.14.51-grsec); • CentOS 6.5 x86/x64 (версия ядра 2.6.32-431); • ContinentOS 4.2 x64 (версия ядра 3.14.22); • Debian 8.0 (версия ядра 3.16.0-4-amd64); • Debian 7.6 x86/x64 (версия ядра 3.2.0-4-686-pae/3.2.0-4-amd64); • Red Hat Enterprise Linux 7.2 (версия ядра 3.10.0-327); • Red Hat Enterprise Linux 7.0 (версия ядра 3.10.0-123); • Red Hat Enterprise Linux 6.5 x86/x64 (версия ядра 2.6.32-431); • Red Hat Enterprise Linux 6.3 x86/x64 (версия ядра 2.6.32-279); • Red Hat Enterprise Linux 5.8 x86/x64 (версия ядра 2.6.18-308); • Red Hat Enterprise Linux 5.5 x86/x64 (версия ядра 2.6.18-194); • Red Hat Enterprise Linux 5.2 x86/x64 (версия ядра 2.6.18-92)
Процессор	В соответствии с требованиями операционной системы, установленной на компьютер
Оперативная память	Минимально – 512 МБ
Жесткий диск (свободное пространство)	Минимально – 600 МБ для раздела, в котором находится каталог /opt

Глава 2

Установка, удаление и обновление

Архивы дистрибутива Secret Net LSP (DEB- и RPM-пакеты) и плагина виртуальных каналов Citrix (RPM-пакеты) поставляются на установочном компакт-диске в соответствующих каталогах:

Каталог	Содержимое
x86_64	Установочные пакеты (RPM, DEB) для архитектуры x64
i686	Установочные пакеты (RPM, DEB) для архитектуры x86
Citrix_token	Установочные пакеты для плагина виртуальных каналов Citrix

Плагин `citrix_token_auth` необходим для передачи данных из персональных идентификаторов Rutooken S/S RF/S micro/ЭЦП/ЭЦП Flash на терминальный сервер на базе ПО Citrix (XenApp и XenDesktop) с установленным СЗИ Secret Net 7, что позволяет выполнять с их помощью аутентификацию на терминальном сервере.

Процедуры установки, обновления и удаления Secret Net LSP выполняются администратором, обладающим правами суперпользователя компьютера, с использованием командной строки эмулятора терминала.

Перед началом установки программного обеспечения (ПО) на компьютер необходимо убедиться в выполнении следующих требований:

- На компьютере установлена только одна поддерживаемая операционная система с одним ядром.
- Ядро операционной системы должно входить в список ядер, заявленных как поддерживаемые компанией — разработчиком СЗИ, и соответствовать устанавливаемому дистрибутиву Secret Net LSP.

Установка

Перед началом установки ПО проверьте выполнение требований к аппаратному и программному обеспечению компьютера (см. стр.[22](#)).



Рекомендуется перед началом установки отключить хранитель экрана и выполнить процедуру установки от начала до конца без перерыва. Так как процедура установки включает в себя замену RAM-модуля, в некоторых операционных системах при установке требуется смена паролей пользователей.

Установка ПО Secret Net LSP в зависимости от используемой операционной системы осуществляется с помощью установочных RPM- и DEB-пакетов:

- `sn-lsp-1.5.xxx-i686.rpm`, `sn-lsp-1.5.xxx-x86_64.rpm` — в среде ОС CentOS 6.5/7.1, ContinentOS 4.2, Red Hat Enterprise Linux 5.2/5.5/5.8/6.3/6.5/7.0/7.5, ALT Linux 7.0.5;
- `sn-lsp-1.5.xxx-i686.deb`, `sn-lsp-1.5.xxx-x86_64.deb` — в среде ОС Debian 7.6/8.0.

Установка плагина виртуальных каналов Citrix осуществляется с помощью RPM-пакетов `citrix_token_auth-1.0-5.el6.i386.rpm`, `citrix_token_auth-1.0-5.el6.x86_64.rpm`, `opencsc-secretnet-0.12.2-3.el6.i386.rpm`.

Для установки ПО Secret Net LSP:

1. Вставьте установочный компакт-диск Secret Net LSP в привод DVD/CD-ROM. Запустите программу эмулятора терминала.

Внимание! Для корректной установки Secret Net LSP в операционной системе Debian 8.0/7.6 необходимо выполнить следующие команды:

```
#sudo apt-get update
```

```
#sudo apt-get install ntp, ntpdate, openssh-server
```

2. Войдите в каталог установки программы для соответствующего дистрибутива Linux. В зависимости от используемого дистрибутива выполните команды:

- для RPM-пакетов:

- для системы с 32-разрядной архитектурой:

```
#rpm -ivh sn-lsp-1.5.xxx-i686.rpm
```

- для системы с 64-разрядной архитектурой:

```
#rpm -ivh sn-lsp-1.5.xxx-x86_64.rpm
```

- для DEB-пакетов:

- для системы с 32-разрядной архитектурой:

```
#dpkg -i sn-lsp-1.5.xxx-i686.deb
```

- для системы с 64-разрядной архитектурой:

```
#dpkg -i sn-lsp-1.5.xxx-x86_64.deb
```

Результатом выполнения процедуры является установка на защищаемом компьютере ПО Secret Net LSP.

3. Перезагрузите компьютер.

После перезагрузки на компьютере будет отключена мандатная система контроля доступа (SELinux, Apparmor, Tomoyo Linux, RSBAC и пр.).

4. Если на компьютере установлен программно-аппаратный комплекс "Соболь", необходимо выполнить переинициализацию шаблонов контроля целостности для каталога /boot/grub.



Программа установки прописывает в конфигурацию загрузки параметр "security=default". Не изменяйте этот параметр. В противном случае вход в систему для обычных пользователей будет заблокирован.

В Secret Net LSP предусмотрено 2 варианта использования механизма затирания остаточной информации: автоматическое затирание в фоновом режиме, реализованное на уровне ядра, и ручной запуск утилиты затирания **shred** (безопасное удаление). По умолчанию после установки в Secret Net LSP автоматическое затирание выключено, так как использование этого механизма приводит к повышенной нагрузке на файловую систему и жесткие диски. Если необходимо, чтобы на компьютере было включено автоматическое затирание, после перезагрузки выполните следующее:

1. Включите автоматическое затирание с помощью параметра "Сервис безопасного удаления" политики "Установки сервисов" (см. стр.[69](#)).
2. Задайте нужный режим работы механизма затирания (см. стр.[70](#)).

Подробнее о затирании остаточной информации см. стр.[13](#), стр.[19](#), стр.[69](#).

Для установки плагина виртуальных каналов Citrix:

1. Выполните вход в систему под учетной записью root.
2. Скопируйте на компьютер из каталога Citrix_token на установочном компакт-диске следующие пакеты:
 - для системы с 32-разрядной архитектурой:
 - opensc-secretnet-0.12.2-3.el6.i386.rpm;
 - citrix_token_auth-1.0-5.el6.i386.rpm;
 - для системы с 64-разрядной архитектурой:

- opensc-secretnet-0.12.2-3.el6.i386.rpm;
 - citrix_token_auth-1.0-5.el6.x86_64.rpm.
- 3.** Установите дополнительные пакеты и удалите pcsc-lite. Для этого в командной оболочке последовательно выполните команды:

```
#yum install zlib.i686 openct.i686
#yum remove pcsc-lite
```

- 4.** Установите пакет opensc-secretnet. Для этого в командной оболочке выполните команду:

```
#rpm -Uhv opensc-secretnet-0.12.2-3.el6.i386.rpm
```

- 5.** Установите пакет citrix_token_auth. Для этого в командной оболочке выполните следующую команду.

Для системы с 32-разрядной архитектурой:

```
#rpm -Uhv citrix_token_auth-1.0-5.el6.i386.rpm
```

Для системы с 64-разрядной архитектурой:

```
#rpm -Uhv citrix_token_auth-1.0-5.el6.x86_64.rpm
```

Установленные модули плагина размещаются в каталоге /opt/Citrix/ICAClient/.

Внимание! При установке плагина в конфигурационные файлы Citrix Receiver добавляются нужные настройки. Если ПО Citrix Receiver еще не установлено, то для работы плагина в файл /opt/Citrix/ICAClient/config/module.ini необходимо вручную добавить следующие строки (выделены жирным шрифтом):

[ICA 3.0]

SNToken=On

VirtualDriver = **SNToken**, Thinwire3.0, Clipboard, ClientDrive, ClientPrinterQueue, ClientAudio, ClientComm, FlashV2, TWI, ZL_FONT, ZLC, ICACTL, SmartCard, UserExperience, MultiMedia

[**SNToken**]

DriverName=sntoken.dll

Удаление

Удаление Secret Net LSP выполняет администратор, который должен обладать правами суперпользователя компьютера.



При удалении Secret Net LSP в операционной системе сохраняется каталог /opt/secretnet-archive с файлами журналов установки/удаления СЗИ. Если после удаления Secret Net LSP эта информация больше не нужна, каталог и его содержимое можно удалить вручную. Перед повторной установкой Secret Net LSP каталог и его содержимое должны быть обязательно удалены.

Для удаления программного обеспечения:

1. Вставьте установочный компакт-диск Secret Net LSP в привод DVD/CD-ROM. Запустите программу эмулятора терминала.
2. Войдите в каталог установки программы для соответствующего дистрибутива Linux. В зависимости от используемого дистрибутива выполните команды:

- для RPM-пакетов:

- для системы с 32-разрядной архитектурой:

```
#rpm -e sn-lsp-1.5.***-i686.rpm
```

- для системы с 64-разрядной архитектурой:

```
#rpm -e sn-lsp-1.5.***-x86_64.rpm
```

- для DEB-пакетов:

- для системы с 32-разрядной архитектурой:

```
#dpkg -r sn-lsp-1.5.***-i686.deb
```

- для системы с 64-разрядной архитектурой:

```
#dpkg -r sn-lsp-1.5.xxx-x86_64.deb
```

- 3.** Перезагрузите компьютер.

Результатом выполнения процедуры является удаление ПО Secret Net LSP.

Обновление

В СЗИ Secret Net LSP реализована возможность обновления программного обеспечения предыдущей версии на текущую (с версии 1.4 на 1.5) с сохранением действующих настроек.

Для обновления ПО:

- 1.** Вставьте установочный компакт-диск Secret Net LSP в привод DVD/CD-ROM. Запустите программу эмулятора терминала.
- 2.** Войдите в каталог установки программы для соответствующего дистрибутива Linux. В зависимости от используемого дистрибутива выполните команды:
 - для системы с 32-разрядной архитектурой:

```
#!/bin/sh
#./upgrade-1.4_to_1.5.sh sn-lsp-1.5.xxx-i686.rpm
```

Примечание. Для обновления ПО с версии 1.3 на 1.5 выполните команду

```
#!/bin/sh
#./upgrade-1.3_to_1.5.sh sn-lsp-1.5.315-i686.rpm
```

Для обновления ПО с версии 1.4 на 1.5 в среде ОС Debian с сохранением настроек Secret Net LSP необходимо сначала вызвать скрипт

```
#!/bin/sh
./pre_upgrade.sh
```

затем выполнить команду

```
#!/bin/sh
#dpkg -i sn-lsp-1.5.315-i686.rpm
```

- для системы с 64-разрядной архитектурой:

```
#!/bin/sh
#./upgrade-1.4_to_1.5.sh sn-lsp-1.5.xxx-x86_64.rpm
```

Примечание. Для обновления ПО с версии 1.3 на 1.5 выполните команду

```
#!/bin/sh
#./upgrade-1.3_to_1.5.sh sn-lsp-1.5.315-x86_64.rpm
```

Для обновления ПО с версии 1.4 на 1.5 в среде ОС Debian с сохранением настроек Secret Net LSP необходимо сначала вызвать скрипт

```
#!/bin/sh
./pre_upgrade.sh
```

затем выполнить команду

```
#!/bin/sh
#dpkg -i sn-lsp-1.5.315-x86_64.rpm
```

- 3.** Перезагрузите компьютер.

Глава 3

Первая загрузка

После установки программного обеспечения и перезагрузки компьютера администратор должен войти в систему и выполнить начальные настройки.

Первый вход в систему администратор выполняет под учетной записью root.

Начальные настройки включают в себя смену паролей пользователей, зарегистрированных на компьютере (см. стр. 34). Смена рекомендуется в поддерживаемых операционных системах.

Перед началом выполнения настроек следует ознакомиться с содержанием следующего раздела, в котором описано приложение "Панель безопасности Secret Net LSP" (далее — панель безопасности).

Кроме начальных настроек при первом входе администратора в систему рекомендуется просмотреть и при необходимости изменить настройки, установленные по умолчанию (см. стр. 30), а также ознакомиться с порядком работы с журналами (см. стр. 33).

Инструментальные средства администратора

При первом входе в систему администратору становятся доступными инструментальные средства, с помощью которых он может сразу приступить к контролю работы подсистем Secret Net LSP и настройке защитных механизмов. Такими средствами являются:

- Панель безопасности Secret Net LSP.
- Интерфейс командной строки.

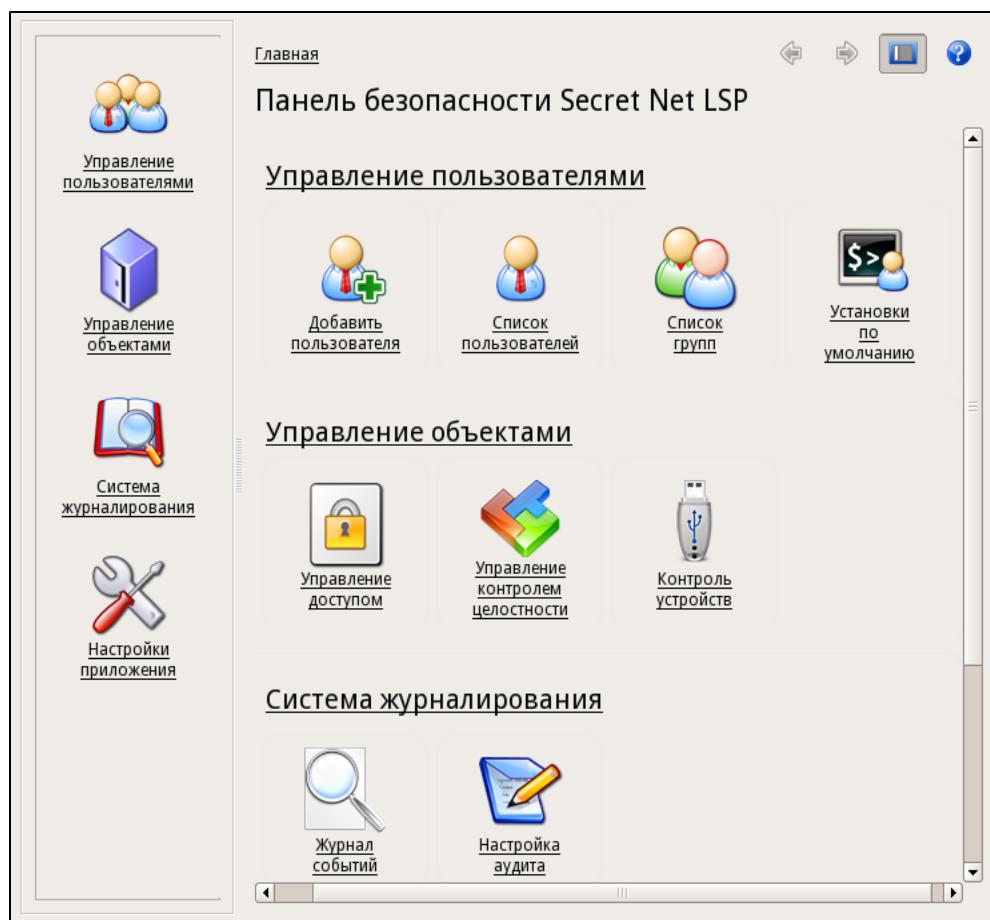
Панель безопасности — приложение с графическим интерфейсом, обеспечивающее выполнение администратором всех необходимых операций в рамках контроля и управления работой защитных механизмов.

Интерфейс командной строки — классический вариант работы в ОС Linux в режиме командной строки, являющийся альтернативным по отношению к использованию графического интерфейса панели управления.

Описание панели безопасности

Вызовите панель безопасности стандартным способом с помощью ярлыка Secret Net LSP на рабочем столе.

На экране появится окно "Панель безопасности Secret Net LSP":



Центральную часть панели безопасности занимает иерархическое меню, расположенное на главной странице и оформленное в виде групп ссылок, каждая из которых включает в себя ссылки с пиктограммами.

Ссылка группы обеспечивает переход на следующую страницу, на которой расположены ссылки с пиктограммами, входящие в группу.

Ссылка с пиктограммой обеспечивает прямой переход на страницу выполнения тех или иных операций.

Описание ссылок с пиктограммами и доступных операций приведено в таблице ниже.

Ссылка, пиктограмма	Описание
	Регистрация в системе нового пользователя и задание его параметров. Включение пользователя в группу (группы). Изменение параметров пароля пользователя, заданных по умолчанию
	Просмотр списка пользователей. Создание нового пользователя. Удаление пользователя. Добавление выбранного пользователя в группы. Изменение атрибутов выбранного пользователя. Разблокирование пользователя
	Просмотр списка групп. Переименование выбранной группы. Редактирование списка пользователей в выбранной группе. Удаление выбранной группы

Ссылка, пиктограмма	Описание
Установки по умолчанию 	Просмотр и изменение параметров учетной записи новых пользователей, устанавливаемых по умолчанию: <ul style="list-style-type: none"> Оболочка; Шаблон домашнего каталога; Создание личной группы пользователя; Создание домашнего каталога
Управление доступом 	Настройка правил разграничения доступа к объектам файловой системы
Управление контролем целостности 	Постановка на контроль и снятие с контроля защищаемых ресурсов файловой системы
Контроль устройств 	Настройка правил разграничения доступа к USB-устройствам
Журнал событий 	Работа с системным журналом и журналом аудита
Настройка аудита 	Настройка подсистемы аудита
Помощь 	Вызов справочной системы
Политики 	Просмотр и настройка политик
Управление лицензией 	Ввод серийного номера при переходе с демонстрационной версии на лицензионную
Настройки удаленного управления 	Настройка параметров подключения к серверу безопасности СЗИ Secret Net 7

При переходе на какую-либо страницу в верхней части панели безопасности отображается строка навигации, индицирующая положение текущей страницы в общей структуре меню. Для возврата на предыдущие страницы используйте ссылки строки навигации или ссылки "Назад" и "Вперед", расположенные в правом верхнем углу.

В левой части панели безопасности расположена панель переходов. Расположенные на ней ссылки позволяют осуществлять быстрый переход к пунктам меню, пропуская промежуточные страницы.

Ссылка, пиктограмма	Описание
Управление пользователями 	Переход на страницу с ссылками: <ul style="list-style-type: none"> Добавить пользователя; Список пользователей; Список групп; Установки по умолчанию
Управление объектами 	Переход на страницу с ссылками: <ul style="list-style-type: none"> Управление доступом; Управление контролем целостности; Контроль устройств
Система журналирования 	Переход на страницу с ссылками: <ul style="list-style-type: none"> Журнал событий; Настройка аудита
Настройки приложения 	Переход на страницу с ссылками: <ul style="list-style-type: none"> Помощь; Политики; Управление лицензией; Настройки удаленного управления

Панель переходов можно скрыть или восстановить. Для скрытия или восстановления панели переходов соответственно отожмите или нажмите кнопку  , расположенную в правом верхнем углу.

Начало работы

При первой загрузке операционной системы, защищаемой СЗИ Secret Net LSP, вступают в действие защитные механизмы. При этом действуют настройки, установленные по умолчанию.

После входа в систему администратор может просмотреть и при необходимости изменить настройки по умолчанию, а также ознакомиться с журналами, в которых были зарегистрированы события, связанные со входом администратора в систему.

Настройки по умолчанию

К настройкам по умолчанию относятся параметры учетных записей пользователей, добавляемых в систему средствами Secret Net LSP, и параметры политик. Значения параметров задаются при установке Secret Net LSP и могут быть изменены администратором.

Параметры учетных записей

К параметрам учетных записей пользователей, добавляемых в систему, относятся:

- оболочка;
- шаблон домашнего каталога;
- создание личной группы пользователя;
- создание группы по умолчанию;
- создание домашнего каталога.

Для просмотра/изменения параметров учетных записей:

- 1.** Вызовите панель безопасности (см. стр. 27) и в группе "Управление пользователями" перейдите на страницу "Установки по умолчанию".

Будет выполнен переход на соответствующую страницу:

- 2.** При необходимости измените значения параметров:

Поле	Описание
Оболочка	Выберите оболочку из раскрывающегося списка
Шаблон домашнего каталога	Введите вручную шаблон
Создавать личную группу пользователя	Для создания личной группы пользователя установите отметку. Имя личной группы будет соответствовать имени пользователя. Если создание личной группы пользователя не требуется, удалите отметку
Группа по умолчанию	Поле доступно, если не создается личная группа пользователя. Выберите из раскрывающегося списка группу. Если поле оставлено незаполненным, новый пользователь будет автоматически включен в виртуальную группу Users
Создавать домашний каталог	Установите отметку, если требуется автоматическое создание домашнего каталога пользователя. Если создание домашнего каталога не требуется, удалите отметку

- 3.** Для сохранения внесенных изменений нажмите кнопку "Применить".

Для отмены выполненных изменений нажмите кнопку "Отменить".

Для возврата на предыдущую страницу нажмите соответствующую ссылку в строке навигации.

Политики

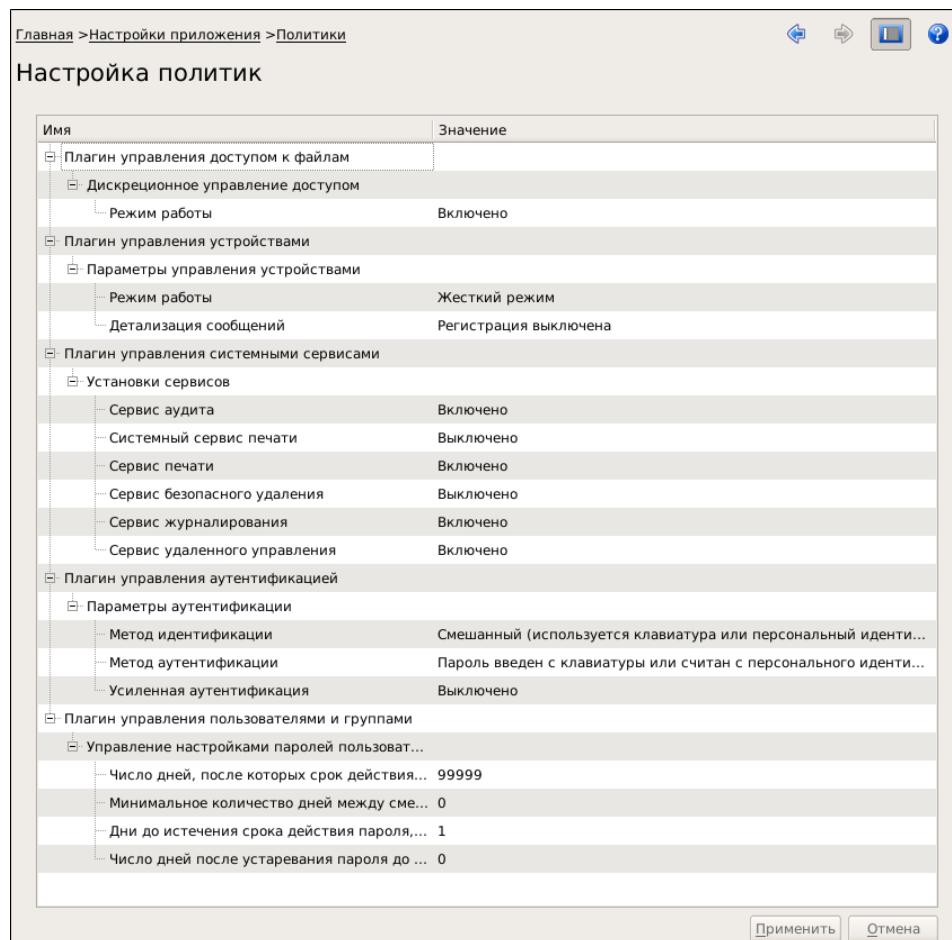
С помощью политик осуществляются следующие настройки СЗИ:

- управление режимом работы подсистемы разграничения доступа к устройствам;
- включение/выключение системных сервисов;
- управление режимом входа в систему;
- настройки параметров паролей, назначаемых новым пользователям по умолчанию.

Настройки выполняются изменением параметров политик.

Для просмотра/изменения параметров политик:

- Вызовите панель безопасности (см. стр. 27) и в группе "Настройки приложения" перейдите на страницу "Настройка политик":



На странице отображаются политики и значения их параметров.

Политика	Описание
Дискреционное управление доступом	Управление режимом работы подсистемы дискреционного управления доступом
Параметры управления устройствами	Управление режимом работы подсистемы разграничения доступа к устройствам и настройка регистрации событий в журнале аудита
Установки сервисов	Включение/выключение системных сервисов
Параметры аутентификации	Задание режима входа пользователей в систему
Управление настройками паролей пользователей и групп	Настройка параметров паролей, назначаемых новым пользователям по умолчанию

Политика "Дискреционное управление доступом" управляет функционированием подсистемы разграничения доступа к объектам файловой системы.

Политика "Параметры управления устройствами" описывается двумя параметрами:

Параметр	Описание
Режим работы	Задание режима работы подсистемы разграничения доступа пользователей к устройствам: отключено, мягкий, жесткий (см. стр. 17 , стр. 64). Значение по умолчанию: "Жесткий режим"
Детализация сообщений	Настройка регистрации событий в журнале аудита (см. стр. 64)

Политика "Установки сервисов" включает в себя параметры, управляющие включением/выключением соответствующего системного сервиса.

Параметр	Описание
Сервис аудита	Включает/выключает аудит. Значение по умолчанию: "Включено"
Системный сервис печати	Включает/выключает системный сервис печати (UNIX). Значение по умолчанию: "Выключено"
Сервис печати	Включает/выключает сервис печати Secret Net LSP. Значение по умолчанию: "Включено"
Сервис безопасного удаления	Включает/выключает сервис безопасного удаления на уровне ядра. Значение по умолчанию: "Выключено"
Сервис журналирования	Включает/выключает регистрацию событий в системном журнале и журнале аудита
Сервис удаленного управления	Включает/выключает сервис удаленного управления СЗИ Secret Net LSP посредством сервера безопасности СЗИ Secret Net 7. Значение по умолчанию: "Выключено"

Политика "Параметры аутентификации" задает режимы идентификации и аутентификации.

Политика "Управление настройками паролей пользователей и групп" включает в себя следующие параметры:

- число дней, после которых срок действия пароля истекает;
- минимальное количество дней между сменами пароля;
- дни до истечения срока действия пароля, когда пользователь будет предупрежден;
- число дней после устаревания пароля до его блокировки.

Параметры со значениями, отличными от значений по умолчанию, выделены жирным шрифтом.

2. Для изменения политики выберите нужный параметр, активируйте поле "Значение" и выберите нужное значение из раскрывающегося списка.
3. Для сохранения изменений нажмите кнопку "Применить".

Просмотр журналов

При первом входе в систему администратор может просмотреть результаты работы механизма регистрации событий и подсистемы ведения журналов. В частности, администратор может просмотреть события, зарегистрированные подсистемами контроля целостности, идентификации и аутентификации в журналах событий и аудита.

Для просмотра журналов:

- Вызовите панель управления безопасностью (см. стр.[27](#)) и в группе "Система журналирования" перейдите на страницу "Журнал событий".

Будет выполнен переход на страницу "Журнал событий".

На странице на вкладках "Система" и "Аудит" представлено содержимое системного журнала и журнала аудита соответственно.

Описание журналов и порядок работы с ними приводится в главе 10 (см. стр.[75](#)).

Смена паролей пользователей

При первом входе в систему рекомендуется сменить пароли всех пользователей, зарегистрированных на компьютере.

Смена паролей пользователей может выполняться администратором как средствами панели управления, так и в режиме командной строки.



Смена паролей в режиме командной строки выполняется стандартными UNIX-командами, поставляемыми в составе Secret Net LSP.

Смена паролей средствами панели управления

Для смены паролей пользователей:

1. Вызовите панель управления безопасностью (см. стр.27) и в группе "Управление пользователями" перейдите на страницу "Список пользователей".
2. Выберите пользователя и в контекстном меню выберите команду "Редактировать".

Будет выполнен переход на страницу "Редактирование пользовательских атрибутов":

Главная > Управление пользователями > Просмотр списка пользователей > Редактирование пользовательских атрибутов

Редактирование пользовательских атрибутов

Имя пользователя:	ppagin *	Изменить пароль								
Главная группа:	ppagin	Параметры входа								
Полное имя:		Персональные идентификаторы								
Оболочка:	/bin/bash									
Домашний каталог:	/home/ppagin									
<input type="checkbox"/> Блокировать пользоват										
Группы пользователя										
<table border="1"> <thead> <tr> <th>Имя</th> </tr> </thead> <tbody> <tr><td>camera</td></tr> <tr><td>vmusers</td></tr> <tr><td>conshelp</td></tr> <tr><td>backupadmin</td></tr> <tr><td><input checked="" type="checkbox"/> ppagin</td></tr> <tr><td>vboxsf</td></tr> <tr><td>snlogger</td></tr> </tbody> </table>			Имя	camera	vmusers	conshelp	backupadmin	<input checked="" type="checkbox"/> ppagin	vboxsf	snlogger
Имя										
camera										
vmusers										
conshelp										
backupadmin										
<input checked="" type="checkbox"/> ppagin										
vboxsf										
snlogger										
<input type="button" value="Применить"/> <input type="button" value="Отменить"/>										

3. Для изменения пароля нажмите кнопку "Изменить пароль".

Появится окно "Изменение пароля":

Изменение пароля

Пароль:	<input type="text"/>
Повторите пароль:	<input type="text"/>
<input type="button" value="Применить"/> <input type="button" value="Отменить"/>	

Введите новый пароль пользователя, повторите ввод и нажмите кнопку "Применить".

Будет выполнен возврат на страницу редактирования пользовательских атрибутов.

4. На странице редактирования пользовательских атрибутов нажмите кнопку "Применить".
Будет выполнен возврат на страницу "Список пользователей".
5. Выберите следующего пользователя и задайте ему пароль, как описано выше (см. пп. 2—4).
Выполните смену паролей для всех пользователей.

Глава 4

Управление пользователями

В рамках управления пользователями администратор может выполнять следующие действия:

- добавлять/удалять пользователей системы;
- изменять атрибуты пользователей;
- добавлять/удалять группы пользователей;
- изменять атрибуты групп;
- включать/исключать пользователей из группы;
- задавать/изменять пароли и атрибуты паролей пользователей;
- изменять настройки по умолчанию для паролей новых пользователей;
- блокировать и разблокировать учетные записи пользователей.

Просмотр списка пользователей

Для просмотра списка пользователей:

- Вызовите панель безопасности и в группе "Управление пользователями" нажмите ссылку "Список пользователей".

Будет выполнен переход на страницу "Список пользователей":

The screenshot shows a window titled 'Список пользователей' (User List). At the top, there is a breadcrumb navigation: Главная > Управление пользователями > Просмотр списка пользователей. Below the title, there is a table with the following columns: Имя (Name), Полное имя (Full Name), Домашний каталог (Home Directory), Оболочка (Shell), and Главная группа (Primary Group). The table lists various system users, such as mysql, named, news, nfsuser, nobody, nsqd, ntpd, openvpn, osec, popa3d, postfix, postgres, postman, ppagin, root, rpc, rpcuser, squid, sshd, and sysload. The user 'ppagin' is currently selected, as indicated by a dark gray background. At the bottom of the window, there are four buttons: 'Создать пользователя' (Create User), 'Редактировать' (Edit), 'Удалить' (Delete), and 'Закрыть' (Close).

Имя	Полное имя	Домашний каталог	Оболочка	Главная группа
mysql	MySQL server	/var/lib/mysql	/dev/null	mysql
named	Bind User	/var/lib/named	/dev/null	named
news	news	/var/spool/news	/dev/null	news
nfsuser	NFS Service User	/dev/null	/dev/null	nfsuser
nobody	Nobody	/var/nobody	/dev/null	nobody
nsqd	NSCD Daemon	/	/dev/null	nsqd
ntpd	OpenNTP dae...	/var/empty	/dev/null	ntpd
openvpn	OpenVPN dae...	/dev/null	/dev/null	openvpn
osec		/dev/null	/dev/null	osec
popa3d	POP3 daemon	/dev/null	/dev/null	popa3d
postfix	Postfix Mail Tr...	/var/spool/pos...	/dev/null	postfix
postgres	PostgreSQL Se...	/var/lib/pgsql	/dev/null	postgres
postman	postman	/dev/null	/dev/null	postman
ppagin		/home/ppagin	/bin/bash	ppagin
root	System Admini...	/root	/bin/bash	root
rpc	Portmapper R...	/	/dev/null	rpc
rpcuser	RPC Service User	/var/lib/nfs	/dev/null	rpcuser
squid	Squid User	/var/spool/squid	/dev/null	squid
sshd		/var/empty	/dev/null	sshd
sysload		/dev/null	/dev/null	sysload

Для каждого пользователя в списке приводится следующая информация:

- имя;
- полное имя;
- домашний каталог;
- оболочка;

- главная группа.

Для добавления в список нового пользователя нажмите кнопку "Создать пользователя" в правом нижнем углу страницы.

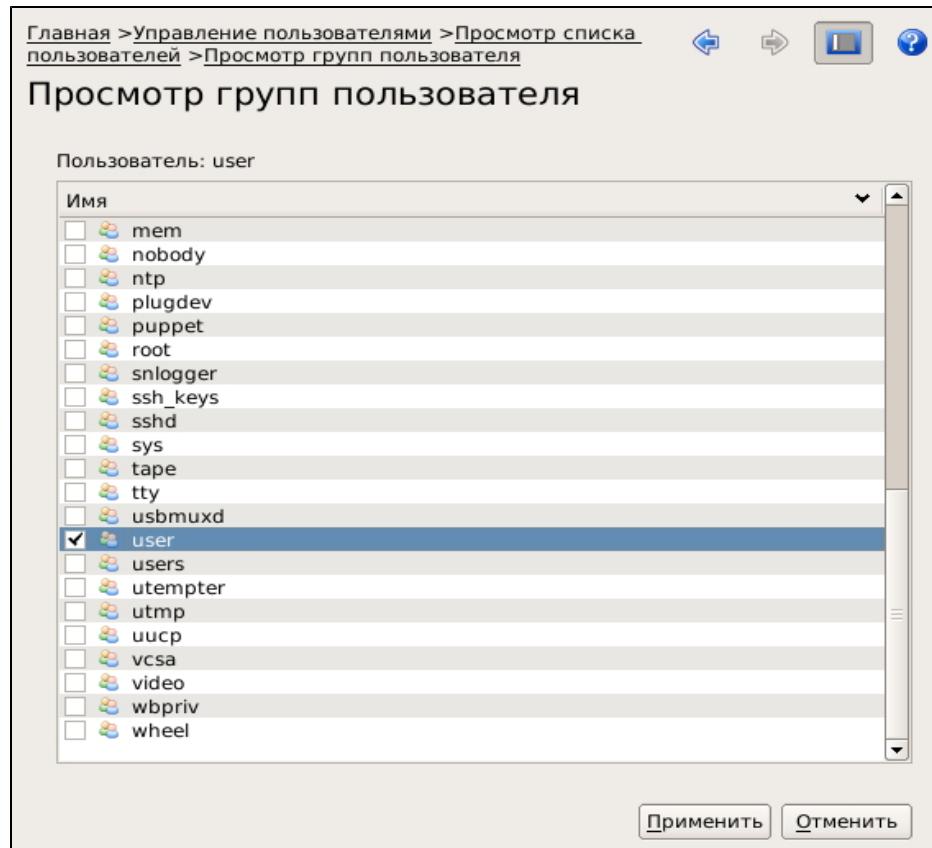
Для каждого выбранного в списке пользователя с помощью контекстного меню можно выполнить следующие операции:

- добавить пользователя в группы (см. стр.[43](#));
- создать нового пользователя (см. стр.[39](#));
- изменить атрибуты пользователя (см. стр.[40](#));
- блокировать/разблокировать учетную запись пользователя (см. стр.[43](#));
- просмотреть перечень персональных идентификаторов пользователя (см. стр.[46](#));
- удалить пользователя из списка (см. стр.[39](#)).

Для просмотра групп, в которые входит выбранный пользователь:

- Вызовите контекстное меню и выберите команду "Добавить в группы" или "Изменить".

Будет выполнен переход на страницу "Просмотр групп пользователя" или "Редактирование пользовательских атрибутов" соответственно, на которых отображается общий список групп:



В списке отмечены группы, в которые входит пользователь.

- Для включения или исключения пользователя из группы установите или удалите отметку соответственно и нажмите кнопку "Применить".

Просмотр списка групп пользователей

Для просмотра списка групп:

- Вызовите панель управления безопасностью и в группе "Управление пользователями" нажмите ссылку "Список групп".

Будет выполнен переход на страницу "Список групп":

Главная >Управление пользователями >Просмотр списка групп

Список групп

Имя
root
bin
daemon
sys
adm
tty
disk
lp
mem
kmem
wheel
firewall
...

Создать группу | Переименовать группу | Члены группы | Удалить группу | Закрыть

Для каждой выбранной в списке группы с помощью команд контекстного меню или кнопок, расположенных в нижней части страницы, можно выполнить следующие операции:

- создать новую группу (см. стр.42);
 - переименовать группу (см. стр.42);
 - редактировать список пользователей группы (см. стр.43);
 - удалить группу (см. стр.42).
2. Для просмотра списка пользователей, входящих в группу, выберите в списке группу и нажмите кнопку "Члены группы".

Будет выполнен переход на страницу "Список пользователей группы":

Главная >Управление пользователями >Просмотр списка групп >Список пользователей группы

Список пользователей группы

Пользователи в группе: ppagin

Имя	Полное имя	Домашний каталог	Оболочка	Главная группа
sshd	/var/empty	/dev/null	sshd	
openvpn	OpenVPN dae...	/dev/null	/dev/null	openvpn
_avahi	Avahi service	/var/run/avahi-...	/dev/null	_avahi
ntpd	OpenNTP dae...	/var/empty	/dev/null	ntpd
tcpdump		/dev/null	/dev/null	tcpdump
postman	postman	/dev/null	/dev/null	postman
bacula	Bacula pseudo...	/var/empty	/bin/false	bacula
_libvirt	libvirt user	/var/lib/libvirt	/bin/false	vmusers
<input checked="" type="checkbox"/> ppagin		/home/ppagin	/bin/bash	ppagin
vboxadd		/var/run/vboxa...	/bin/false	bin

Установить список пользователей | Отменить

В списке пользователи, включенные в состав группы, отмечены галочкой слева от имени пользователя.

- Для включения или исключения пользователя из группы установите или удалите отметку соответственно и нажмите кнопку "Установить список пользователей".

Добавление и удаление пользователей

Для добавления пользователя:

1. Вызовите панель безопасности и в группе "Управление пользователями" нажмите ссылку "Добавить пользователя".

Будет выполнен переход на страницу "Добавить пользователя":

Главная > Управление пользователями > Добавить пользователя

Добавить пользователя

Имя пользователя: *

Пароль: *

Подтверждение: *

Главная группа: Параметры входа

Полное имя:

Оболочка: *

Домашний каталог: /home/%u

Блокировать пользователя

Группы пользователя

Имя
<input type="checkbox"/> root
<input type="checkbox"/> bin
<input type="checkbox"/> daemon
<input type="checkbox"/> svs

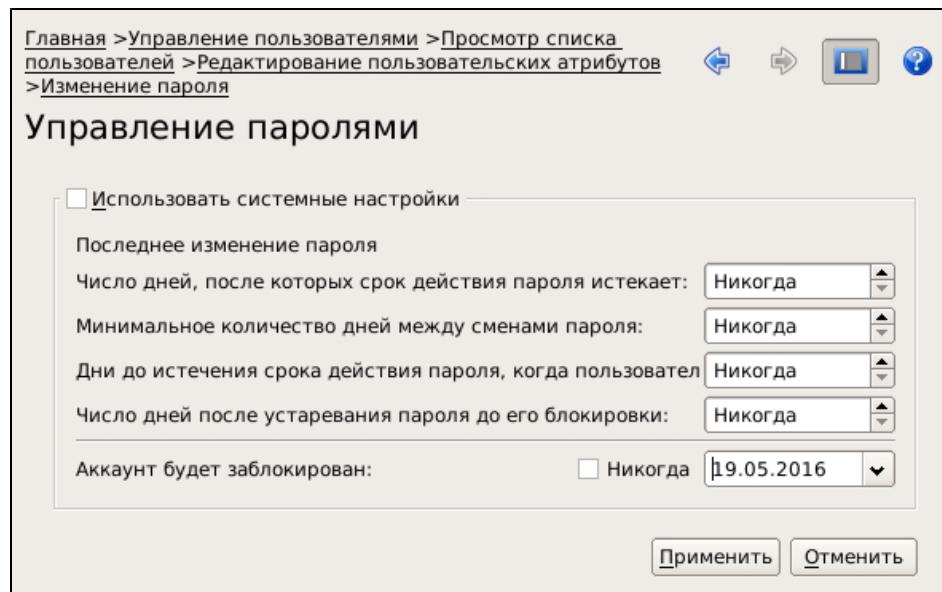
Применить Отменить

2. Заполните поля атрибутов пользователя.

Поля, отмеченные звездочкой, являются обязательными для заполнения. Поля "Главная группа" и "Оболочка" выбираются из списка. Поле "Блокировать пользователя" доступно только после добавления пользователя в список.

3. Для изменения параметров пароля, задаваемых по умолчанию, нажмите кнопку "Управление паролем".

Будет выполнен переход на страницу "Управление паролями":



- 4.** Если необходимо изменить параметры пароля, задаваемые по умолчанию, укажите нужные значения.

Если необходимо оставить значения параметров, задаваемые по умолчанию, установите отметку в поле "Использовать системные настройки".

Нажмите кнопку "Применить".

Будет выполнен возврат на страницу "Добавить пользователя".

- 5.** Установите отметки в группах, в которые должен быть включен пользователь.

- 6.** Нажмите кнопку "Применить".

Будет выполнен переход на страницу "Список пользователей". В списке появится добавленный пользователь.

Для удаления пользователя:

- 1.** Вызовите панель безопасности и в группе "Управление пользователями" нажмите ссылку "Список пользователей".

Будет выполнен переход на страницу "Список пользователей".

- 2.** Выберите в списке пользователя, вызовите контекстное меню и выберите команду "Удалить".

Появится запрос на подтверждение удаления пользователя и его домашнего каталога.

- 3.** Если не требуется удалять домашний каталог пользователя, удалите отметку (по умолчанию домашний каталог удаляется).

Нажмите кнопку "OK".

Пользователь будет удален из списка (системы).

Изменение атрибутов пользователя

Атрибутами пользователя являются:

- имя пользователя;
- главная группа;
- полное имя;
- оболочка;
- домашний каталог;
- блокировка учетной записи;
- пароль;
- список групп, в которые включен пользователь.

Для изменения атрибутов пользователя:

1. Вызовите панель безопасности (см. стр.[27](#)) и перейдите на страницу "Список пользователей".
Будет выполнен переход на страницу "Список пользователей".
 2. Выберите в списке пользователя и в контекстном меню команду "Изменить".
Будет выполнен переход на страницу "Редактирование пользовательских атрибутов":

Главная > Управление пользователями > Просмотр списка пользователей > Редактирование пользовательских атрибутов

Редактирование пользовательских атрибутов

Имя пользователя:	<input type="text" value="ppagin"/> *	<input type="button" value="Изменить пароль"/>						
Главная группа:	<input type="text" value="ppagin"/> *	<input type="button" value="Параметры входа"/>						
Полное имя:	<input type="text" value="ppagin..."/>	<input type="button" value="Персональные идентификаторы"/>						
Оболочка:	<input type="text" value="/bin/bash"/> *							
Домашний каталог:	<input type="text" value="/home/ppagin"/>							
<input type="checkbox"/> Блокировать пользователя								
Группы пользователя								
<table border="1"> <thead> <tr> <th>Имя</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> utmp</td> </tr> <tr> <td><input checked="" type="checkbox"/> video</td> </tr> <tr> <td><input type="checkbox"/> sasl</td> </tr> <tr> <td><input checked="" type="checkbox"/> plugdev</td> </tr> <tr> <td><input type="checkbox"/> staff</td> </tr> </tbody> </table>			Имя	<input type="checkbox"/> utmp	<input checked="" type="checkbox"/> video	<input type="checkbox"/> sasl	<input checked="" type="checkbox"/> plugdev	<input type="checkbox"/> staff
Имя								
<input type="checkbox"/> utmp								
<input checked="" type="checkbox"/> video								
<input type="checkbox"/> sasl								
<input checked="" type="checkbox"/> plugdev								
<input type="checkbox"/> staff								
<input type="button" value="Применить"/> <input type="button" value="Отменить"/>								

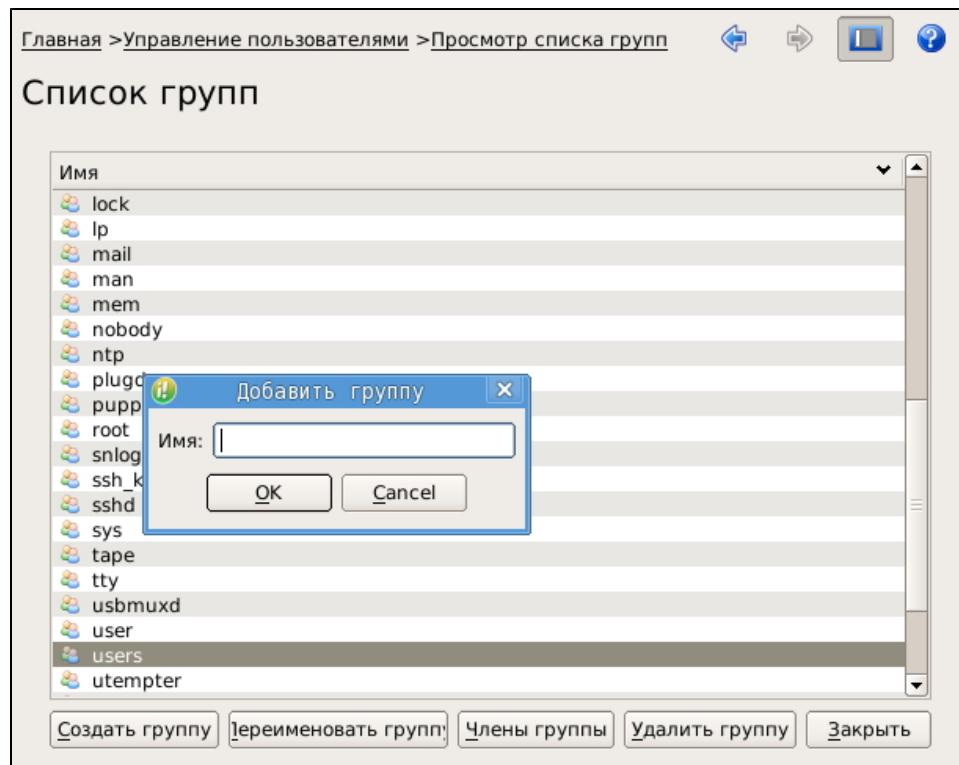
3. Внесите необходимые изменения в полях атрибутов.
 4. При необходимости заблокировать или разблокировать пользователя установите или удалите отметку в соответствующем поле.
 5. Для изменения атрибутов пароля (параметры пароля по умолчанию) нажмите кнопку "Параметры входа".
Будет выполнен переход на страницу "Управление паролями" (см. п. 3 процедуры на стр.[39](#)).
 6. Внесите необходимые изменения и нажмите кнопку "Применить".
Будет выполнен возврат на страницу редактирования пользовательских атрибутов.
 7. При необходимости изменения пароля пользователя нажмите кнопку "Изменить пароль".
Появится окно "Изменение пароля".
 8. Введите новый пароль пользователя, повторите ввод и нажмите кнопку "Применить".
Будет выполнен возврат на страницу редактирования пользовательских атрибутов.
 9. При необходимости изменения членства пользователя в группах установите нужные отметки в списке групп пользователя.
 10. Для завершения изменений нажмите кнопку "Применить".
Будет выполнен возврат на страницу "Список пользователей".

Добавление и удаление групп пользователей

Для добавления новой группы пользователей:

1. Вызовите панель безопасности и перейдите на страницу "Список групп" (см. стр.[37](#)).
2. Нажмите кнопку "Создать группу".

Появится окно ввода имени новой группы:



3. Введите имя группы и нажмите кнопку "Применить".

В связи с особенностями различных версий операционных систем рекомендуется при вводе не использовать символы верхнего регистра.

Будет выполнен переход на страницу "Список пользователей группы".

4. Укажите пользователей, которые должны быть включены в группу, и нажмите кнопку "Установить список пользователей".

Будет выполнен возврат на страницу "Список групп".

Для удаления группы пользователей:

1. Вызовите панель безопасности и перейдите на страницу "Список групп" (см. стр.[37](#)).
 2. Выберите группу и нажмите кнопку "Удалить группу".
- Появится окно предупреждения об удалении группы.
3. Для удаления группы нажмите кнопку "OK".
- Группа будет удалена из списка.

Изменение атрибутов группы

Изменение атрибутов группы подразумевает переименование и изменение состава включенных в нее пользователей.

Для переименования группы:

1. Вызовите панель безопасности и перейдите на страницу "Список групп" (см. стр.[37](#)).

2. Выберите в списке группу и нажмите кнопку "Переименовать группу".
Строка с именем выбранной группы станет доступной для редактирования.
3. Введите новое имя группы и нажмите клавишу <Enter>.

Для изменения состава группы:

1. Вызовите панель безопасности и перейдите на страницу "Список групп" (см. стр.[37](#)).
2. Выберите в списке группу и нажмите кнопку "Редактировать список пользователей".
Будет выполнен переход на страницу "Список пользователей группы". В общем списке отмечены пользователи, включенные в состав группы.
3. Установите или удалите нужные отметки и нажмите кнопку "Установить список пользователей".
Будет выполнен возврат на страницу "Список групп".

Включение и исключение пользователей из группы

Включить/исключить пользователя из группы можно любым из двух способов:

- На странице "Список пользователей" выбрать пользователя в общем списке и добавить или исключить его из выбираемых из общего списка групп.
- На странице "Список групп" выбрать группу в общем списке и редактированием списка пользователей включить или исключить из нее пользователя, выбранного из общего списка.

Изменение паролей и атрибутов паролей пользователей

У пользователя можно изменить атрибуты пароля (параметры пароля, заданные по умолчанию при добавлении пользователя в систему).

Для изменения пароля и атрибутов пароля:

1. Вызовите панель безопасности и перейдите на страницу "Список пользователей" (см. стр.[36](#)).
2. Выберите пользователя и в контекстном меню выберите команду "Изменить".
Будет выполнен переход на страницу "Редактирование пользовательских атрибутов" (см. стр.[40](#)).
3. Для изменения пароля нажмите кнопку "Изменить пароль". Изменение пароля описано в процедуре изменения атрибутов пользователя (см. стр.[40](#)).
4. Для изменения атрибутов пароля нажмите кнопку "Управление паролем". Изменение атрибутов описано в процедуре изменения атрибутов пользователя (см. стр.[40](#)).
5. После произведенных изменений нажмите на странице "Редактирование пользовательских атрибутов" кнопку "Применить".
Будет выполнен возврат на страницу "Список пользователей".

Блокировка и разблокировка учетной записи пользователя

Для блокировки/разблокировки пользователя:

1. Вызовите панель безопасности и в группе "Управление пользователями" перейдите на страницу "Список пользователей".
2. Выберите пользователя, вызовите контекстное меню и выберите команду "Блокировать" или "Разблокировать".

Блокировка/разблокировка может быть выполнена на странице "Редактирование пользовательских атрибутов" (см. стр.[40](#)).

Глава 5

Защита входа в систему

Для защиты входа в систему администратор выполняет следующие действия:

- настройка и контроль параметров парольной политики;
- включение/выключение режима усиленной аутентификации;
- настройка блокировки входа при нарушении целостности контролируемых объектов файловой системы;
- блокировка учетных записей пользователей;
- присвоение пользователям персональных идентификаторов и обеспечение режима усиленной аутентификации;
- управление режимом входа пользователей в систему;
- аудит событий входа пользователей в систему.

Настройка и контроль параметров паролей по умолчанию

При добавлении в систему нового пользователя для него по умолчанию устанавливаются настройки пароля. Такими настройками являются:

- срок действия пароля;
- число дней до разрешения смены пароля;
- за сколько дней до устаревания пароля будет производиться оповещение пользователя;
- число дней после устаревания пароля до его блокировки;
- время, когда учетная запись пользователя будет заблокирована.

Администратор может изменить значения параметров пароля по умолчанию для добавляемых пользователей.



Измененные значения параметров будут применены только к вновь добавляемым пользователям. На остальных пользователей изменения не распространяются.

Настройка параметров пароля для пользователя приведена на стр.[43](#).

Для изменения настроек пароля по умолчанию:

1. Вызовите панель безопасности и в группе "Управление пользователями" перейдите на страницу "Параметры паролей".
 2. Задайте необходимые значения параметров и нажмите кнопку "Применить".
- Будет выполнен возврат на главную страницу.

Включение и выключение режима усиленной аутентификации



Для корректной реализации режима усиленной аутентификации эталонное значение свертки пароля пользователя должно храниться в БД доменных служб Active Directory (AD DS), но не в БД служб облегченного доступа Active Directory (AD LDS).

Для включения/выключения режима усиленной аутентификации:

Пояснение. После установки Secret Net LSP параметр "Усиленная аутентификация" принимает значение "Выключено" по умолчанию.

1. Вызовите панель безопасности (см. стр.[27](#)) и в группе "Настройки приложения" перейдите на страницу "Настройка политик".
На экране появится окно "Настройка политик" (см. стр.[32](#)).
2. В политике "Параметры аутентификации" установите требуемое значение параметра "Усиленная аутентификация" — "Включено"/"Выключено".

Настройка блокировки входа при нарушении целостности

Для защиты входа в систему предусмотрена блокировка при нарушении целостности объектов файловой системы, поставленных на контроль.

Блокировка распространяется на всех пользователей компьютера. Снять блокировку может только администратор (см. стр.[68](#)).

Настройка блокировки выполняется в подсистеме контроля целостности при постановке ресурса на контроль (см. стр.[66](#)).

Блокировка учетных записей пользователей

Администратор может заблокировать или разблокировать учетную запись пользователя. Блокировка и разблокировка учетной записи описаны на стр.[43](#).

Персональные идентификаторы

Персональный идентификатор — устройство для хранения информации, необходимой при идентификации и аутентификации пользователя. В идентификаторе могут храниться ключи для усиленной аутентификации пользователя.

В Secret Net LSP используются персональные идентификаторы семейства Rutooken и iButton.

Персональный идентификатор выдается пользователю администратором. Пользователю можно присвоить несколько идентификаторов. Один и тот же персональный идентификатор не может быть присвоен нескольким пользователям одновременно.

Подготовка персональных идентификаторов к использованию возлагается на администратора. При подготовке используются сторонние утилиты.

Администратор может выполнять следующие операции с идентификаторами:

Инициализация идентификатора
Форматирование, обеспечивающее возможность использования идентификатора в Secret Net LSP. Инициализация требуется, когда в персональном идентификаторе по каким-либо причинам была нарушена или отсутствует структура данных
Присвоение идентификатора
Добавление в базу данных Secret Net LSP сведений о том, что пользователю принадлежит идентификатор данного типа с уникальным серийным номером
Отмена присвоения идентификатора
Удаление из базы данных Secret Net LSP информации о принадлежности данного персонального идентификатора данному пользователю. Далее для простоты эту операцию будем называть "удаление идентификатора"
Включение режима хранения пароля в идентификаторе
Добавление в базу данных Secret Net LSP сведений о включении для пользователя режима хранения пароля в идентификаторе. Одновременно с этой операцией выполняется запись пароля в идентификатор. После включения режима пароль пользователя при входе в систему не вводится с клавиатуры, а считывается из идентификатора
Отключение режима хранения пароля в идентификаторе
Операция, противоположная предыдущей. Одновременно с отключением режима хранения выполняется удаление пароля из памяти персонального идентификатора. Идентификатор остается закрепленным за пользователем
Запись и удаление ключей для усиленной аутентификации
Используется для хранения в идентификаторе ключей для усиленной аутентификации пользователя

Для обеспечения работы пользователей администратор должен:

- Присвоить идентификаторы — зарегистрировать идентификаторы в системе и связать их с пользователями.
- При необходимости (в зависимости от используемого варианта ввода идентификационных данных при входе в систему) записать пароли пользователей в идентификаторы.
- При необходимости (если используется режим усиленной аутентификации) записать ключ в идентификатор.
- Выдать пользователям присвоенные им идентификаторы.
- Ознакомить пользователей с порядком применения идентификаторов.
- Проверить и при необходимости задать режим входа пользователей в систему.

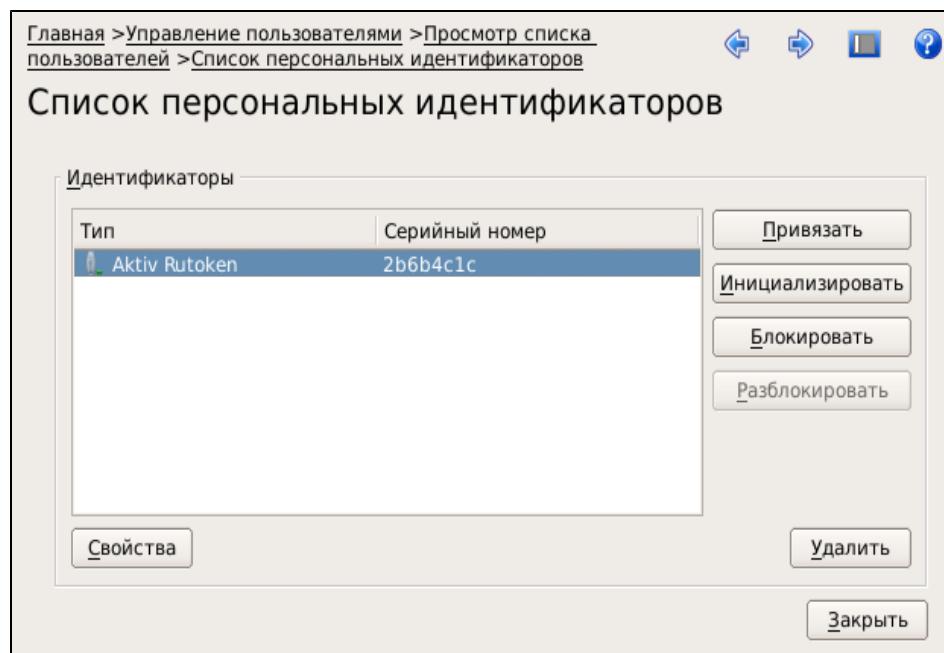
Просмотр сведений об идентификаторах пользователя

Сведения об идентификаторах пользователя отображаются на странице "Список персональных идентификаторов".

Для просмотра сведений об идентификаторах пользователя:

1. В панели безопасности перейдите на страницу "Список пользователей".
2. Выберите в списке пользователя, вызовите контекстное меню и выберите команду "Персональные идентификаторы".

Откроется окно "Список персональных идентификаторов":



В списке отображаются присвоенные пользователю идентификаторы. Для каждого идентификатора указан тип и серийный номер. Если пользователь не имеет идентификаторов, список будет пустым.

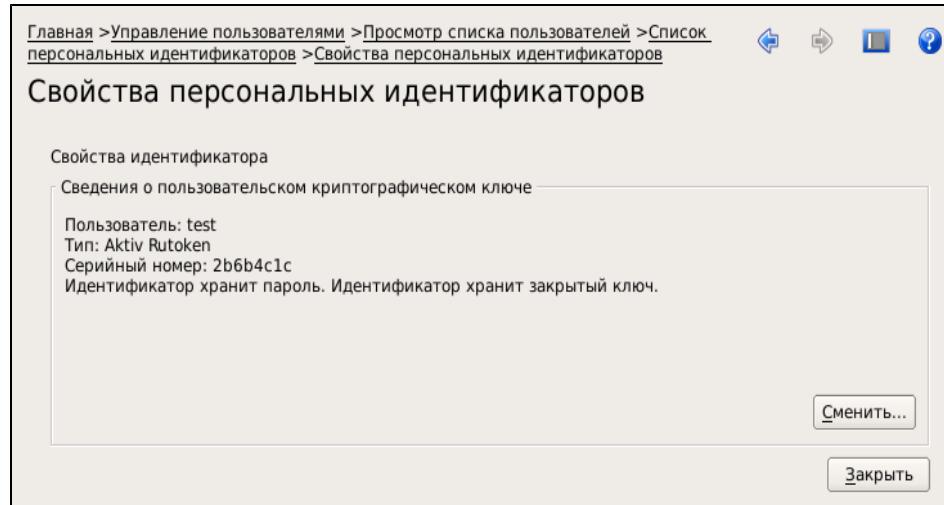
На странице можно выполнить следующие операции:

- проинициализировать идентификатор;
- присвоить пользователю новый идентификатор;
- задать режим хранения пароля в идентификаторе;
- записать в идентификатор закрытый ключ пользователя;
- отменить присвоение идентификатора пользователю;
- просмотреть сведения о хранении в идентификаторе пароля и/или закрытого ключа пользователя;
- проверить принадлежность идентификаторов пользователям.

Для просмотра сведений о хранении пароля и ключа:

- Выберите в списке идентификатор и нажмите кнопку "Свойства".

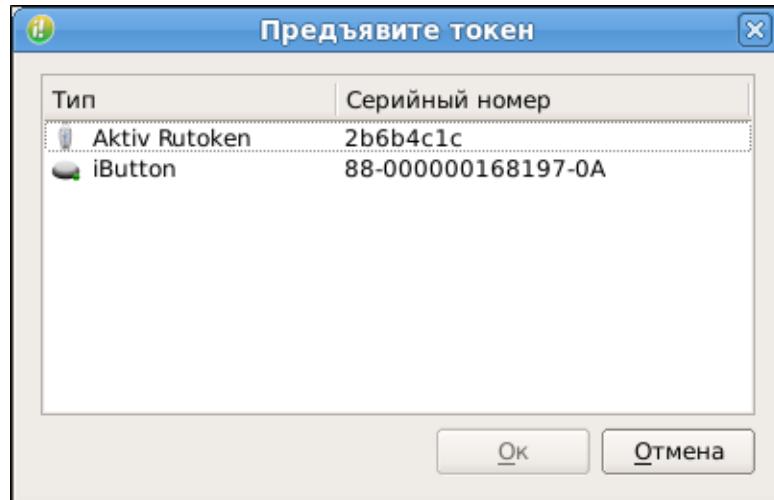
Откроется окно "Свойства персональных идентификаторов":



В окне отображается информация:

- имя пользователя, которому принадлежит данный идентификатор;
 - тип и серийный номер идентификатора;
 - сведения о хранении пароля и/или ключа пользователя.
- Если пользователю присвоено несколько идентификаторов, для просмотра сведений о другом идентификаторе нажмите кнопку "Сменить".

Появится запрос на предъявление идентификатора:



- Предъявите идентификатор и после появления типа и серийного номера предъявленного идентификатора в окне запроса выделите его и нажмите кнопку "OK".

В окне "Свойства персональных идентификаторов" появятся сведения о предъявленном идентификаторе.

- Для завершения просмотра нажмите кнопку "Закрыть".

Будет выполнен возврат к списку персональных идентификаторов.

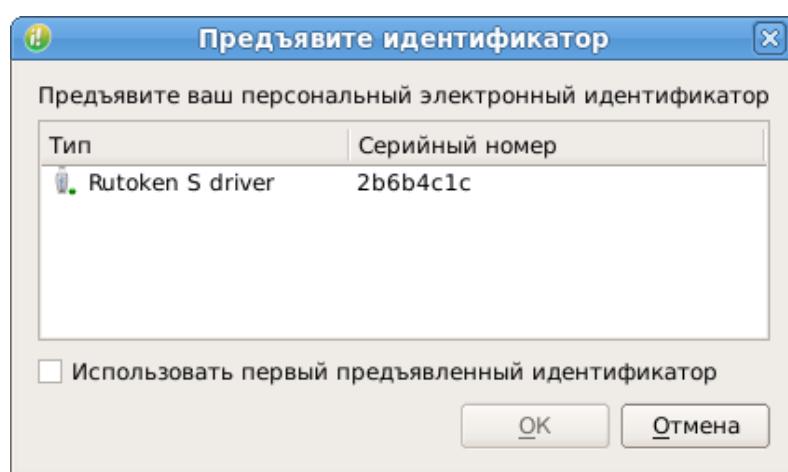
Инициализация идентификатора

Инициализацию можно выполнять в списке персональных идентификаторов любого пользователя.

Для инициализации идентификатора:

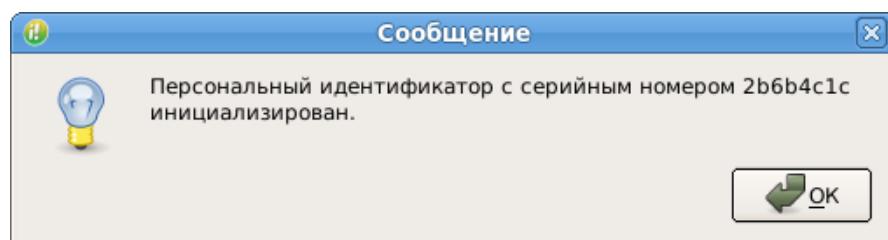
1. Вызовите панель управления безопасностью и в группе "Управление пользователями" перейдите на страницу "Список пользователей".
2. Выберите в списке любого пользователя, вызовите контекстное меню и выберите команду "Персональные идентификаторы".
3. Предъявите идентификатор, подлежащий инициализации, и нажмите кнопку "Инициализировать".
4. Предъявите идентификатор.

Предъявленный идентификатор (его тип и серийный номер) появится в окне запроса:



5. Выделите идентификатор, подлежащий инициализации, и нажмите кнопку "OK".

Выделенный идентификатор будет проинициализирован и на экране появится сообщение:



6. Нажмите кнопку "OK" в окне сообщения.

Присвоение идентификатора

При выполнении процедуры присвоения идентификатора предусмотрена запись в него пароля и закрытого ключа пользователя.

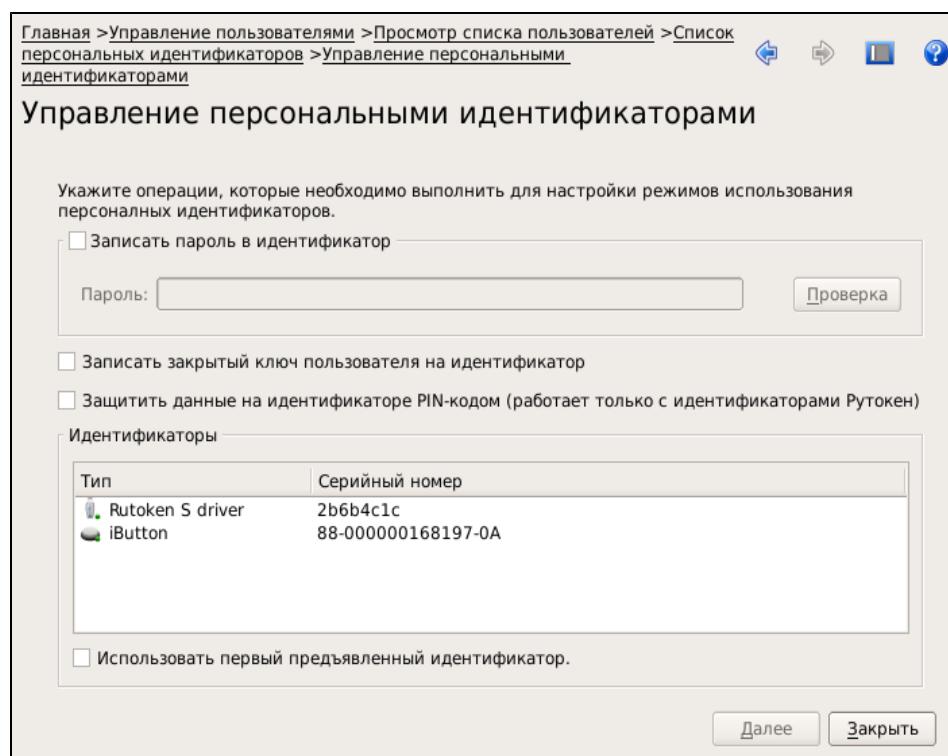
Для записи пароля в идентификатор потребуется ввести пароль данного пользователя.

Если у пользователя еще нет ключа для усиленной аутентификации, ключ будет сгенерирован и записан в идентификатор.

Для записи в идентификатор уже имеющегося у пользователя закрытого ключа потребуется предъявить идентификатор, на котором этот ключ записан.

Для присвоения идентификатора:

1. Вызовите панель безопасности и в группе "Управление пользователями" перейдите на страницу "Список пользователей".
2. Выберите в списке пользователя, вызовите контекстное меню и выберите команду "Персональные идентификаторы".
Откроется окно "Список персональных идентификаторов".
3. Нажмите кнопку "Привязать".
Откроется окно "Управление персональными идентификаторами":



4. Если в идентификаторе должен храниться пароль пользователя, установите отметку в поле "Записать пароль в идентификатор", введите пароль пользователя и нажмите кнопку "Проверка".
Будет выполнена проверка, и в случае правильно введенного пароля справа от поля "Пароль" появится подтверждающая отметка.
5. Если в идентификаторе должен храниться закрытый ключ пользователя, установите отметку в поле "Записать закрытый ключ пользователя на идентификатор".
6. Если идентификатор должен быть защищен PIN-кодом, установите отметку в поле "Защитить данные на идентификаторе PIN-кодом".
7. Если точно известно, какой идентификатор нужно предъявить для присвоения пользователю, установите отметку в поле "Использовать первый предъявленный идентификатор" и предъявите его.
Перейдите к пункту 9.
8. Если необходимо для предъявления выбрать идентификатор из нескольких имеющихся, удалите отметку в поле "Использовать первый предъявленный идентификатор" и поочередно предъявляйте идентификаторы.
Предъявляемые идентификаторы (тип и серийный номер) будут отображаться в списке "Идентификаторы" (см. рис. в п. 3).
При появлении в списке нужного идентификатора выделите его.
9. Нажмите кнопку "Далее".

- Если было выбрано хранение закрытого ключа и у пользователя уже имеется идентификатор с хранящимся в нем ключом, появится запрос на предъявление идентификатора пользователю.
Предъявите идентификатор с хранящимся в нем ключом.
- Если идентификатор должен быть защищен PIN-кодом, появится запрос на его ввод.
Введите PIN-код и нажмите кнопку "OK" в окне запроса.

Будет выполнена привязка идентификатора к пользователю, и в зависимости от настроек, выполненных в пп. **4–6**, в идентификатор будут записаны (или не записаны) пароль и/или ключ и установлен (или не установлен) признак защиты PIN-кодом.

Отмена присвоения идентификатора

Если в идентификаторе пользователя хранится пароль и/или закрытый ключ, эти данные при отмене присвоения идентификатора затираются.

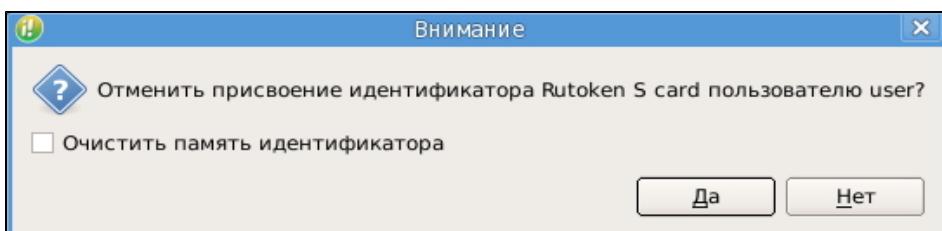
Для отмены присвоения идентификатора:

1. Перейдите на страницу "Список пользователей", выберите пользователя, вызовите контекстное меню и выберите команду "Персональные идентификаторы".

Откроется окно "Список персональных идентификаторов".

2. Выберите идентификатор и нажмите кнопку "Удалить".

Появится окно "Внимание":



3. Если необходимо очистить память идентификатора, установите отметку в соответствующем поле окна предупреждения.

Ошибка
Если удаляемый идентификатор является единственным идентификатором пользователя и в СЗИ установлен режим входа в систему с обязательным предъявлением последнего, после отмены присвоения пользователь не сможет войти в систему.

4. Нажмите кнопку "Да" в окне предупреждения.

Будет выполнена отмена присвоения идентификатора.

Запись пароля в идентификатор

При необходимости администратор может записать пароль в идентификатор пользователя (если он не был записан при присвоении идентификатора).

Для записи пароля в идентификатор:

1. Выполните процедуру отмены присвоения идентификатора, описанную выше (см. стр.**50**).
2. Выполните процедуру присвоения идентификатора, используя опцию "Записать пароль в идентификатор" (см. стр.**48**).

Проверка принадлежности идентификатора

Для проверки принадлежности идентификатора:

1. Вызовите панель безопасности и в группе "Управление пользователями" перейдите на страницу "Список пользователей".
2. Выберите в списке любого пользователя, вызовите контекстное меню и выберите команду "Персональные идентификаторы".

Откроется окно "Список персональных идентификаторов". В списке отображаются присвоенные пользователю идентификаторы.

3. Нажмите кнопку "Привязать".

Появится запрос на предъявление персонального идентификатора.

4. Предъявите идентификатор.

Если идентификатор присвоен какому-либо пользователю, появится соответствующее сообщение с указанием имени пользователя.

5. Закройте окно сообщения.

Блокировка идентификатора

Администратор может временно заблокировать вход пользователя по идентификатору.

Для блокировки идентификатора:

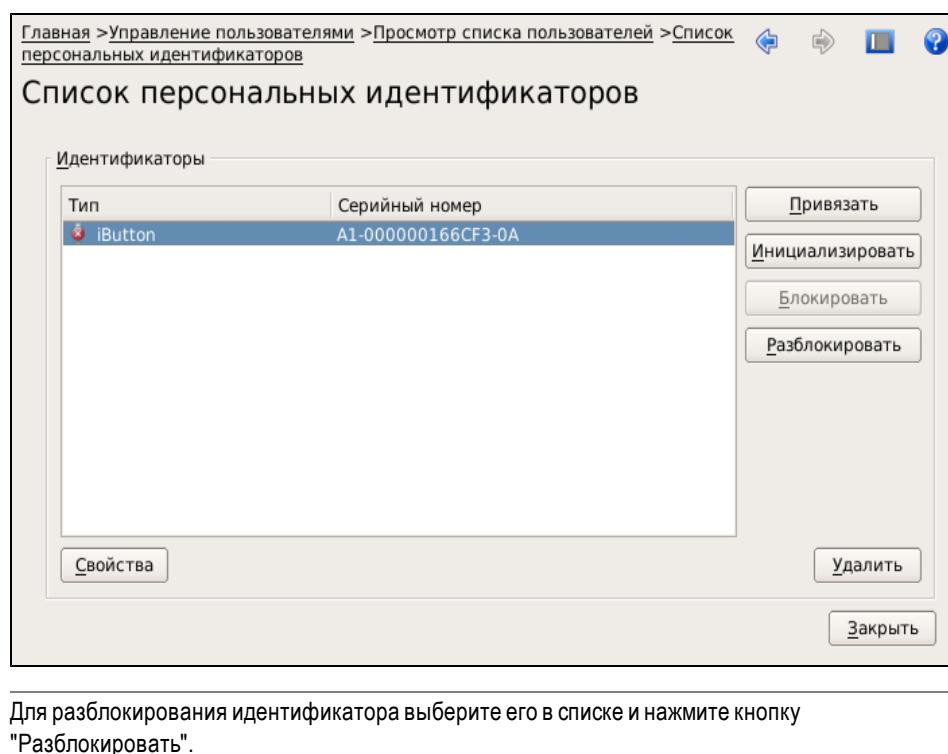
1. В панели безопасности перейдите на страницу "Список пользователей".

2. Выберите в списке пользователя, вызовите контекстное меню и выберите команду "Персональные идентификаторы".

Откроется окно "Список персональных идентификаторов".

3. Выберите в списке идентификатор и нажмите кнопку "Блокировать".

Идентификатор будет заблокирован и на его пиктограмме появится отметка красного цвета:



Управление режимом входа в систему

По умолчанию после установки для всех пользователей задан режим входа, при котором ввод имени и пароля пользователя осуществляется с клавиатуры или путем предъявления идентификатора.

Изменение режима входа задается политикой "Параметры усиленной аутентификации" на странице "Настройка политик".

Для просмотра/изменения политики входа в систему:

1. Вызовите панель безопасности (см. стр. 27) и в группе "Настройки приложения" перейдите на страницу "Политики".

Откроется окно "Настройка политик".

2. Раскройте политику "Параметры усиленной аутентификации".
3. Для изменения параметров идентификации и/или аутентификации выделите параметр "Метод идентификации" и/или "Метод аутентификации" и в поле "Значение" из раскрывающегося списка выберите нужное значение.
4. Для сохранения внесенных изменений нажмите кнопку "Применить".

Управление режимом аутентификации

В Secret Net LSP используется аутентификация двух типов — локальная и доменная. Доменная аутентификация позволяет выполнять вход в систему под именем доменного пользователя.



Внимание! Для использования доменной аутентификации требуется наличие в системе библиотеки pam_winbind.so, также необходимо включить данный компьютер в домен. Этот тип аутентификации используется как при совместном функционировании Secret Net LSP с сервером безопасности СЗИ Secret Net 7, так и без этого. Включить компьютер в домен можно стандартными средствами ОС Windows.

Для просмотра/изменения режима аутентификации:

1. Вызовите панель безопасности (см. стр.[27](#)) и в группе "Настройки приложения" перейдите на страницу "Настройки удаленного управления".
2. В поле "Тип аутентификации" выберите нужное значение:
 - "Доменная" — чтобы включить доменную аутентификацию;
 - "Локальная" — чтобы включить локальную аутентификацию.

Совет. Для настройки режима аутентификации также можно использовать утилиту **snnetparamcfg**. Описание утилиты и особенности ее применения приведены в приложении (см. стр.[94](#)).

Глава 6

Управление доступом к объектам файловой системы

В рамках дискреционного разграничения доступа администратор выполняет следующие функции:

- включает/выключает функционирование подсистемы дискреционного управления доступом;
- просматривает и изменяет права доступа UNIX;
- составляет и редактирует списки POSIX ACL;
- ведет аудит событий, связанных с работой механизма разграничения доступа.



При создании нового ресурса файловой системы (каталога, файла) пользователь, создавший его, автоматически становится его владельцем. При этом в зависимости от типа ресурса (каталога, файла) на него по умолчанию устанавливаются права доступа, вычисляемые на основании маски. Пользователь-владелец может при необходимости изменить установленные по умолчанию права доступа.

Изменение прав доступа к ресурсам осуществляется с помощью утилиты управления правами доступа и описано в документе "Средство защиты информации Secret Net LSP. Руководство пользователя".

Включение и выключение

Пояснение. После установки Secret Net LSP параметр "Режим работы" политики "Дискреционное управление доступом" принимает значение "Включено" по умолчанию.

Для включения/выключения работы подсистемы дискреционного управления доступом:

1. Вызовите панель безопасности (см. стр.[27](#)) и в группе "Настройки приложения" перейдите на страницу "Настройка политик".
На экране появится окно "Настройка политик" (см. стр.[32](#)).
2. В политике "Дискреционное управление доступом" установите требуемое значение параметра "Режим работы" — "Включено"/"Выключено".

Просмотр прав доступа к объектам

Просмотр и управление правами доступа к объектам файловой системы осуществляется на странице "Управление доступом".

Для перехода на страницу управления доступом:

- Вызовите панель безопасности (см. стр.[27](#)) и в группе "Доступ к объектам" нажмите ссылку "Управление доступом".

Будет выполнен переход на соответствующую страницу:

Главная > Управление объектами > Управление доступом

Управление доступом

Имя	Размер	Тип	Дата изменения	Права доступа
/		Drive	18.06.12 15:07	rwxr-xr-x
.config		Folder	18.06.12 15:07	rwxr-xr-x
bin		Folder	18.06.12 15:05	rwxr-xr-x
boot		Folder	16.04.12 20:10	rwx-----
cgroup		Folder	31.01.11 18:04	r-xg-xr-x
dev		Folder	18.06.12 15:10	rwxr-xr-x
etc		Folder	18.06.12 15:10	rwxr-xr-x
home		Folder	18.06.12 15:10	rwxr-xr-x
lib		Folder	16.04.12 20:06	rwxr-xr-x
lib64		Folder	18.06.12 15:05	rwxr-xr-x
lost+found		Folder	16.04.12 19:59	rwx-----
media		Folder	16.04.12 20:11	rwxr-xr-x
mnt		Folder	16.04.12 20:12	rwxr-xr-x
opt		Folder	18.06.12 15:04	rwxr-xr-x

На странице представлен корневой каталог с указанием прав доступа UNIX для каждой папки каталога. Для просмотра прав доступа на вложенные объекты раскройте папку.

Изначально права доступа UNIX устанавливаются в соответствии с правами, определенными в ОС.

Для просмотра/изменения прав доступа:

- Выберите объект доступа, вызовите контекстное меню и выберите команду "Редактировать права" или "Просматривать права".

Если была выбрана команда "Просматривать права", будет выполнен переход на страницу просмотра прав для выбранного объекта:

Главная > Управление объектами > Управление доступом > Просмотр объектов доступа

Просмотр объектов доступа

Файл "/home/pragin/.pulse-cookie"

Права доступа Unix

Владелец: pragin	rwx	Чтение, запись и исполнение
Группа: pragin	r--	Чтение
Остальные	---x	Выполнение

Файл не выгружается из памяти (бит sticky)

Права доступа Posix ACL

Субъект прав доступа	Права доступа	Расшифровка	Эффективные права
Пользователь:pragin	r-x	Чтение и выполнение	r-- (Чтение)
Группа:exim	r-x	Чтение и выполнение	r-- (Чтение)
Маска	r--	Чтение	

[Назад к списку](#) [Редактировать...](#)

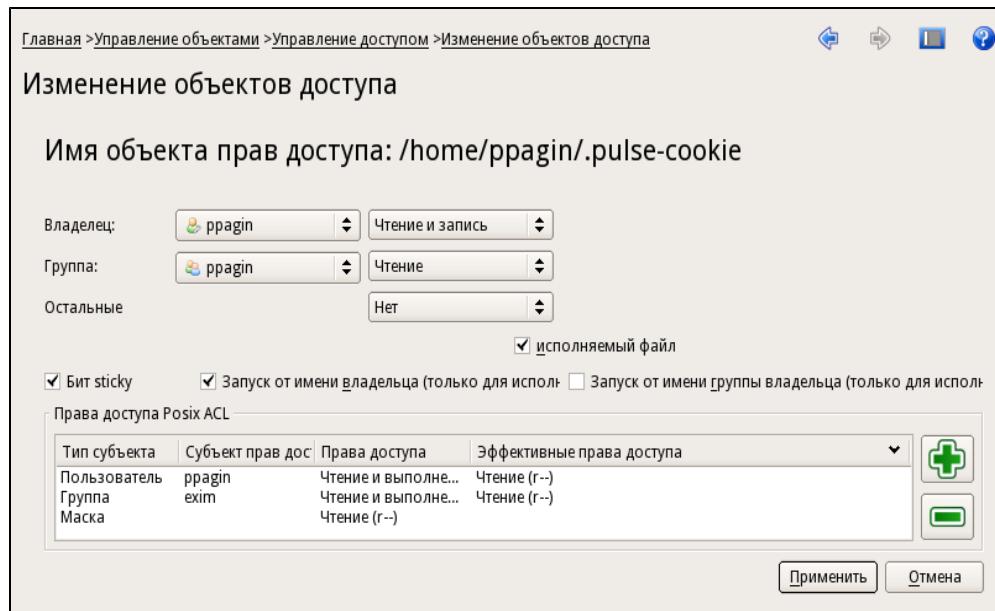
На странице представлены текущие значения прав доступа UNIX и список прав доступа POSIX ACL.

Если права доступа POSIX ACL администратором не задавались, список будет пустым. Это означает, что права доступа POSIX ACL для данного объекта соответствуют правам доступа UNIX (для владельца, группы владельца и остальных).

Если администратор добавлял или изменял права ACL, в списке POSIX ACL будет содержаться перечень субъектов доступа (пользователей и групп) с указанием их прав доступа к данному объекту, а также эффективные права (в случае применения маски). Кроме того, если объектом доступа является каталог, в списке могут отображаться наследуемые права доступа, т.е. права, распространяемые на создаваемые в данном каталоге файлы и подкаталоги для всех владельцев, всех групп владельцев и остальных.

- Для возврата на страницу "Управление доступом" нажмите кнопку "Назад к списку" или воспользуйтесь строкой навигации.
- Для перехода на страницу редактирования прав доступа нажмите кнопку "Редактировать".

Если была выбрана команда "Редактировать права", будет выполнен переход на страницу изменения прав доступа для выбранного объекта:



На странице отображаются текущие права доступа UNIX и список POSIX ACL. На этой странице администратор может выполнить следующие операции для данного объекта:

- изменить владельца и его права доступа UNIX;
- изменить группу-владельца и ее права доступа UNIX;
- изменить права доступа UNIX остальных;
- установить/удалить атрибут **sticky bit**;
- установить/удалить признак исполняемого файла;
- установить/удалить флаги запуска от имени владельца и/или группы-владельца (только для исполняемого файла);
- изменить/отредактировать список POSIX ACL для данного объекта.

Изменение прав доступа UNIX

Для изменения прав доступа UNIX:

1. Перейдите на страницу редактирования прав для выбранного объекта.
2. Для изменения владельца объекта или группы-владельца выберите их из раскрывающихся списков пользователей или групп.
3. При необходимости измените права раздельно для владельца, группы и остальных.

Права выбираются из раскрывающихся списков. При этом содержание списка для каталогов отличается от содержания списка для файлов.

Каталог	Файл
<ul style="list-style-type: none"> • Нет прав (--- • Выполнение (-x) • Запись (-w-) • Запись и выполнение (wx-) • Чтение (r--) • Чтение и выполнение (r-x) • Чтение и запись (rw-) • Чтение, запись и выполнение (rwx) 	<ul style="list-style-type: none"> • Нет прав (--- • Запись (-w-) • Чтение (r--) • Чтение и запись(rw-)

4. Если объектом является каталог и необходимо, чтобы файлы, содержащиеся в каталоге, могли удалять и переименовывать только владельцы каталога и файла или пользователь root, установите отметку в поле "Бит Sticky".
5. Если объектом является файл и он должен быть исполняемым, установите отметку в поле "Исполняемый файл" (для каталогов поле недоступно).
6. Если объекты в каталоге должны наследовать группу-владельца, установите отметки в соответствующих полях (для каталогов доступно только поле "Наследовать группу владельца").
7. Для сохранения настроек прав доступа UNIX нажмите кнопку "Применить".
Будет выполнен возврат на страницу "Управление доступом".

Редактирование списка POSIX ACL

Для составления/редактирования списка POSIX ACL:

1. Перейдите на страницу редактирования прав для выбранного объекта.
2. Для добавления новой записи в список нажмите кнопку  , расположенную справа.
В списке появится новая строка для задания прав доступа.
3. Выделите в строке поле "Тип субъекта" и в раскрывающемся списке выберите нужное значение.

Тип субъекта	Описание
Пользователь	Права устанавливаются для пользователя
Группа	Права устанавливаются для группы
Мaska	Добавляется автоматически. Задает эффективное значение прав для пользователей и групп
По умолчанию для всех владельцев	Только для каталогов. Задает наследование прав для всех владельцев на создаваемые в каталоге файлы и подкаталоги
По умолчанию для всех групп владельцев	Только для каталогов. Задает наследование прав для всех групп владельцев на создаваемые в каталоге файлы и подкаталоги
По умолчанию для остальных	Только для каталогов. Задает наследование прав для остальных на создаваемые в каталоге файлы и подкаталоги
Мaska по умолчанию	Только для каталогов. Мaska для наследуемых прав по умолчанию

4. Если типом субъекта было выбрано "пользователь" или "группа", выделите в строке поле "Субъект прав доступа" и в раскрывающемся списке выберите пользователя или группу.
5. Выделите в строке поле "Права доступа" и в раскрывающемся списке выберите нужное значение.

При добавлении в список хотя бы одного типа субъекта по умолчанию (для каталогов) в список будут добавлены все остальные. При этом будут автоматически установлены эффективные права.

6. Добавьте в список все необходимые субъекты доступа и установите их права (см. пп. 2–5).
 7. Для редактирования строки выделите ее в списке и выполните необходимые действия, описанные в предыдущих пунктах.
 8. Для удаления выбранной в списке строки нажмите кнопку  , расположенную справа.
 9. Для сохранения списка нажмите кнопку "Применить".
- Будет выполнен возврат на страницу "Управление доступом".

Глава 7

Разграничение доступа к устройствам

Контроль и управление доступом к устройствам осуществляются администратором средствами подсистемы разграничения доступа. В рамках контроля и управления администратор выполняет следующие функции:

- составляет и при необходимости корректирует список контролируемых устройств;
- устанавливает и при необходимости изменяет права доступа;
- управляет режимом работы подсистемы разграничения доступа;
- ведет аудит событий, связанных с доступом к контролируемым устройствам.

После установки СЗИ Secret Net LSP для USB-устройств и шин USB, SATA, IEEE 1394 по умолчанию всем пользователям устанавливаются права, разрешающие чтение и запись.

После выполнения администратором настроек в подсистеме (регистрации устройств и задания прав доступа к ним, включения жесткого режима работы) пользователи смогут подключать только зарегистрированные устройства и выполнять только те операции, которые определены для них в правах доступа.

Права доступа пользователей к устройству могут наследоваться от прав доступа кшине, к которой подключается данное устройство.

Если для разных групп, в которые входит пользователь, установлены запрещающие и разрешающие права доступа, при вычислении эффективных прав доступа к устройству запрещающие права имеют приоритет над разрешающими.

Список устройств

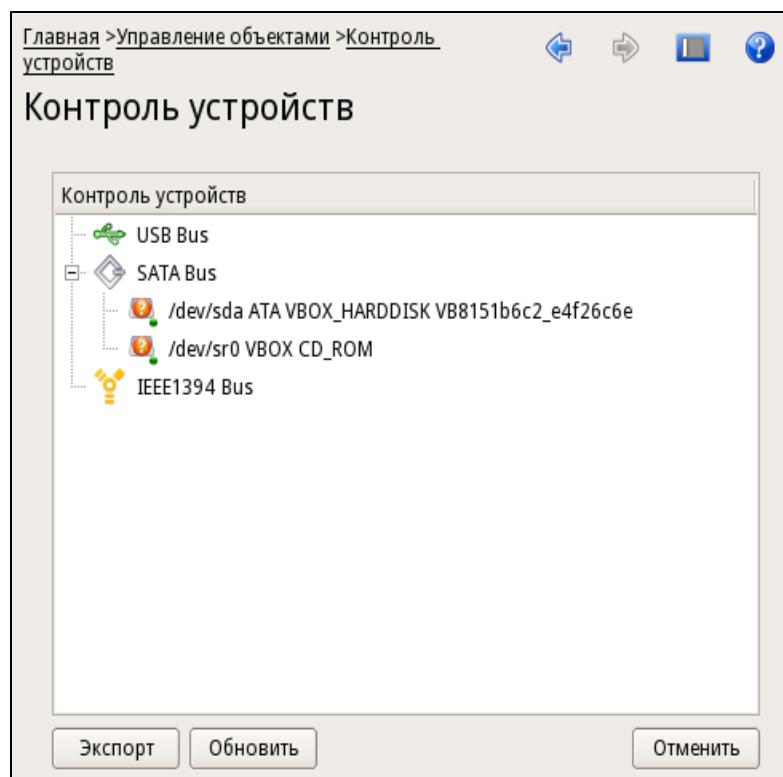
Список контролируемых устройств формируется при регистрации нового устройства и добавлении его в список.

При просмотре списка устройств можно выполнить следующее:

- зарегистрировать новое устройство;
- просмотреть или изменить права доступа к зарегистрированным устройствам;
- отменить регистрацию устройства;
- сохранить в файл текущие права доступа пользователей и групп к устройствам с возможностью последующего вывода на печать.

Для просмотра зарегистрированных устройств:

1. Вызовите панель безопасности (см. стр. 27) и перейдите на страницу "Контроль устройств":



На странице представлен список подключенных (как зарегистрированных, так и не зарегистрированных) устройств, сгруппированных по шинам USB, SATA и IEEE 1394.

Для отображения шин используются следующие пиктограммы:

	Шина USB
	Шина SATA
	Шина IEEE 1394

Для отображения устройств используются следующие пиктограммы:

	USB-устройство
	SATA-устройство
	Устройство IEEE 1394

Для отображения статуса устройства используются следующие пиктограммы (на примере USB-устройства).

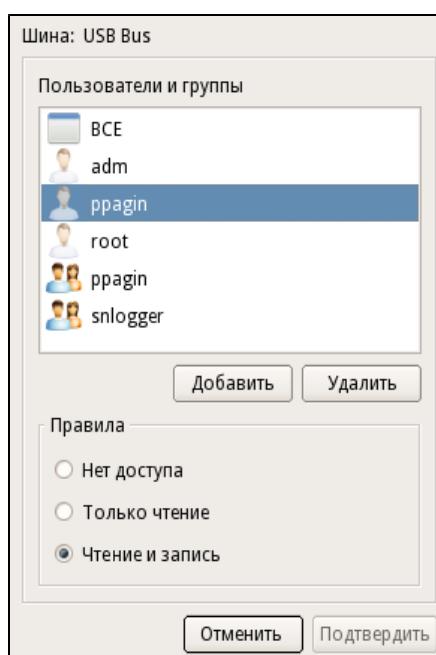
	Устройство зарегистрировано и подключено
	Устройство зарегистрировано и не подключено

	Устройство не зарегистрировано и подключено
--	---

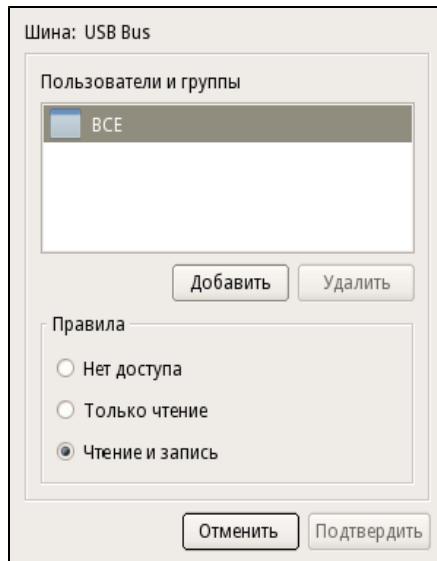
В нижней части страницы расположены 3 кнопки:

Экспорт	Сохранение списка устройств и правил разграничения доступа в файл
Обновить	Обновление списка подключенных и зарегистрированных устройств
Отменить	Возврат на страницу группы "Контроль устройств"

- Для просмотра устройств, подключенных к шине, раскройте соответствующую группу.
- Для просмотра прав доступа к устройству(шине) выберите его в списке, вызовите контекстное меню и выберите команду "Настройка правил". Откроется окно со списком пользователей и групп, которым определены права доступа к данному устройству:



Если права доступа к данному устройству не назначались, в списке отображаются только установленные по умолчанию для всех пользователей права, разрешающие чтение и запись:



- Для просмотра прав доступа пользователя (группы) выберите его в списке. При этом в нижней части окна отобразятся правила — права доступа выбранного пользователя к устройству.
- Для сохранения настроек прав доступа к устройствам нажмите кнопку "Экспорт".
Откроется окно предварительного просмотра прав доступа к устройствам.
- Для возврата на страницу "Контроль устройств" нажмите кнопку "Отменить", расположенную в нижней части окна.

Регистрация устройства и назначение прав доступа

Регистрация устройства осуществляется при его подключении.

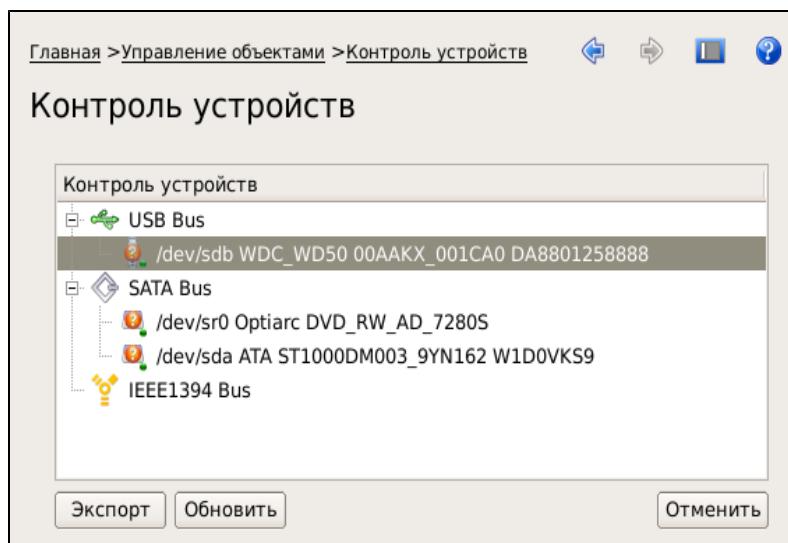
Для регистрации устройства:

1. Подключите устройство.

В зависимости от используемого контроллера для подключения устройства может потребоваться выключение компьютера. В этом случае выключите компьютер, подключите устройство и затем включите компьютер и войдите в систему.

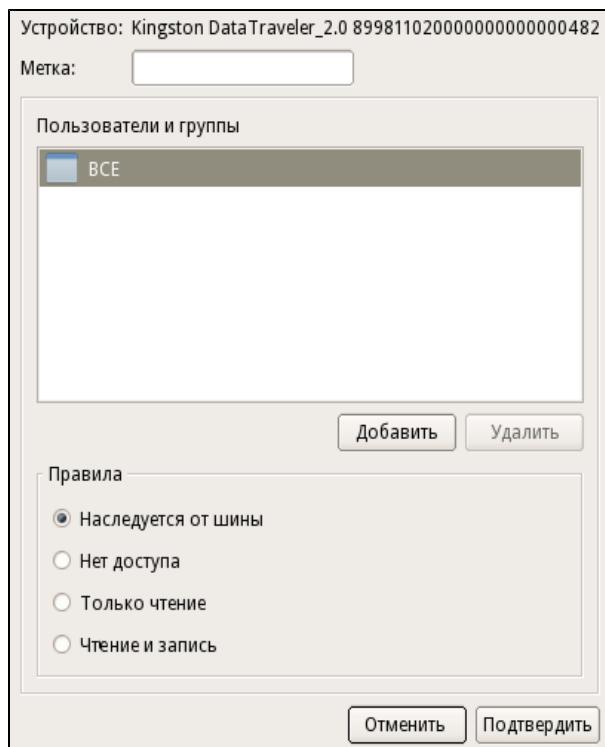
2. Вызовите панель безопасности, перейдите на страницу "Контроль устройств" и нажмите кнопку "Обновить".

В списке устройств появится подключенное устройство:



- 3.** Вызовите контекстное меню к устройству и выберите команду "Настроить правила".

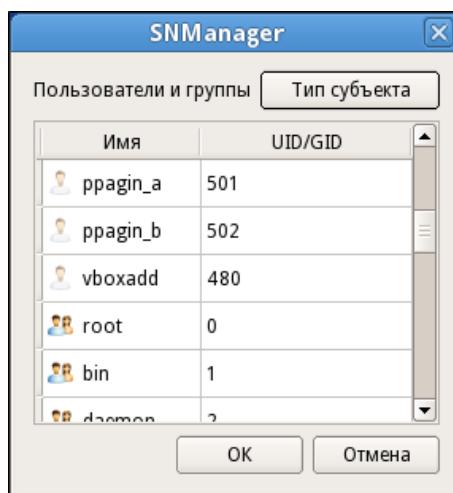
Появится окно настройки прав доступа к данному устройству:



Если права доступа к данному устройству не назначались, в списке отображаются только установленные по умолчанию права для всех пользователей, разрешающие чтение и запись.

- 4.** Введите метку устройства (необязательно) и для задания прав доступа к объекту нажмите кнопку "Добавить".

Появится окно выбора субъектов доступа:



В окне представлен список всех пользователей и групп.

Для удобства можно использовать фильтр отображения только пользователей или только групп. Для этого нажмите кнопку "Тип субъекта" и в раскрывающемся списке удалите ненужную отметку.

- 5.** Выберите субъект доступа и нажмите кнопку "OK".

Этот субъект доступа появится в окне настройки прав доступа к объекту.

- 6.** Выделите субъект доступа и установите нужные отметки в группе "Правила".

- 7.** Добавьте все субъекты, которым необходимо установить права доступа к данному объекту (см. пп. **4—6**).

Для удаления субъекта и прав доступа выделите его в списке и нажмите кнопку "Удалить".

- 8.** После формирования списка субъектов и прав доступа нажмите кнопку "Подтвердить", расположенную в нижней части окна.

Устройство будет зарегистрировано и поставлено на контроль. При этом пиктограмма устройства в списке изменит свой вид и будет соответствовать статусу "Устройство зарегистрировано и подключено".

Отмена регистрации устройства

Для отмены регистрации устройства:

- 1.** Перейдите на страницу "Контроль устройств".
- 2.** Выберите устройство в списке, вызовите контекстное меню и выберите команду "Снять с регистрации".

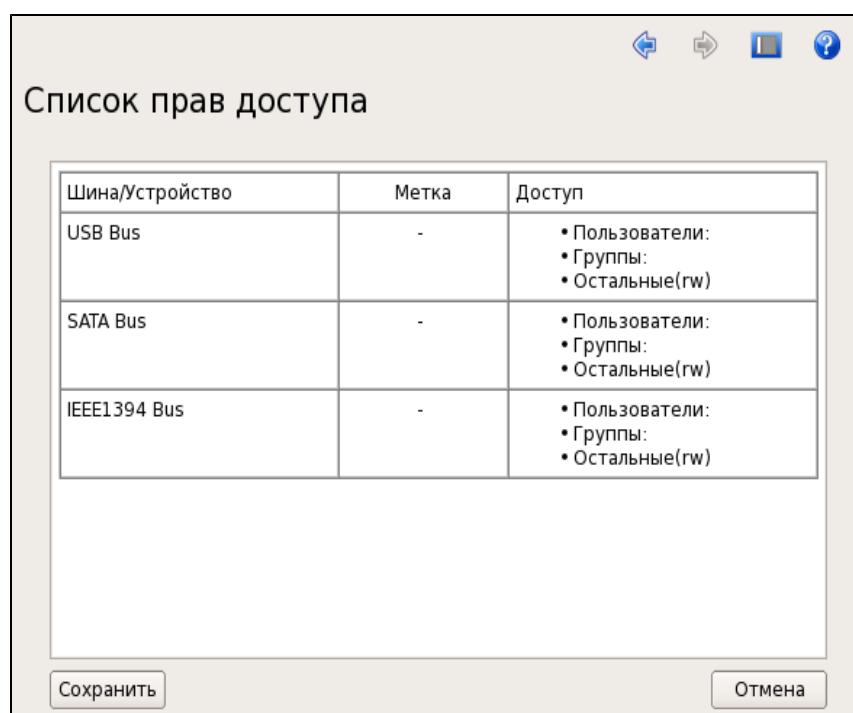
Устройство будет снято с регистрации и удалено из списка контролируемых устройств.

Сохранение настроек прав доступа в файл

Для сохранения настроек:

- 1.** Перейдите на страницу "Контроль устройств".
- 2.** Нажмите кнопку "Экспорт".

Откроется окно предварительного просмотра прав доступа к устройствам:



- 3.** Нажмите кнопку "Сохранить".

Откроется стандартный диалог сохранения файла.

- 4.** Введите имя файла, укажите путь и сохраните файл.

Управление режимом работы подсистемы

Подсистема разграничения доступа к устройствам работает в одном из трех режимов (подробнее см. стр.[17](#)):

- отключено;
- мягкий;
- жесткий.

По умолчанию после установки СЗИ Secret Net LSP включен жесткий режим. При этом для всех USB-, SATA- и IEEE 1394-шин установлены разрешающие права на чтение и запись для всех пользователей и групп.

Изменение режима работы подсистемы осуществляется администратором.

Для изменения режима работы подсистемы:

1. Вызовите панель безопасности и в группе "Настройки приложения" перейдите на страницу "Политики".
2. Выберите в списке политику "Параметры управления устройствами" и установите у параметра "Режим" нужное значение.

Аудит событий

Аудит действий, связанных с доступом субъектов к контролируемым устройствам, ведется по следующим событиям, регистрируемым в журнале аудита:

- Регистрация устройства, снятие с учета.
- Изменение прав доступа к устройству (шине).
- Попытки подключения/отключения устройств.
- Ошибки работы подсистемы.
- Попытки монтирования или демонтирования файловых систем на контролируемых устройствах.

В дополнение к перечисленным выше событиям в журнале аудита могут регистрироваться события с определенным результатом доступа к устройству (результат определяется на основании назначенных прав доступа, см. стр.[61](#)). При этом можно задать регистрацию только событий с неуспешным результатом доступа или с успешным и успешным.

Настройка регистрации событий по результату доступа к устройству выполняется администратором с помощью политики "Параметры управления устройствами".

Для настройки регистрации событий:

1. Вызовите панель безопасности (см. стр.[27](#)) и в группе "Настройки приложений" перейдите на страницу "Политики".
Будет выполнен переход на страницу "Настройка политик".
2. Выберите в списке политику "Параметры управления устройствами" и установите у параметра "Детализация сообщений" нужное значение.

Значение параметра	Описание
Регистрация выключена	События подключения/отключения устройств в журнале аудита не регистрируются
Регистрировать неуспешные попытки доступа	В журнале аудита регистрируются только события с неуспешным результатом доступа к устройствам
Регистрировать все попытки доступа	В журнале аудита регистрируются события с неуспешным и успешным результатом доступа

3. Для сохранения внесенных изменений нажмите кнопку "Применить".

Глава 8

Контроль целостности

В рамках настройки и управления работой механизма контроля целостности администратор выполняет следующие функции:

- ставит на контроль/снимает с контроля ресурсы файловой системы;
- задает/изменяет реакцию СЗИ по фактам нарушения целостности защищаемых ресурсов;
- запускает вручную процедуру проверки;
- выполняет разблокировку входа в систему;
- ведет аудит событий, связанных с нарушением контроля целостности.

Управление работой механизма контроля целостности осуществляется на странице "Управление контролем целостности" панели управления.



Основные процедуры, связанные с управлением работой механизма и описанные далее в этой главе, могут выполняться в режиме командной строки. Для выполнения процедур используется утилита **snaidectl**. Описание утилиты и особенности ее применения приведены в приложении (см. стр. 92).

Для перехода на страницу управления контролем целостности:

- Вызовите панель безопасности и в группе "Контроль целостности" перейдите по ссылке "Управление контролем целостности".

Будет выполнен переход на страницу "Управление контролем целостности":

Объекты файловой системы				
Имя	Размер	Тип	Дата модификации	Контроль целостности
/		Drive	18.05.12 15:54	
.ATEST_...		Folder	18.05.12 14:02	
.config		Folder	18.05.12 14:01	
.dbus		Folder	05.04.12 18:45	
bin		Folder	18.05.12 13:57	
boot		Folder	05.04.12 18:43	
dev		Folder	18.05.12 15:14	
etc		Folder	18.05.12 16:27	
home		Folder	18.05.12 14:05	
lib		Folder	18.05.12 15:14	
lost+fou...		Folder	16.12.11 8:34	

На странице представлен список папок корневого каталога жесткого диска компьютера (объекты файловой системы). Папки, поставленные на контроль, в колонке "Контроль целостности" отмечены пиктограммой и соответствующей записью о реакции на нарушение целостности объекта.

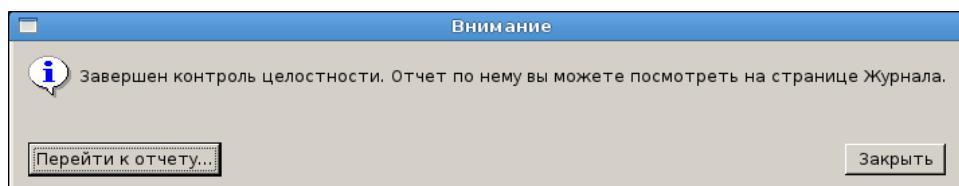
Пиктограмма	Описание
	При нарушении целостности будет выполнена только регистрация изменений. Никаких других действий предпринято не будет
	При нарушении целостности будут выполнены регистрация изменений и восстановление объекта

Пиктограмма	Описание
	При нарушении целостности будут зарегистрированы изменения и заблокирован вход в систему
	При нарушении целостности будут зарегистрированы изменения, восстановлен объект и заблокирован вход в систему
	Объект является системным

Папки, включающие в себя вложенные папки или файлы, поставленные на контроль, имеют отметку в виде звездочки.

- Для просмотра объектов, поставленных на контроль, раскройте папку, помеченную звездочкой.
- Для перехода в режим работы с журналом или управления доступом нажмите соответствующую ссылку в нижней части страницы.
- Для запуска проверки целостности ресурсов, поставленных на контроль, нажмите кнопку "Запустить проверку".

Начнется процесс проверки в соответствии с установленными настройками и после его завершения на экране появится сообщение об окончании проверки:



Для просмотра результатов проверки нажмите в окне сообщения кнопку "Перейти к отчету".

Будет выполнен переход на страницу "Журнал событий". Работа с журналом событий описана в главе 10 (см. стр.[75](#)).

Постановка ресурсов на контроль

Постановка ресурса на контроль включает в себя задание реакции системы защиты на факт нарушения целостности защищаемого объекта. Независимо от выбранной реакции в журнале регистрируются все события, связанные с работой механизмов контроля целостности. Сведения о событиях, регистрируемых в журналах, приведены в приложении (см. стр.[97](#)).

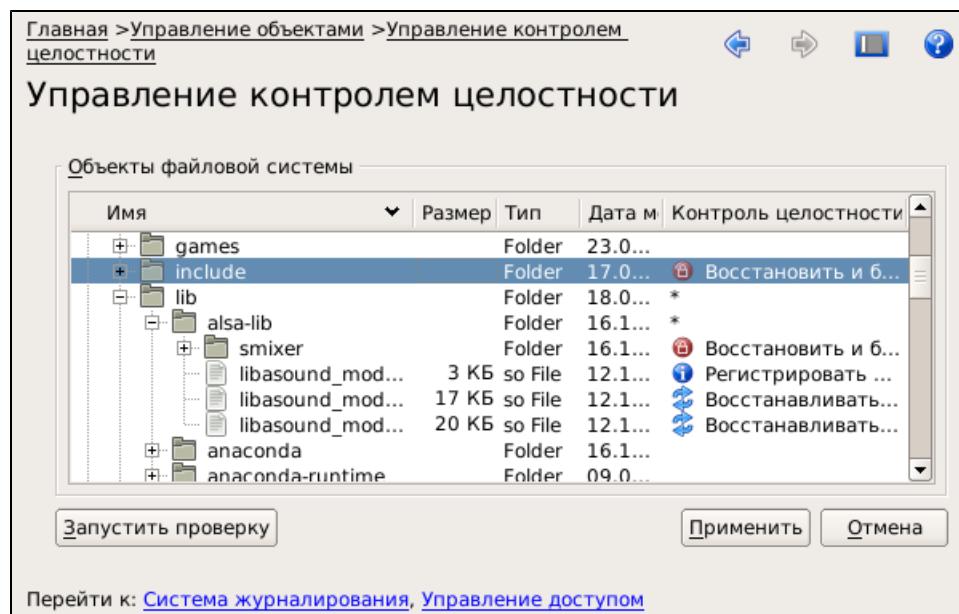
Для постановки ресурса на контроль:

1. Выберите в списке ресурс (папку или файл), вызовите контекстное меню и выберите нужную команду:

Команда	Описание
Регистрировать изменения	При обнаружении нарушения целостности объекта никаких действий СЗИ предпринято не будет
Восстанавливать при изменении	При обнаружении нарушения целостности объект будет восстановлен
Блокировать при изменении	При обнаружении нарушения целостности объекта после перезагрузки или выключения и повторного включения вход в систему будет заблокирован. Разблокировать вход в систему сможет только администратор
Восстановить и блокировать	При обнаружении нарушения целостности объект будет восстановлен, а вход в систему заблокирован. Разблокировать компьютер сможет только администратор

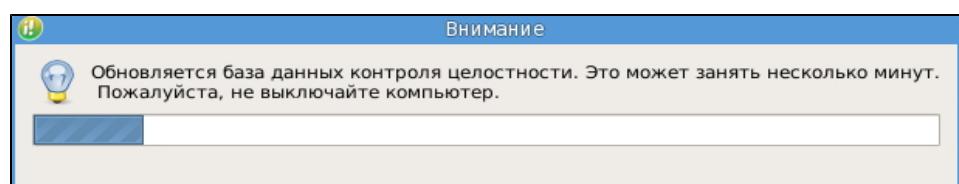
При постановке папки на контроль в проверку будут включены все вложенные в нее объекты.

В колонке "Контроль целостности" у объекта, поставленного на контроль, появится запись, соответствующая выбранной реакции на нарушение целостности:



2. При необходимости повторите действия п.1 для других объектов, подлежащих постановке на контроль.
3. Нажмите кнопку "Применить".

На экране появится предупреждение и начнется обновление базы данных контроля целостности:



Дождитесь завершения обновления базы данных.

4. При необходимости немедленно выполнить проверку объектов, поставленных на контроль, нажмите кнопку "Запустить проверку".

Начнется процесс проверки и после его завершения на экране появится сообщение об окончании проверки (см. описание страницы "Управление контролем целостности" на стр.65).

- Для просмотра результатов нажмите кнопку "Перейти к отчету".
- Для возврата на страницу "Управление контролем целостности" нажмите кнопку "Закрыть".

Снятие ресурса с контроля

Для снятия ресурса с контроля:

1. Выберите на странице "Управление контролем целостности" ресурс, вызовите контекстное меню и выберите команду "Снять с контроля".

В колонке "Контроль целостности" запись о постановке объекта на контроль будет удалена.

2. Нажмите кнопку "Применить".

На экране появится предупреждение и начнется обновление базы данных контроля целостности.

Дождитесь завершения обновления базы данных.

Изменение реакции СЗИ на нарушение целостности

Для изменения реакции:

1. Выберите на странице "Управление контролем целостности" ресурс, вызовите контекстное меню и выберите нужную команду.

В колонке "Контроль целостности" запись о постановке объекта на контроль будет изменена.

2. Нажмите кнопку "Применить".

На экране появится предупреждение и начнется обновление базы данных контроля целостности.

Дождитесь завершения обновления базы данных.

Разблокирование входа в систему

Снять блокировку входа, вызванную нарушением целостности защищаемых объектов, может только администратор с правами суперпользователя root.

Процедура снятия блокировки включает в себя:

- устранение причины блокировки;
- при необходимости переинициализацию базы данных контроля целостности;
- запуск скрипта для разблокирования компьютера.

Для снятия блокировки:

1. Войдите в систему с правами суперпользователя root.

2. Запустите эмулятор терминала.

3. Выполните:

```
/opt/secretnet/bin/snaidectl -i
```

Дождитесь завершения обновления базы данных.

4. Выполните:

```
/opt/secretnet/sbin/snunlock
```

В окне эмулятора терминала появится сообщение об успешном разблокировании компьютера.

5. Проверьте вход в систему под именем зарегистрированного пользователя компьютера.

Аудит контроля целостности

Аудит событий, связанных с работой механизма контроля целостности и восстановления, проводится в соответствии с общим порядком, описанным в главе 10.

Глава 9

Затирание остаточной информации

В рамках работы по управлению механизмом затирания остаточной информации администратор выполняет следующие функции:

- включает/отключает механизм затирания в файловых системах на жестких и внешних дисках;
- настраивает режим работы механизма затирания;
- проводит аудит событий, связанных с затиранием остаточной информации.



Внимание! Во избежание безвозвратной потери данных на внешних носителях, вызванной аварийными ситуациями (например, сбой питания и пр.), при включенном механизме затирания остаточной информации рекомендуется регулярно выполнять резервное копирование данных.

Включение и отключение механизма затирания

При установке Secret Net LSP по умолчанию механизм затирания на жестких дисках выключен. При необходимости администратор может его включить.

Для включения/отключения механизма затирания:

1. Вызовите панель безопасности (см. стр.[27](#)) и перейдите на страницу "Политики".
2. Выберите параметр "Сервис безопасного удаления" политики "Установки сервисов" и измените значение.
 - Для отключения механизма выберите значение "Выключено".
 - Для включения механизма выберите значение "Включено".
 - Для возврата к значению по умолчанию нажмите синюю стрелку, расположенную справа.

Имя	Значение
Плагин управления устройствами	
Параметры управления устройствами	
Режим работы	Жесткий режим
Детализация сообщений	Регистрация выключена
Плагин управления системными сервисами	
Установки сервисов	
Сервис аудита	Включено
Системный сервис печати	Выключено
Сервис печати	Включено
Сервис безопасного удаления	Выключено
Сервис журналирования	Включено
Плагин управления усиленной аутентификацией	
Параметры усиленной аутентификации	
Метод идентификации	Смешанный (используется клавиатура и л...
Метод аутентификации	Пароль введен с клавиатуры или считан с ...
Плагин управления пользователями и группами	

При выборе значения, отличного от значения по умолчанию, название измененного параметра выделяется жирным шрифтом.

3. Для сохранения изменений нажмите кнопку "Применить".

Изменение режима затирания остаточной информации

Расширенные настройки механизма затирания остаточной информации (асинхронный режим) задаются в конфигурационном файле **sntrashd.conf**, хранящемся в папке /opt/secretnet/etc.



Если в указанной папке конфигурационный файл отсутствует, это означает, что по умолчанию механизм затирания работает в синхронном режиме. В этом случае для изменения режима работы механизма необходимо создать конфигурационный файл вручную, указав в нем необходимые настройки (см. ниже).

Для изменения режима затирания:

1. Откройте на редактирование конфигурационный файл /opt/secretnet/etc/sntrashd.conf.
2. Если в конфигурационном файле явно задан синхронный режим, параметр настройки представлен следующей строкой:
/ sync
Для отмены синхронного режима удалите строку.
3. Для задания асинхронного режима затирания для всех объектов файловой системы введите строку с параметром настройки:
/ async
4. Для задания асинхронного режима для какой-либо папки или внешнего запоминающего устройства введите строку с параметром настройки и укажите путь к папке или к папке – точке монтирования устройства, например:
/home/tmp async
или
/var async
5. Сохраните изменения в конфигурационном файле и поместите его в папку /opt/secretnet/etc.
6. Перезагрузите компьютер.

Ручной запуск утилиты безопасного удаления

Независимо от включенного или выключеного режима затирания можно принудительно использовать безопасное удаление с помощью ручного запуска утилит **shred** и **secrm**.

Утилита **secrm** может встраиваться в командное меню файлового менеджера (например, Nautilus, Dolphin или Thunar).



Если в качестве файлового менеджера используется Nautilus, для него должно быть установлено расширение Nautilus actions.

Безопасное удаление неэффективно в сетевых и журналируемых файловых системах.

Запуск утилиты **secrm** в режиме графического интерфейса

При безопасном удалении файлов в режиме графического интерфейса по умолчанию используются 3 прохода записи маскирующей последовательности в файл перед его удалением.

Для запуска утилиты безопасного удаления:

- Запустите командную оболочку и введите команду:
`/opt/secretnet/bin/secrm - -configure`

После запуска утилиты рекомендуется перезапустить файловый менеджер Nautilus командой nautilus-q.

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

Запуск утилиты shred в режиме командной строки

Для удаления файла:

- Запустите командную оболочку и введите команду, указав ключи и имя удаляемого файла:

```
/opt/secretnet/bin/shred [ключ] file
```

Для удаления нескольких файлов укажите их подряд или используйте маску:

```
/opt/secretnet/bin/shred [ключ] file1 file2 file3
```

или

```
/opt/secretnet/bin/shred [ключ] *.txt
```

Используемые ключи:

Ключ	Описание
-u	Удаление и обрезание файла
-n	Количество проходов перезаписи
-z	Добавление нулей в конце файла

Более подробные сведения о применении утилиты **shred** приведены в приложении на стр.[90](#).

Глава 10

Настройка удаленного управления

Secret Net LSP может функционировать совместно с сервером безопасности СЗИ Secret Net 7 (пакет обновления 4 и выше). СЗИ Secret Net 7 в режиме совместного функционирования позволяет осуществлять:

- отображение информации о состоянии компьютеров, защищаемых с помощью Secret Net LSP, и происходящих на них событиях НСД;
- просмотр журнала событий, полученных с защищаемых Secret Net LSP компьютеров;
- выдачу команд для оперативного управления защищаемыми Secret Net LSP компьютерами: блокировка и разблокирование, перезагрузка, выключение.

Подробная информация об использовании данных функций содержится в документе "Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления", входящем в комплект поставки СЗИ Secret Net 7.



Для совместного функционирования Secret Net LSP с сервером безопасности СЗИ Secret Net 7 требуется наличие в системе библиотеки pam_winbind.so, также необходимо включить данный компьютер в домен, связанный с нужным сервером безопасности. Включить компьютер в домен можно стандартными средствами ОС Windows.

Для включения/выключения режима удаленного управления:

Пояснение. После установки Secret Net LSP параметр "Сервис удаленного управления" принимает значение "Включено" по умолчанию.

1. Вызовите панель безопасности (см. стр. 27) и в группе "Настройки приложения" перейдите на страницу "Настройка политик".
На экране появится окно "Настройка политик" (см. стр. 32).
2. В политике "Установки сервисов" установите требуемое значение параметра "Сервис удаленного управления" — "Включено"/"Выключено".

Для включения компьютера в домен Windows:

1. Вызовите панель безопасности (см. стр. 27) и в группе "Настройки приложения" перейдите на страницу "Настройки удаленного управления":

Главная >Настройки приложения >Настройки удаленного управления

Настройки удаленного управления

Расположение сервера безопасности: AD

Логин: [empty]

Пароль: [empty]

Обновлять настройки с сервера безопасности: Каждые 10 минут

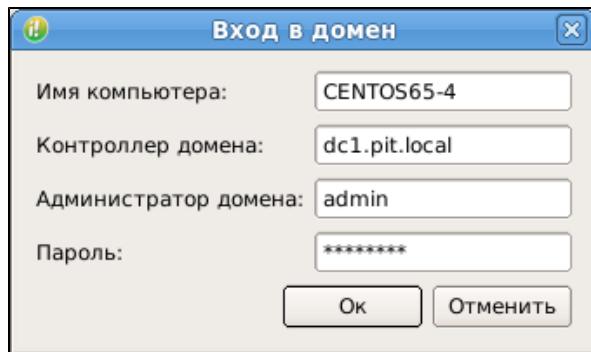
Включить удаленное управление

Войти в домен...

Статус подключения: отключено

2. В открывшемся окне нажмите кнопку "Войти в домен".

На экране появится окно "Вход в домен":



3. Введите в поля окна "Вход в домен":

- "Имя компьютера" — имя компьютера в домене;
- "Контроллер домена" — полное имя контроллера домена (FQDN);
- "Администратор домена" — имя (логин) администратора домена;
- "Пароль" — пароль администратора домена.

4. Нажмите кнопку "Ok".

Совет. Для включения компьютера в домен Windows с использованием командной строки выполните команду:

```
#/opt/secretnet/usr/scripts/domain.sh <hostname> <dc> <login>
<password>
```

где <hostname> — имя компьютера в домене, <dc> — полное имя контроллера домена (FQDN), <login> — имя (логин) администратора домена, <password> — пароль администратора домена.

Для настройки удаленного управления:

1. Включите данный компьютер в домен, связанный с нужным сервером безопасности.
2. Выполните подчинение данного компьютера соответствующему серверу безопасности в программе оперативного управления СЗИ Secret Net.

Подробное описание этой операции см. в документе "Средство защиты информации Secret Net 7. Руководство администратора. Работа с программой оперативного управления".

3. Вызовите панель безопасности (см. стр. 27) и в группе "Настройки приложения" перейдите на страницу "Настройки удаленного управления" (см. рисунок выше).

4. Настройте параметры соединения с сервером безопасности:
 - в поле "Расположение сервера безопасности" выберите тип хранилища данных, используемый сервером безопасности — AD или LDS;
 - в поле "Логин" укажите доменное имя пользователя данного компьютера, под которым он будет входить в систему и подключаться к серверу безопасности, а в поле "Пароль" — пароль этого пользователя;

Пояснение. Для работы в системе другого пользователя значения параметров "Логин" и "Пароль" необходимо изменить. При смене пароля текущего пользователя необходимо изменить значение параметра "Пароль".

- в поле "Обновлять настройки с сервера безопасности" укажите необходимый временной интервал обновления параметров Secret Net LSP — "Никогда"/"Каждые 10 минут"/"Каждые 30 минут"/"Каждый час".

5. Нажмите кнопку "Включить удаленное управление".

При успешном соединении с сервером безопасности название кнопки изменится на "Выключить удаленное управление", а в поле "Удаленное управление" появится значение "Включено". Для отключения режима удаленного управления нажмите эту кнопку еще раз.

При возникновении ошибок на экране появится одно из сообщений:

- "Неверный логин или пароль" — имя пользователя или его пароль указаны неправильно;
- "Этот компьютер не подчинен серверу безопасности" — не выполнено действие **2** данной процедуры;
- "Не удалось подключиться к серверу безопасности" — возникли другие ошибки, например, нет доступа к домену Windows или неправильно настроены сетевые интерфейсы компьютера.

Совет. Для настройки удаленного управления также можно использовать утилиту **snetctl**. Описание утилиты и особенности ее применения приведены в приложении (см. стр.[94](#)).

Глава 11

Аудит

Под аудитом системы защиты понимается отслеживание событий, происходивших в системе за определенный период времени.

Основными задачами аудита являются:

- контроль состояния защищенности системы;
- выявление причин произошедших изменений;
- определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;
- установление времени изменений.



При использовании аудита в Secret Net LSP необходимо учитывать следующие ограничения:

- 1.** Аудит неэффективен в сетевых файловых системах.
- 2.** При удалении файла, поставленного на учет в рамках аудита, и последующем создании другого файла с таким же именем последний будет поставлен на учет только при следующей загрузке системы или после внесения каких-либо изменений в настройки (правила) аудита, так как привязка правила аудита к номеру индексного дескриптора файловой системы выполняется на системном уровне.

Для проведения аудита в СЗИ Secret Net LSP используются системный журнал и журнал аудита.

Системный журнал

Для просмотра системного журнала:

- Вызовите панель управления безопасностью (см. стр. 27) и в группе "Система журналирования" перейдите на страницу "Журнал событий".
- Откроется вкладка "Система":

Дата/Время	Тип сообщения	Важность	Приложение	Сообщение
02/06/2016...	Группа сообще...	Информа...	snaide	
02/06/2016...	Группа сообще...	Информа...	snaide	Mtime : 2011-09-23 19:02:51 , 2015-07-02 ...
02/06/2016...	Группа сообще...	Информа...	snaide	
02/06/2016...	Группа сообще...	Информа...	snaide	Mtime : 2015-04-08 14:12:28 , 2015-07-02 ...
02/06/2016...	Группа сообще...	Информа...	snaide	
02/06/2016...	Группа сообще...	Информа...	snaide	-----
02/06/2016...	Группа сообще...	Информа...	snaide	Detailed information about changes:
02/06/2016...	Группа сообще...	Информа...	snaide	
02/06/2016...	Группа сообще...	Информа...	snaide	restored: /usr/share/backgrounds/default.png
02/06/2016...	Группа сообще...	Информа...	snaide	changed: /usr/share/backgrounds/default.png
02/06/2016...	Группа сообще...	Информа...	snaide	restored: /usr/share/anaconda/pixmaps/splash.png
02/06/2016...	Группа сообще...	Информа...	snaide	changed: /usr/share/anaconda/pixmaps/splash.png

На вкладке представлен список зарегистрированных событий. Каждое событие отображается в списке отдельной записью и содержит следующую информацию:

- дата и время;
- тип сообщения;
- важность;
- приложение, зарегистрировавшее событие;
- описание сообщения.

По умолчанию на странице отображается последняя тысяча записей базы данных. Для вывода предыдущей тысячи записей нажмите кнопку "Вперед". Для возврата к предыдущим просмотренным записям нажмите кнопку "Назад". При перемещении по записям с помощью кнопок "Вперед" и "Назад" с помощью элемента позиционирования отображается текущее положение просматриваемых записей по отношению ко всему списку. Для отображения в журнале нужного диапазона записей сдвиньте движок позиционирования в требуемое положение и нажмите кнопку "Позиция".

Предусмотрена фильтрация отображаемой информации по следующим параметрам:

- по описанию события;
- интервалу времени регистрации событий;
- настраиваемым фильтрам, выбираемым из списка.

Для применения нужного фильтра его необходимо добавить в список и настроить параметры фильтрации.

Для фильтрации по описанию события:

- В поле "Сообщение" введите часть слова текста сообщения и нажмите кнопку "Построить отчет".

Для фильтрации по интервалу времени:

- В поле "Период" из раскрывающегося списка выберите нужное значение:
 - "Весь период";
 - "За неделю";
 - "За месяц";
 - "Заданный".

Если выбрано значение "За неделю", "За месяц" или "Заданный", становятся доступными поля для ввода начальной и конечной даты интервала.

Выберите нужные даты из раскрывающегося календаря и нажмите кнопку "Построить отчет".

Для фильтрации по настраиваемому фильтру

- В поле "Фильтр" выберите из раскрывающегося списка нужный фильтр и нажмите кнопку "Построить отчет".

Для добавления в список нового фильтра:

1. Выберите в поле "Фильтр" значение "Новый фильтр" и нажмите кнопку "Дополнительно" (при этом кнопка фиксируется в нажатом положении).

На странице появится группа полей и кнопок для создания и настройки нового фильтра:

2. Укажите параметры фильтрации.

Поле	Описание
Имя фильтра	Введите имя добавляемого фильтра
Группа сообщений	Выберите группу сообщений из раскрывающегося списка
Тип сообщения	Выберите тип сообщения из раскрывающегося списка
Минимальная важность	Выберите важность сообщения из раскрывающегося списка
Приложение	Введите название или часть названия приложения, зарегистрировавшего событие
Сортировать по	Выберите способ сортировки из раскрывающегося списка
Порядок сортировки	Выберите порядок сортировки (прямой или обратный)

3. Для сохранения настроек фильтра и добавления его в список нажмите кнопку "Сохранить", расположенную справа.

Для скрытия группы полей и кнопок настройки фильтра отожмите кнопку "Дополнительно".

Новый фильтр будет добавлен в список.

Для удаления/редактирования параметров фильтра:

- Выберите в поле "Фильтр" название фильтра, предназначенного для удаления или редактирования, и нажмите кнопку "Дополнительно".
На странице появится группа полей и кнопок для настройки параметров фильтра.
- Для удаления фильтра нажмите кнопку "Удалить", расположенную справа.
Фильтр будет удален из списка.
- Для редактирования параметров фильтра внесите нужные изменения.
Если требуется отменить изменения, нажмите кнопку "Восстановить", расположенную справа.

- 4.** После внесения изменений в настройки фильтра нажмите кнопку "Сохранить", расположенную справа.

Для сохранения отчета в файл:

- 1.** После просмотра сведений, содержащихся в журнале, нажмите кнопку "Сохранить отчет", расположенную в нижнем правом углу страницы.

Откроется стандартный диалог сохранения файла.

Предусмотрено сохранение отчетов в файлах форматов htm, html и txt.

- 2.** Выберите папку для сохранения файла, введите его название и нажмите кнопку "Сохранить".

Для запуска режима интерактивного мониторинга:

- Установите отметку в поле "Интерактивный мониторинг".

Контроль печати

Система Secret Net LSP контролирует вывод файлов на печать. В системном журнале регистрируются следующие события:

- начало печати документа;
- печать страницы документа;
- ошибка печати документа.

Журнал аудита

В журнале аудита хранятся сведения о событиях, удовлетворяющих требованиям правил аудита. Задание правил аудита описано в разделе "Настройка аудита" (см. стр.[81](#)).

Для просмотра журнала аудита:

- 1.** Вызовите панель управления безопасностью (см.стр.[27](#)) и в группе "Система журнализирования" перейдите на страницу "Журнал событий".

Страница откроется на вкладке "Система". Перейдите на вкладку "Аудит":

Дата/Время	Пользователь	Группа	Доступ	Приложение	Объект	Результат
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получение...	SNManager	/tmp	Успех

На вкладке представлен список событий, зарегистрированных в соответствии с настройками аудита.

Каждое событие отображается в списке отдельной записью и содержит следующую информацию:

- дата и время;
- пользователь;
- группа;
- доступ;
- приложение, сгенерировавшее данное событие;
- объект;
- результат выполнения операции;
- детализированное описание события.

По умолчанию на странице отображается последняя тысяча записей базы данных. Для вывода следующей тысячи записей нажмите кнопку "Вперед". Для возврата к предыдущим просмотренным записям нажмите кнопку "Назад".

Для отображения нужного диапазона записей используйте движок позиционирования, как описано в разделе "Системный журнал" (см. стр. 75).

По умолчанию детализированное описание событий в списке не показано.

Для отображения детализации событий:

1. Установите отметку в поле "Показывать секцию "Детализация".

В списке событий появится колонка с детализацией событий. Детализация базируется на системных записях аудита, полученных из ядра.

2. Для просмотра всего содержимого ячейки с детализацией события выделите ее в списке.

Раскроется полное содержимое ячейки:

Дата/Время	Пользователь	Группа	Доступ	Приложение	Объект	Результат	Детализация
18/05/2016...	root	root	Получе...	SNManager	/tmp/g...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/.l...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/.l...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/.l...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/g...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/g...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/g...	Успех	type=SYSCALL msg=sn...
18/05/2016...	root	root	Получе...	SNManager	/tmp/g...	Успех	type=SYSCALL msg=sn...

Предусмотрена фильтрация отображаемой информации по следующим параметрам:

- по описанию события;
- интервалу времени регистрации событий;

- настраиваемым фильтрам, выбираемым из списка.

Для применения нужного фильтра его необходимо добавить в список и настроить параметры фильтрации.

Для фильтрации по описанию события:

- В поле "Строка" введите часть текста сообщения и нажмите кнопку "Построить отчет".

Для фильтрации по интервалу времени:

- В поле "Период" из раскрывающегося списка выберите нужное значение:
 - "Весь период";
 - "За неделю";
 - "За месяц";
 - "Заданный".

Если выбрано значение "За неделю", "За месяц" или "Заданный", становятся доступными поля для ввода начальной и конечной даты интервала.

Выберите нужные даты из раскрывающегося календаря и нажмите кнопку "Построить отчет".

Для фильтрации по настраиваемому фильтру

- В поле "Фильтр" выберите из раскрывающегося списка нужный фильтр и нажмите кнопку "Построить отчет".

Для добавления в список нового фильтра:

- Выберите в поле "Фильтр" значение "Новый фильтр" и нажмите кнопку "Дополнительно" (при этом кнопка фиксируется в нажатом положении).

На странице появится группа полей и кнопок для создания и настройки нового фильтра:

Дата/Время	Пользователь	Группа	Доступ	Приложение	Объект	Результат
18/05/2016...	root	root	Получен...	SNManager	/tmp/g...	Успех
18/05/2016...	root	root	Получен...	SNManager	/tmp	Успех
18/05/2016...	root	root	Получен...	SNManager	/tmp/g...	Успех

- Укажите параметры фильтрации.

Поле	Описание
Имя фильтра	Введите имя добавляемого фильтра

Поле	Описание
Доступ	Выберите тип доступа из раскрывающегося списка
Пользователь	Введите имя пользователя
Приложение	Введите имя приложения
Группа	Введите имя группы
Объект	Введите имя объекта
Результат	Выберите результат из раскрывающегося списка (успешно, неуспешно, любой результат)
Сортировать по	Выберите из раскрывающегося списка способ сортировки
Порядок сортировки	Выберите из раскрывающегося списка порядок сортировки (прямой или обратный)

- 3.** Для сохранения настроек фильтра и добавления его в список нажмите кнопку "Сохранить", расположенную справа.

Для скрытия группы полей и кнопок настройки фильтра отожмите кнопку "Дополнительно".

Новый фильтр будет добавлен в список.

Для удаления/редактирования параметров фильтра:

- 1.** Выберите в поле "Фильтр" название фильтра, предназначенного для удаления или редактирования, и нажмите кнопку "Дополнительно".

На странице появится группа полей и кнопок для настройки фильтра.

- 2.** Для удаления фильтра нажмите кнопку "Удалить", расположенную справа. Фильтр будет удален из списка.

- 3.** Для редактирования параметров фильтра внесите нужные изменения.

Если требуется отменить изменения, нажмите кнопку "Восстановить", расположенную справа.

- 4.** После внесения изменений нажмите кнопку "Сохранить", расположенную справа.

Для сохранения отчета в файл:

- 1.** После просмотра сведений, содержащихся в журнале, нажмите кнопку "Сохранить отчет", расположенную в нижнем правом углу страницы.

Откроется стандартный диалог сохранения файла.

Предусмотрено сохранение отчетов в файлах форматов htm, html и txt.

- 2.** Выберите папку для сохранения файла, введите его название и нажмите кнопку "Сохранить".

Для запуска режима интерактивного мониторинга:

- Установите отметку в поле "Интерактивный мониторинг".

Настройка аудита

Для проведения аудита администратор должен задать правила, определяющие регистрацию тех или иных событий в журнале аудита. Правило описывает, какое действие над объектом каким субъектом и с каким результатом должно быть зарегистрировано в журнале. При этом задание правил разделено на настройку аудита объектов и настройку аудита сети.

Настройка аудита объектов заключается в следующем: для определенного объекта файловой системы (каталога или файла) задается правило. В нем указывается субъект (пользователь или группа) и составляется перечень действий (например, чтение или переименование файла/каталога, удаление и пр.), завершающихся с определенным результатом ("успех" или "ошибка"). Для

объекта может быть задано произвольное количество правил. Совокупность правил, заданных для объектов, составляет общую политику аудита объектов.

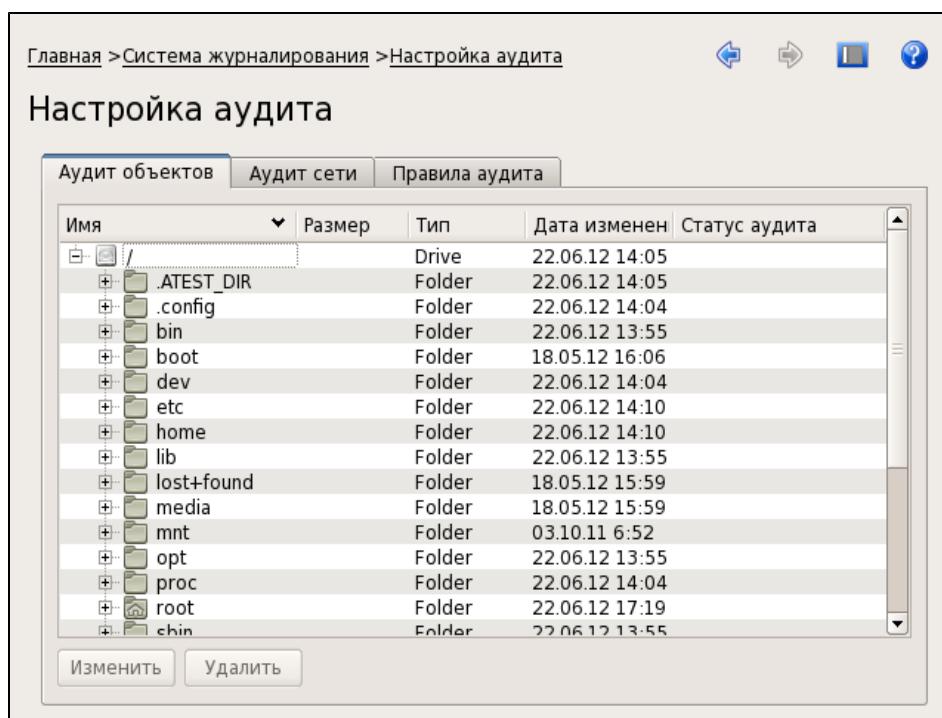
Настройка аудита сети заключается в задании правил для выбранных субъектов (пользователей и групп). Правило определяет сетевые операции, завершающиеся определенным результатом и подлежащие регистрации в журнале. Совокупность правил, заданных для субъектов, составляет общую политику аудита сети.

Для настройки правил аудита:

- Вызовите панель управления безопасностью (см. стр. 27) и в группе "Система журналирования" перейдите на страницу "Настройка аудита".

Откроется страница "Настройка аудита", содержащая 3 вкладки:

Вкладка	Описание
Аудит объектов	Настройка правил аудита объектов
Аудит сети	Настройка правил аудита сети
Правила аудита	Просмотр сводной таблицы правил аудита



- Для настройки правил аудита перейдите на соответствующую вкладку.

Аудит объектов

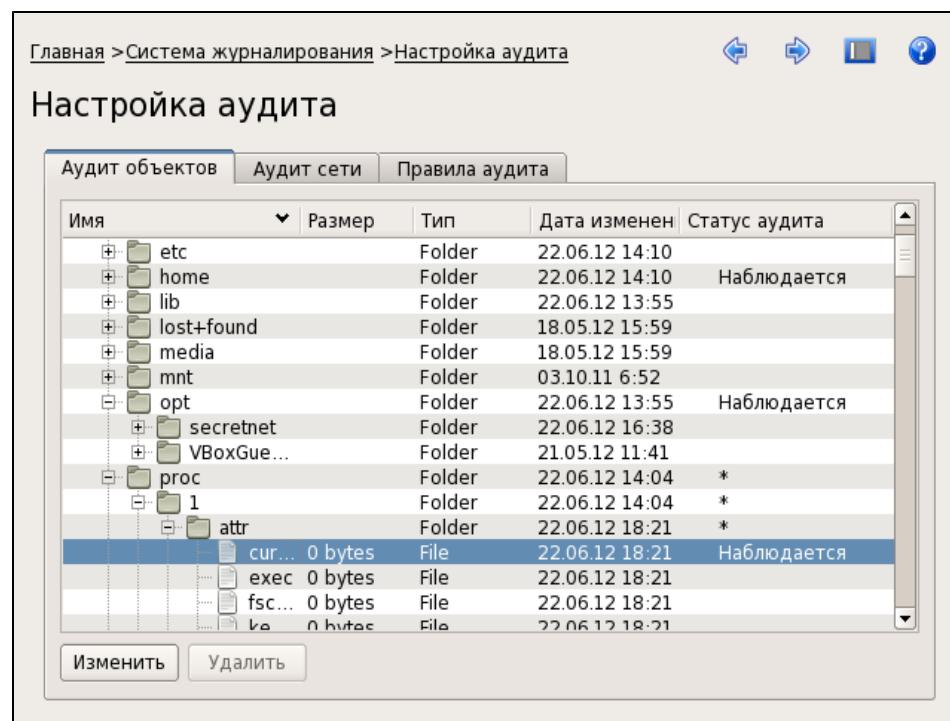
Для настройки аудита объектов:

- На странице "Настройка аудита" перейдите на вкладку "Аудит объектов".

На вкладке отображается корневая папка объектов файловой системы.

У папок корневого каталога, поставленных на контроль в рамках аудита, в колонке "Статус аудита" отображается отметка "Наблюдается".

Если на контроль поставлен вложенный объект (каталог или файл), родительский объект (папка) в колонке "Статус аудита" имеет отметку в виде звездочки.

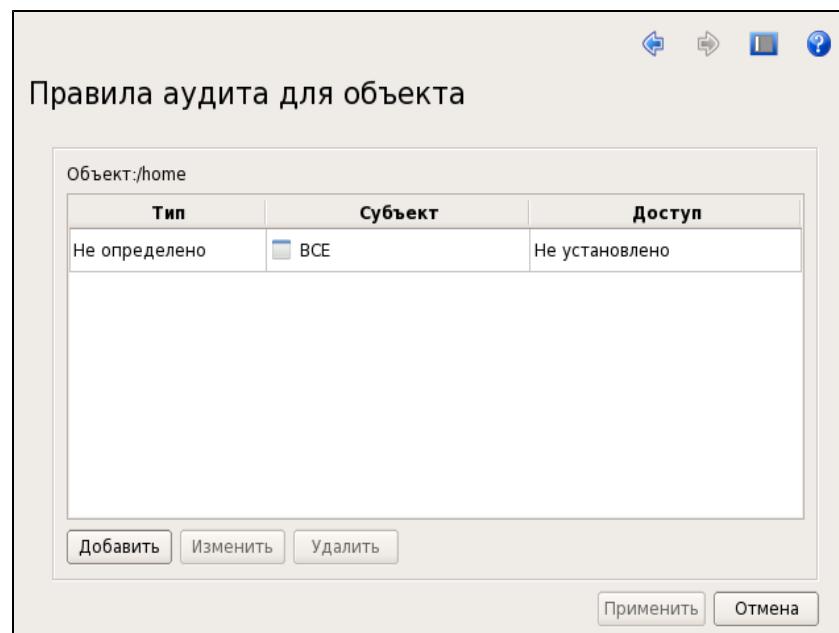


2. Для задания/редактирования правила (или правил) выберите объект, вызовите контекстное меню и выберите команду "Настроить правила".



Если в выбранном объекте (каталоге) находится символьная ссылка или сам объект является символьной ссылкой, то на объекты, на которые указывает ссылка, правила аудита распространяться не будут, так как правила применяются только к действительным файлам и каталогам. При этом сам файл — символьная ссылка будет поставлен на контроль. Если выбранный объект является символьной ссылкой, после выбора команды "Настроить правила" будет выведено соответствующее предупреждение.

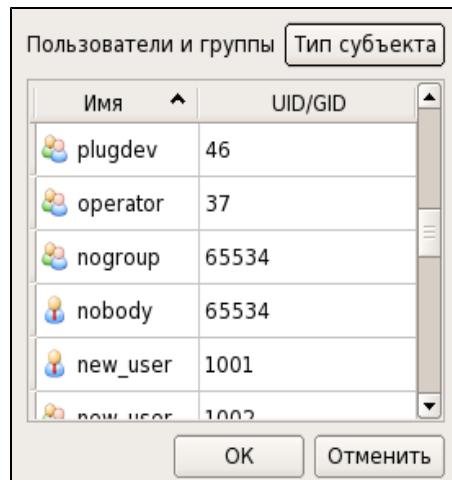
Появится окно "Правила аудита для объекта":



Если правила аудита для данного объекта не настраивались, при первом открытии окна "Правила аудита для объекта" в нем будет отображаться шаблон правила для всех субъектов (см. рисунок выше). При этом параметр "тип" (успех/ошибка) не определен, параметр "доступ" — не установлен.

3. Для добавления нового правила нажмите кнопку "Добавить".

Появится окно "Пользователи и группы":

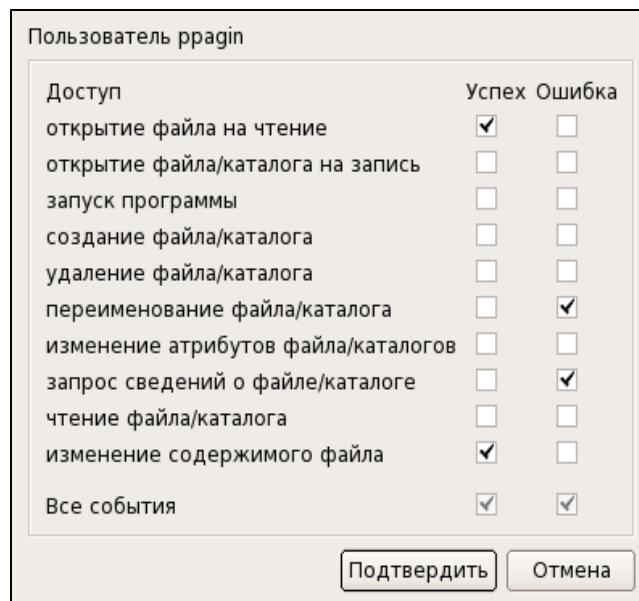


В окне представлен список всех субъектов (пользователей и групп).

Для удобства можно использовать фильтр отображения в списке только пользователей или только групп. Для этого нажмите кнопку "Тип субъекта" и в раскрывающемся списке удалите ненужную отметку.

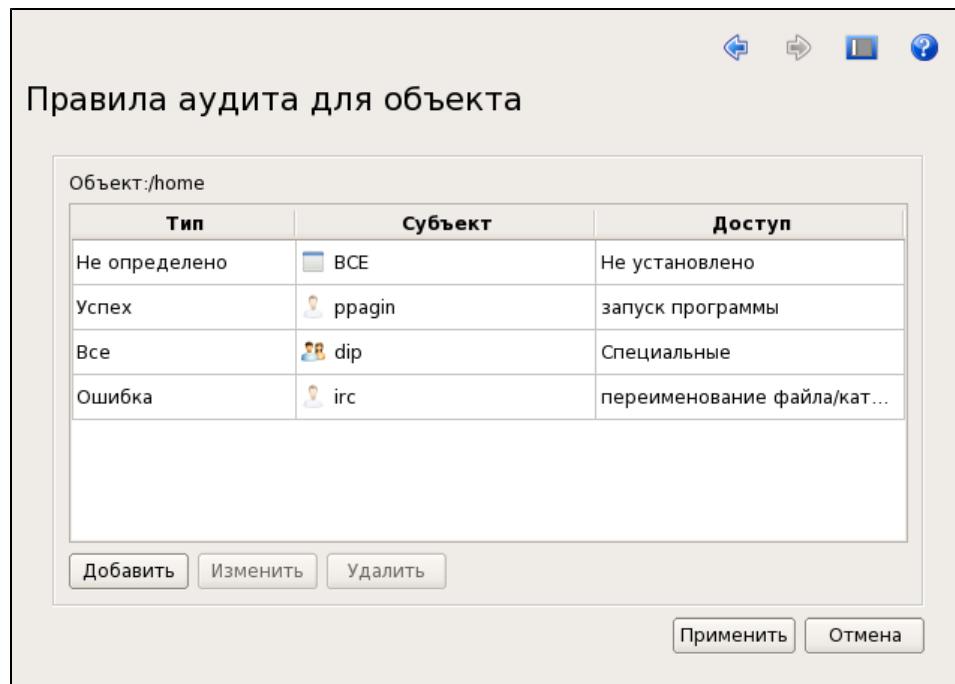
4. Выберите субъект и нажмите кнопку "OK".

Появится окно настройки правила:



5. Установите нужные отметки и нажмите кнопку "Подтвердить".

Окно закроется, и в окне "Правила аудита для объекта" появится строка добавленного правила:



- 6.** Для изменения правила выберите его и нажмите кнопку "Изменить".

Для удаления правила выберите его в списке и нажмите кнопку "Удалить".

- 7.** После добавления всех правил нажмите кнопку "Подтвердить".

Окно "Правила аудита для объекта" закроется, и на странице "Настройка аудита" в списке объектов в колонке "Статус аудита" появится отметка о постановке объекта на контроль.

- 8.** При необходимости выберите другой объект и настройте для него правила аудита в соответствии с пп. **2—7** данной процедуры.

Для снятия объекта с контроля:

- На вкладке "Аудит объектов" выберите объект, поставленный на контроль, вызовите контекстное меню и выберите команду "Очистить".

Объект будет снят с учета и в колонке "Статус аудита" отметка о постановке объекта на учет будет удалена.

Аудит сети

Для настройки аудита сети:

- На странице "Настройка аудита" перейдите на вкладку "Аудит сети".

На вкладке отображаются правила аудита сети:

Тип	Субъект	Доступ
Не определено	Все	Не установлено
Ошибка	backup	Специальные
Успех	Ip	Специальные
Ошибка	ppagin	создание сокета
Успех	ssh	Специальные

Если правила аудита сети не настраивались, при первом открытии вкладки "Аудит сети" в ней будет отображаться шаблон правила для всех субъектов (см. рисунок выше). При этом параметр "тип" (успех/ошибка) не определен, параметр "доступ" — не установлен.

- Для добавления нового правила нажмите кнопку "Добавить".

Появится окно "Пользователи и группы".

- Выберите субъект и нажмите кнопку "OK".

Появится окно настройки правила:

- Задайте правило для выбранного субъекта и нажмите кнопку "Сохранить".

!
Если для работы с сетевыми соединениями программа использует файловые операции чтения/записи, прием и передача датаграмм регистрироваться не будет.

Окно настройки правила закроется, и на вкладке "Аудит сети" появится добавленное правило.

- Для изменения/удаления правила выберите его и нажмите кнопку "Изменить"/"Удалить".

Просмотр правил аудита

- Для просмотра сводной таблицы правил аудита объектов и аудита сети перейдите на вкладку "Правила аудита":

Главная > Система журналирования > Настройка аудита

Настройка аудита

Аудит объектов Аудит сети Правила аудита

* Все пользователи и группы

* Пользователь backup

Правила сети:

Пресеты	Результат
установление сетевого соединения	Ошибка

* Пользователь daemon

Пресеты	Результат	Объекты
создание файла/каталога	Ошибка	◦ /proc/1/attr/current

* Пользователь irc

Пресеты	Результат	Объекты
переименование файла/каталога	Ошибка	◦ /home

Приложение

Утилиты Secret Net LSP

В данном разделе приведено описание специализированных утилит, используемых в защитных подсистемах Secret Net LSP, а также особенности их применения для выполнения основных операций в режиме командной строки.

Приведенные ниже утилиты используются в следующих задачах:

- настройка параметров политик;
- управление персональными идентификаторами;
- безопасное удаление;
- разграничение доступа к устройствам;
- контроль целостности объектов файловой системы;
- настройка правил аудита;
- управление режимом аутентификации;
- настройка удаленного управления;
- резервное копирование;
- работа с журналами.

Утилиты расположены в каталогах /opt/secretnet/bin и /opt/secretnet/sbin (утилиты snnetpamcfg и snnetctl).

Настройка параметров политик

Для выполнения настройки параметров политик (см. стр.[44](#), стр.[53](#)) используется утилита **snpolctl**, расположенная в каталоге /opt/secretnet/bin.

Примеры команд:

<code>snpolctl -p token_mgr -c authentication,strength,1</code>	Установить значение параметра "Усиленная аутентификация" — "Включено"
<code>snpolctl -p token_mgr -c authentication,strength,0</code>	Установить значение параметра "Усиленная аутентификация" — "Выключено"
<code>snpolctl -p control -c access_control,mode,1</code>	Установить значение параметра "Режим работы" подсистемы разграничения доступа к объектам файловой системы — "Включено"
<code>snpolctl -p control -c access_control,mode,0</code>	Установить значение параметра "Режим работы" подсистемы разграничения доступа к объектам файловой системы — "Выключено"

Управление персональными идентификаторами

Для выполнения операций с персональными идентификаторами (см. стр.[45](#)) используется утилита **sntokenctl**, расположенная в каталоге /opt/secretnet/bin.

Ключ	Описание
-l	--list Выводит список всех зарегистрированных персональных идентификаторов с привязкой к пользователям. В составе нескольких команд всегда выполняется первой
-b <ПОЛЬЗОВАТЕЛЬ>	--bind <ПОЛЬЗОВАТЕЛЬ> Привязывает новый идентификатор к пользователю. Не используется с ключами "-P", "-K", "-c" и "-u"

Ключ		Описание
-с <ПОЛЬЗОВАТЕЛЬ>	--change <ПОЛЬЗОВАТЕЛЬ>	Меняет ключи пользователя. Не используется с ключами "-Р", "-К", "-в" и "-у"
-а	--set -acls	Только для идентификаторов Rutooken. Защищает файл привязки на идентификаторе PIN-кодом. Не используется с ключами "-Р" и "-К"
-р	--write-password	Записывает пароль пользователя в идентификатор. Используется с ключом "-в"
-к	--write-key	Записывает закрытый ключ в идентификатор. Используется с ключом "-в". Если у пользователя еще нет пары ключей, она генерируется. Если у пользователя уже есть пара ключей, необходимо предъявить идентификатор, в котором хранится закрытый ключ
-s <НОМЕР>	--serial <НОМЕР>	Выполняет операцию с идентификатором с указанным серийным номером. Используется с ключами "-у", "-Р", "-К", "-г" и "-R"
-Р	--add-password	Дозаписывает пароль на уже привязанный идентификатор. Не используется с ключами "-в", "-R" и "-у"
-К	--add-key	Дозаписывает ключ на уже привязанный идентификатор. Если у пользователя еще нет пары ключей, она генерируется. Если у пользователя уже есть пара ключей, потребуется предъявить идентификатор, в котором хранится закрытый ключ. Не используется с ключами "-в", "-г" и "-у"
-г	--remove-password	Удаляет пароль пользователя из привязанного идентификатора
-R	--remove-key	Удаляет закрытый ключ из ранее привязанного идентификатора
-у	--unbind	Отвязывает идентификатор. Не используется с ключами "-Р", "-К" и "-в"
-d	--delete	Удаляет данные Secret Net LSP из идентификатора. Используется с ключом "-у"
-е	--erase	Удаляет данные из идентификатора. Идентификатор не должен быть присвоен пользователю
-L	--lock	Блокирует идентификатор
-U	--unlock	Разблокирует идентификатор

Ключ	Описание	
-B<ПОЛЬЗОВАТЕЛЬ>	Назначает ранее привязанный идентификатор (например, в Secret Net для Windows) ПОЛЬЗОВАТЕЛЮ. У ПОЛЬЗОВАТЕЛЯ не должно быть присвоенных идентификаторов. Обрабатываемый идентификатор проверяется на предмет наличия пароля и ключа. Если что-либо обнаруживается, эти данные привязываются к ПОЛЬЗОВАТЕЛЮ. При указании данного ключа все остальные ключи игнорируются	
-S	--change-password	Меняет пароль пользователя на пароль, хранящийся в идентификаторе. Используется совместно с ключом "-B"

Примеры команд:

sntokenctl -b test_user -p	Привязать новый идентификатор к пользователю test_user и записать в идентификатор пароль
sntokenctl -u -s 12345678	Отвязать идентификатор с серийным номером 12345678
sntokenctl -L -s 12345678	Разблокировать идентификатор с серийным номером 12345678

Безопасное удаление

Для безопасного удаления файлов (см. стр. 69) используется утилита **shred**, расположенная в каталоге /opt/secretnet/bin.

Ключ		Описание
-f	--force	Изменяет права, разрешая запись, если необходимо
-n	--iterations=N	Переписывает N раз вместо (3) по умолчанию
	--random-source=ФАЙЛ	Получает случайные числа из файла (по умолчанию /dev/urandom)
-s	--size=N	Очищает N байт (возможны суффиксы вида K,M,G)
-u	--remove	Обрезает и удаляет файл после перезаписи
-v	--verbose	Показывает прогресс
-x	--exact	Не округляет размеры файлов до следующего целого блока . По умолчанию для необычных файлов
-z	--zero	Перезаписывает в конце нулями, чтобы скрыть перемешивание
	--help	Выводит справочную информацию о применении утилиты
	--version	Выводит информацию о версии утилиты

Для удаления обычных файлов используется ключ --remove (-u).



В некоторых файловых системах применение утилиты **shred** не дает гарантии эффективного безопасного удаления. Примерами таких файловых систем являются:

- Журналирующие файловые системы в составе операционных систем AIX и Solaris: JFS, ReiserFS, XFS,Ext3 и др. В таких системах утилита **shred** работает корректно, если в них отключен режим кеширования.
- Файловые системы, которые записывают избыточные данные и сохраняют работоспособность даже в случаях неудачных записей, например, файловые системы, основанные на технологии RAID.

- Файловые системы, которые создают снимки состояния, например, NFS-сервер от Network Appliance.
- Файловые системы, которые кешируют файлы во временных хранилищах, например, клиенты NFS версии 3.
- Сжатые файловые системы.

Разграничение доступа к устройствам

Для разграничения и контроля прав доступа к устройствам (см. стр. 58) используется утилита **sndevctl**, расположенная в каталоге /opt/secretnet/bin.

Ключ		Описание
-l	--list	Отображает список шин и устройств
	--verbose	Отображает детализированный список шин и устройств
-r	--rules	Отображает правила для шин и устройств
	--dev-id	Отображает детализированную информацию о правилах для устройств
	--bus-id	Отображает детализированную информацию о правилах для шин
-a	--add	Добавляет устройство
-d	--delete	Удаляет устройство
-s	--set	Устанавливает права доступа для шины или устройства
-v	--verbose	Выводит более детальную информацию
-h	--help	Выводит справочную информацию о применении утилиты

Параметры для команд:

Параметр	Описание
--bus-id	Идентификатор для шины
--device-id	Идентификатор для устройства
--idVendor	Идентификатор производителя
--idProduct	Идентификатор продукта
--vendor	Производитель
--product	Продукт
--serial	Серийный номер
-u; --user	Данные пользователя
-g; --group	Данные группы

Примеры команд:

sndevctl --list	Вывести список всех устройств
sndevctl --lv	Вывести детализированный список всех устройств
sndevctl --rules	Вывести правила для всех устройств
sndevctl --rules --bus-id=usb	Вывести детализированную информацию о правилах для устройств, подключаемых к USB-шине
sndevctl --rules --dev-id=1	Вывести детализированную информацию о правилах для устройства 1
sndevctl --add 8:0	Добавить устройство с идентификаторами 8 (major) и 0 (minor)

<code>snctl --set --dev-id=1 --label="Kingston" --user=test:write --group=test:read --default=none</code>	Установить права доступа к устройству 1 и присвоить устройству метку Kingston. Права доступа: для пользователя test — запись; для группы test — чтение; для остальных — нет доступа
<code>snctl --set --bus-id=usb --user=test:write --group=test:read --default=none</code>	Установить права доступа к USB-шине: для пользователя test — запись; для группы test — чтение; для остальных — нет доступа

Контроль целостности

Для выполнения процедур, связанных с контролем целостности объектов файловой системы (см. стр. [65](#)), используется утилита **snaidectl**, расположенная в каталоге /opt/secretnet/bin.

Ключ		Описание
-c	--check	Выполняет контроль целостности. Если указана данная опция, остальные опции учитываться не будут
-l	--list=[ФАЙЛ,...]	Показывает файлы, для которых включен контроль целостности. Может принимать аргумент — разделенный запятыми список файлов. Данную опцию можно указать только один раз и она всегда обрабатывается первой
-s	--set <ФАЙЛЫ=ФЛАГ:...>	Включает контроль целостности для файлов. Список файлов разделен запятыми. Если данная опция указана несколько раз, опции будут объединены в один запрос. Допустимые флаги: <ul style="list-style-type: none"> • NORMAL — обнаруживать и протоколировать любые изменения файла; • NORMALBACK — обнаруживать, протоколировать и отменять любые изменения файла (восстановить файл из резервной копии); • NORMALLOCK — если файл изменен, запротоколировать событие и заблокировать систему; • NORMALBACKLOCK — восстановить измененный файл и заблокировать систему
-u	--unset <ФАЙЛ,...>	Отключает контроль целостности для файлов. Список файлов разделен запятыми. Если данная опция указана несколько раз, опции будут объединены
-U	--unset-all	Отключает контроль целостности для всех объектов. Данную опцию нельзя использовать совместно с другими
-i	--init	Переинициализирует базу данных контроля целостности. Если указан данный ключ, остальные ключи не учитываются



В некоторых случаях, в зависимости от структуры каталогов и наличия символьических ссылок, при выполнении контроля целостности с ключом "-c" (-check) в выводимом отчете значение параметра Total number of files может отличаться от действительного в сторону увеличения.

Примеры команд:

snaidectl --list=file1,file2	Показать параметры для файлов file1 и file2
snaidectl --s file1=NORMAL:file2=NORMALBACK	Включает контроль для файлов file1 и file2 с флагами NORMAL и NORMALBACK соответственно
snaidectl -u file1	Отключает контроль для файла file1

Исключения:

snaidectl -s /etc=NORMAL	Включает контроль для каталога /etc
snaidectl -u /etc/modules.conf	Отключает контроль для файла /etc/modules.conf

Правила аудита

Для просмотра и редактирования правил аудита (см. стр. 75) используется утилита **snauditctl**, расположенная в каталоге /opt/secretnet/bin.

Ключ		Описание
-l	--list	Показывает текущие правила аудита
-A	--add	Добавляет правило аудита
-m	--modify=ID	Изменяет правило с идентификатором ID
-d	--delete=ID	Удаляет правило с идентификатором ID
-D	--delete-all	Удаляет все правила
-c	--comment=ТЕКСТ	Устанавливает текстовый комментарий для правила. Используется с ключами "-A" и "-m"
-u	--user =ПОЛЬЗОВАТЕЛЬ, ...	Разделенный запятыми список пользователей, к которым применяется правило
-g	--group=ГРУППА	Разделенный запятыми список групп, к которым применяется правило
-o	--object=ОБЪЕКТ	Контролируемый ОБЪЕКТ (файл или каталог). Если требуется отслеживать несколько файлов и/или каталогов, укажите данную опцию несколько раз (для каждого объекта)
-a	--action =ДЕЙСТВИЕ,...	Разделенный запятыми список действий, отслеживаемых правилом. Возможные действия: <ul style="list-style-type: none">• Read – чтение файла или каталога;• Stat – запрос свойств файла или каталога;• Write – запись в файл;• Chattr – изменение свойств файла или каталога;• Rename – переименование файла или каталога;• Delete – удаление файла или каталога;• Create – создание файла или каталога;• Exec – запуск программы;• Socket – открытие сокета;• Dgram – отправка/прием датаграмм;• Connect – установление сетевого соединения;• Openr – открытие файла на чтение;• Openw – открытие файла/каталога на запись

Если требуется отслеживать операции записи в каталоге, укажите действие openw.

Если опции "-u" и "-g" не указаны, создаваемое правило применяется ко всем пользователям.

Примеры команд:

snauditctl -A -o /etc/passwd -a openr	Следить за попытками чтения файла /etc/passwd любым пользователем. Показать параметры для файлов file1 и file2
snaudit -A -o /sbin -a exec -u test_user	Следить за попытками пользователя запустить программу из каталога /sbin

Управление режимом аутентификации

Для управления режимом аутентификации (см. стр.[52](#)) используется утилита **snnetparamcfg**, расположенная в каталоге /opt/secretnet/sbin.

Параметр	Описание
--disable-network	Изменяет настройки рабочих модулей на необходимые для локальной аутентификации
--enable-network	Изменяет настройки рабочих модулей на необходимые для доменной аутентификации
--status	Возвращает текущий режим аутентификации (domain или local)
--help	Выводит справочную информацию о применении утилиты

Настройка удаленного управления

Для настройки удаленного управления (см. стр.[72](#)) используется утилита **snnetctl**, расположенная в каталоге /opt/secretnet/sbin.

Ключ		Описание
-e	--enable	Включает режим удаленного управления. В обязательном порядке также необходимо указать параметры -l, -u, -p
-d	--disable	Выключает режим удаленного управления
-s	--status	Показывает текущее состояние соединения с сервером безопасности
-l	--location <location>	Определяет тип хранилища данных, используемый сервером безопасности. <location> может принимать значения AD или LDS
-u	--login <login>	Определяет доменное имя пользователя данного компьютера, под которым он будет входить в систему
-p	--password <password>	Определяет пароль доменного пользователя
-h	--help	Выводит справочную информацию о применении утилиты

Примеры команд:

snnetctl -e -l AD -u user1 -p qwerty123	Подключиться к серверу безопасности с типом хранилища данных AD, под именем пользователя user1 с паролем qwerty123
snnetctl --disabler	Выключить режим удаленного управления
snnetctl -s	Показать текущее состояние соединения с сервером безопасности

Резервное копирование настроек Secret Net LSP

Для выполнения операций резервного копирования и восстановления используется утилита **snbckctl**, расположенная в каталоге /opt/secretnet/bin.

Объектами копирования и восстановления являются:

- данные о пользователях и группах;
- база данных настроек Secret Net LSP;
- содержимое журналов.

Ключ		Описание
-l	--list	Выводит список имеющихся резервных копий. Данную опцию можно указать только один раз и она всегда обрабатывается первой
-b	--backup=[ОБЪЕКТ,...]	Выполняет резервное копирование объектов (список, разделенный запятыми). Если объекты не указаны, выполняет полное резервное копирование. Допустимые объекты: <ul style="list-style-type: none"> • Users – данные о пользователях и группах; • Snsettings – база данных настроек Secret Net LSP; • Logs – журналы ; • Не может использоваться с опциями "-r" и "-d"
-d	--delete	Удаляет резервную копию. Требуется указание опции "-i"
-r	--restore=[ОБЪЕКТ,...]	Восстанавливает указанные объекты из резервной копии (список, разделенный запятыми). Требуется указание опции "-i". Если объекты не указаны, пытается выполнить полное восстановление. Не может использоваться с опциями "-b" и "-d"
-i	--id <ID>	Указывает ID резервной копии. Используется совместно с опциями "-r" и "-d"
-c		Комментарий для новой резервной копии. Используется совместно с опцией "-b"

Примеры команд:

snbckctl -b	Выполняет полное резервное копирование
snbckctl -r -I 10	Выполняет полное восстановление из резервной копии с ID 10
snbckctl --backup=users,snsettings	Выполняет резервное копирование базы данных пользователей и настроек Secret Net LSP
snbckctl -i 11 --restore=users	Восстанавливает данные о пользователях из резервной копии с ID 11

Экспорт и импорт настроек Secret Net LSP

Для экспортации настроек:

1. Выполните резервное копирование настроек Secret Net LSP:

```
#snbckctl -b
```

или

```
#snbckctl --backup
```

Архив резервной копии сохраняется в каталоге /opt/secretnet/usr/backup и имеет имя <ID_резервной_копии>.tar.gz.

2. Выполните вывод резервных копий:

```
#snbckctl -l
```

3. Выполните экспорт необходимой резервной копии:

```
#snbckctl -e -i <ID_резервной_копии>
```

или

```
#snbckctl --export --id <ID_резервной_копии>
```

Для импорта настроек:

1. Скопируйте файл архива резервной копии в каталог /opt/secretnet/usr/backup/.

2. Выполните импорт резервной копии:

```
#snbckctl -m -i <ID_резервной_копии>
```

или

```
#snbckctl --import --id <ID_резервной_копии>
```

где ID_резервной_копии – это имя файла архива без расширения.

3. Выполните восстановление настроек из импортированной резервной копии:

```
#snbckctl -r -i <ID_резервной_копии>
```

где ID_резервной_копии – это имя каталога, полученного в результате выполнения операции импорта (см. действие 2).

Перенос конфигурации Secret Net LSP предыдущих версий на Secret Net LSP 1.5

С помощью утилиты **snbckctl**, расположенной в каталоге /opt/secretnet/bin, можно выполнить сохранение конфигурации Secret Net LSP предыдущих версий и ее перенос на Secret Net LSP 1.5 при обновлении версии СЗИ.

Для переноса конфигурации:

1. Выполните вход в систему под учетной записью root.
2. Сохраните конфигурацию Secret Net LSP. Для этого в командной оболочке выполните команду:

```
#snbckctl -b
```

Конфигурация сохраняется в каталоге /opt/secretnet/usr/backup/<ID>, где – <ID> это сгенерированный системой номер резервной копии.

3. Скопируйте созданную резервную копию в папку пользователя. Для этого в командной оболочке выполните команду:

```
#cp -r /opt/secretnet/usr/backup/<ID> /home/user/
```

4. Удалите Secret Net LSP предыдущей версии. Для этого необходимо запустить установочный файл и согласиться на удаление ПО.

5. Обновите ОС до необходимой версии ядра.

6. Установите Secret Net LSP 1.5.

7. Скопируйте созданную резервную копию в каталог /opt/secretnet/usr/backup. Для этого в командной оболочке выполните команду:

```
#cp -r /home/user/<ID> /opt/secretnet/usr/backup/
```

8. Восстановите конфигурацию из резервной копии. Для этого в командной оболочке выполните команду:

```
#snbckctl -r -i <ID>
```

В случае возникновения ошибок выполните команду повторно.

Работа с журналами

Для работы с журналами используется утилита **snjrn1**. С помощью утилиты можно выполнять следующие операции:

- просматривать записи системного журнала и журнала аудита";
- удалять записи из базы данных журналов;
- экспорттировать записи журналов в файл;
- импортировать записи журналов из файла.

Утилита вызывается из каталога /opt/secretnet/bin.

Ключ		Описание
-h	--help	Выводит справочную информацию о применении утилиты
-S	--syslog	Использование базы данных системного журнала
-A	--audit	Использование базы данных журнала аудита
-w	--view	Только просмотр выбранных записей. Если временной период не указан, по умолчанию берется текущий день
-e	--export=ФАЙЛ	Экспорт журналов из базы в файл
-d	--delete	Удаление экспортированных записей из базы данных
-i	--import=ФАЙЛ	Импорт журналов из файла в базу данных
-D	--delete-only	Только удаление записей из базы без экспорта. Ключ нельзя использовать совместно с ключами "-i" и "-e"
-f	--from=ДАТА	Просмотр/экспорт/удаление записей, созданных не ранее чем ДАТА (ДД.ММ.ГГГГ)
-t	--to=ДАТА	Просмотр/экспорт/удаление записей, созданных не позднее чем ДАТА (ДД.ММ.ГГГГ). Удаляет пароль пользователя из привязанного идентификатора
-v	--verbose	Вывод отладочных сообщений

События, регистрируемые в системном журнале

Все события, регистрируемые в системном журнале, разделяются по сообщениям на группы. В свою очередь внутри групп события разделяются по типам сообщений.

Кроме того, каждое событие имеет определенный уровень важности. События, соответствующие одному и тому же уровню важности, в журнале отображаются записью определенного цвета.

В данном разделе приведены используемые в Secret Net LSP уровни важности событий и группы и типы сообщений.

Уровни важности событий

Emergency/Очень важное
Alert/Тревога
Critical/Критическое
Error/Ошибка
Warning/Предупреждение
Notice/Замечание
Info/Информация
Debug/Отладка

Группы сообщений

System messages/Системные сообщения
Common Secret Net events/Общие события Secret Net LSP
Authentication/Аутентификация и идентификация
Integrity/Контроль целостности
Backup/Резервное копирование
Printing/Система печати
Trash daemon/Сервис очистки файловой системы
Journal subsystem/Сервис журналирования
Common control/Общие настройки
Audit control/Управление аудитом
Service control/Управление сервисами
User control/Управление пользователями
Integrity control/Управление контролем целостности
Backup control/Управление резервным копированием
Access control/Управление контролем доступа
Strengthen authentication control/Управление усиленной аутентификацией
Kernel/События модулей ядра

Типы сообщений

Группа событий "Системные сообщения"

System message/Системное сообщение

Группа событий "Общие события Secret Net LSP"

Common Secret Net group msg/Группа событий общих сообщений Secret Net LSP
Not authorized access/Несанкционированное действие
Warning/Предупреждение
Debug/Отладочное сообщение
Computer blocked/Компьютер заблокирован
Computer unblocked/Компьютер разблокирован

Группа событий "Аутентификация и идентификация"

Authentication group msg/Группа событий аутентификации
User login/Вход пользователя
User logout/Завершение работы пользователя
Authentication error/Ошибка аутентификации
User blocked/Запрет входа пользователя
Sudo denied/Запрет исполнения от имени другого пользователя
Sudo/Выполнение задания от имени другого пользователя

Группа событий "Контроль целостности"

Integrity group msg/Группа сообщений контроля целостности
Start Integrity check/Начало обработки задания на КЦ
Stop Integrity check/Завершение обработки задания на КЦ
Integrity task error/Нарушение целостности при обработке задания
Error in Integrity database/Ошибка открытия БД КЦ
Create integrity database/Создание БД КЦ
Integrity resource error/Нарушение целостности объекта
Restore from reference value/Восстановление объекта из эталонного значения
Error on resource backup/Ошибка при восстановлении объекта
No reference value/Отсутствует эталонное значение объекта

Группа событий "Система печати"

Printing group msg/Группа сообщений системы печати
Print page/Печать страницы документа
Error on print/Ошибка печати документа
Start printing/Начало печати документа

Группа событий "Сервис очистки файловой системы"

Trashd group msg/Группа событий сервиса очистки ФС
--

Группа событий "Сервис журналирования"

Snjournald group msg/Группа событий сервиса журналирования
--

Группа событий "Общие настройки"

Policy group msg/Группа сообщений общих настроек
Change policy/Изменение политики
Error on policy change/Ошибка изменения политики

Группа событий "Управление аудитом"

Audit control group msg/Группа событий управления аудитом
Add audit rule/Постановка объекта на аудит
Error on audit rules add/Ошибка постановки объекта на аудит
Clear audit rules/Очистка списка аудита

Группа событий "Управление сервисами"

Services group msg/Группа событий управления сервисами
Start service/Запуск сервиса
Stop service/Остановка сервиса

Группа событий "Управление пользователями"

Users control group msg/Группа событий управления пользователями
Add user/group/Добавление пользователя/группы
Delete user/group/Удаление пользователя/группы
Change user/group/Изменены параметры пользователя/группы
Change password/Изменен пароль для учетной записи
User/group blocked/Пользователь/группа заблокированы
Error on user/group add/Ошибка добавления пользователя/группы
Error on user/group del/Ошибка удаления пользователя/группы
Error on user/group change/Ошибка изменения параметров пользователя/группы

Группа событий "Управление контролем целостности"

Integrity control group msg/Группа сообщений управления контролем целостности
Add aobject to integrity monitoring/Установка объекта на контроль целостности
Error on object intergrity monitoring addition/Ошибка добавления/обновления ресурса к контролю
Remove object from intergity monitoring/Снятие объекта с контроля целостности

Группа событий "Управление резервным копированием"

Backup group msg/Группа сообщений резервного копирования
Error on resource adding to reference value/Ошибка добавления/обновления ресурса к эталону
Error on resource restoring from reference/Ошибка восстановления ресурса из эталона
Add resource to reference value/Добавление/обновление ресурса к эталону
Restore resource from reference/Восстановление ресурса из эталона

Группа событий "Управление контролем доступа"

Access control group msg/Группа сообщений контроля доступа
Change access rights/Смена прав доступа
Error on change access rights/Ошибка смены прав доступа
Change ACL rights/Смена прав доступа ACL
Error on change ACL rights/Ошибка смены прав доступа ACL

Группа событий "Управление усиленной аутентификацией"

Strengthen authentication group msg/Группа сообщений усиленной аутентификации

Группа сообщений "События модулей ядра"

Kernel SN-module message/Сообщение модуля ядра Secret Net LSP

События, регистрируемые в журнале аудита

Регистрируемые в журнале аудита события разделяются по типу сообщения. В данном разделе приведены используемые в рамках аудита типы сообщений.

Типы сообщений

Добавление устройства
Запись на устройство
Запись файла
Запуск приложения
Изменение атрибутов
Монтирование устройства
Неизвестно
Открытие сетевого соединения
Открытие файла на чтение
Открытие файла/каталога на запись
Переименование
Получение информации
Прием/передача датаграмм
Создание
Удаление
Удаление устройства
Установление соединения
Чтение с устройства
Чтение файла/каталога
Любой тип

Управление режимами работы модулей ядра

В Secret Net LSP предусмотрены возможность получения информации о режимах работы отдельных подсистем и управление режимами их работы на уровне ядра.

Информация о работе подсистем

Для получения информации о режиме работы и статистике по подсистемам используется содержимое файла /proc/snsecure/stats. Содержимое этого файла генерируется модулями ядра в момент запроса и представляет собой актуальную информацию о состоянии подсистем и параметрах их работы.

Ниже приведен пример вывода информации о работе подсистем.

```
# cat /proc/snsecure/stats
safe_access:
    enabled
safe_delete:
    enabled
RN:258 TR:272 UN(syn):4013 UN(asy):0
safe_memory:
    enabled
        4K:66176491 2M:0 1G:0
```

```
safe_secdev:  
    enabled (hard)
```

Пояснения:

- safe_access — контроль доступа;
- safe_delete — затирание файлов;
- safe_memory — затирание памяти;
- safe_secdev — контроль устройств.

RN — число затираний при переименованиях (rename);
TR — число затираний при изменении размера (truncate);
UN(syn) и UN(asy) — число затираний при удалении в синхронном и асинхронном режимах (unlink).

4K — число затираний 4-килобайтных страниц;
2M или 4M — число затираний 2- или 4- мегабайтных страниц;
1G — число затираний гигабайтных страниц.

Управление режимами работы

Ниже приведены примеры команды управления режимами работы (включение/выключение) для подсистем.

Контроль доступа

Контроль доступа может быть включен или выключен:

- 0 — выключено;
- 1 — включено.

Пример команды выключения:

```
# sysctl -w secretnet.secure.safe_access=0
```

Затирание файлов

Затирание файлов может быть включено или выключено:

- 0 — выключено;
- 1 — включено.

Пример команды на включение:

```
# sysctl -w secretnet.secure.safe_delete=1
```

Затирание памяти

Затирание памяти может быть включено или выключено:

- 0 — выключено;
- 1 — включено.

Пример команды на выключение:

```
# sysctl -w secretnet.secure.safe_memory=0
```

Контроль устройств

Предусмотрены 3 режима работы подсистемы:

- 0 — выключен;
- 1 — включен мягкий режим;
- 2 — включен жесткий режим.

Пример команды на включение мягкого режима:

```
# sysctl -w secretnet.secure.safe_secdev=1
```

Дополнительно имеется возможность задания уровня детализации сообщений в контроле доступа к устройствам:

- 0 — не регистрировать;
- 1 — регистрировать запреты;
- 2 — регистрировать запреты и разрешения.

Пример задания уровня детализации сообщений:

```
# sysctl -w secretnet.secure.safe_secdev_verbose=<0|1|2>
```

Функциональный контроль

В Secret Net LSP реализован функциональный контроль, обеспечивающий проверку целостности компонентов СЗИ и их работоспособности.

Проверка целостности компонентов СЗИ выполняется автоматически при загрузке ОС до старта Secret Net LSP. Перечень проверяемых компонентов формируется при установке СЗИ и хранится в конфигурационном файле.

Нарушение целостности проверяемых компонентов приводит к блокировке компьютера. Снять блокировку может только администратор с правами суперпользователя root.

После успешной проверки целостности осуществляются запуск Secret Net LSP и проверка работоспособности СЗИ. При этом проверяются:

- загрузка модулей ядра СЗИ;
- запуск основных сервисов Secret Net LSP и ОС;
- работоспособность файловых баз данных Secret Net LSP.

Результаты проверки целостности компонентов СЗИ и их работоспособности регистрируются в системном журнале. Если на момент выполнения проверки сервис регистрации событий недоступен, информация о результатах проверки помещается в специальный файл журнала (/opt/secretnet/var/log/sncheck.log).

При необходимости администратор может вручную запустить процедуру функционального контроля, используя утилиту **snfc**.

Запуск утилиты осуществляется в режиме командной строки. Ниже в таблице приведено описание ключей, применяемых при запуске утилиты администратором.

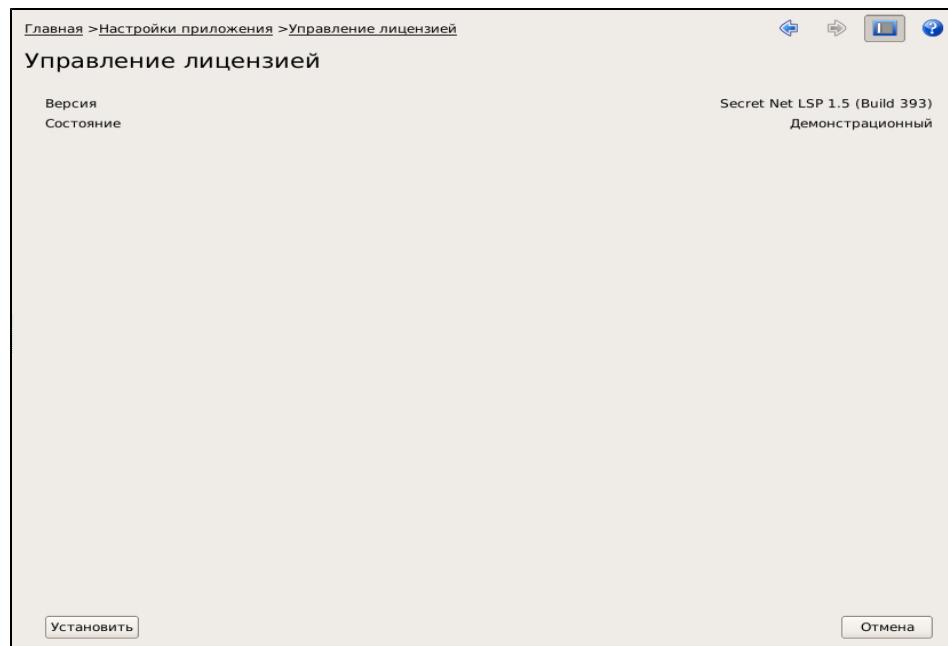
Ключ		Описание
-i	--init	Переинициализация БД контроля целостности. Используется после внесения изменений в системные файлы Secret Net LSP
	--test	Полная проверка целостности компонентов Secret Net LSP и проверка сервисов

Замена серийного номера демонстрационной версии

Для перехода с демонстрационной версии Secret Net LSP на рабочую необходимо заменить файл лицензии, активированной при установке демонстрационной версии.

Для замены серийного номера:

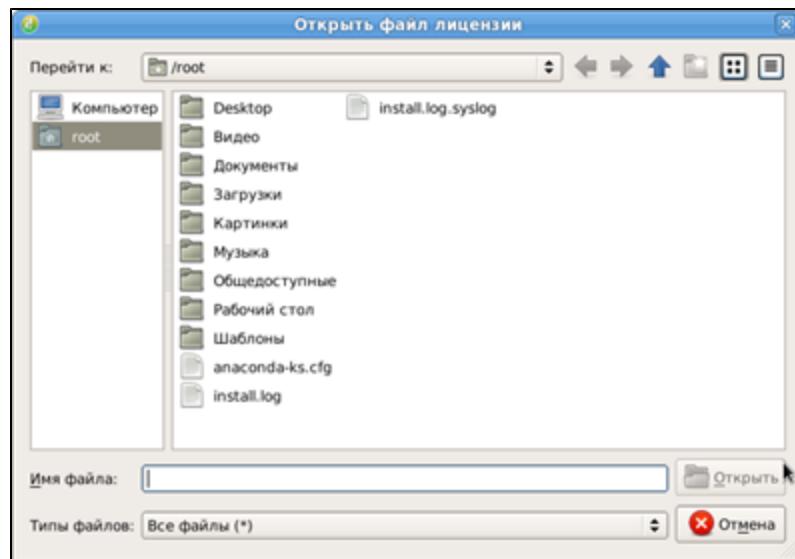
1. Вызовите панель безопасности Secret Net LSP (см. стр. [27](#)) и в группе "Настройки приложения" перейдите на страницу "Управление лицензией":



На странице отображается вид лицензии. Для демоверсии в поле "Состояние" будет отображаться значение "Демонстрационная".

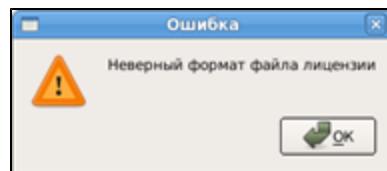
2. Нажмите кнопку "Установить".

Появится окно выбора места расположения файла лицензии:



3. Найдите и выберите новый файл лицензии и нажмите кнопку "Установить".

Если был выбран неверный файл лицензии, на экране появится соответствующее сообщение.



Нажмите кнопку "OK" в окне сообщения и повторите выбор файла лицензии.

При выборе правильного файла лицензии и ее успешной активации на странице "Управление лицензией" значение в поле "Состояние" изменится на "Действительная".

Обновление операционной системы

При обновлении операционной системы необходимо учитывать следующее:

- Работа Secret Net LSP возможна только в том случае, если ядро операционной системы входит в список поддерживаемых ядер.
- На компьютере должна быть установлена только одна операционная система с одним ядром.
- После установки Secret Net LSP обновление части пакетов операционной системы блокируется.

При установленной на компьютере системе Secret Net LSP обновление операционной системы следует выполнять в консоли в следующем порядке:

1. До запуска обновления сбросьте локаль в C, например, командой:

```
export LC_ALL=C LANG=C
```

2. Запустите и выполните обновление в соответствии с особенностями установленного дистрибутива операционной системы.



Для операционных систем CentOS и RHEL необходимо использовать ключ `--skip-broken`.

3. При необходимости перезагрузите компьютер.