КОД безопасности

Средство защиты информации

Secret Net LSP

Руководство администратора

RU.88338853.501410.017 91

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

Оглавление

Введение

Руководство предназначено для администраторов изделия "Средство защиты информации Secret Net LSP" RU.88338853.501410.017 (далее — Secret Net LSP, СЗИ, СЗИ Secret Net LSP). 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.

Важная и дополнительная информация оформлена в виде примечаний.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (https://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 https://www.securitycode.ru/ . 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 предназначен для защиты от НСД к информационным ресурсам компьютеров, функционирующих под управлением следующих дистрибутивов Linux:

- Альт 8 СП;
- Альт Рабочая Станция/Сервер 9;
- Альт Рабочая Станция/Сервер 10;
- Альт Рабочая Станция К 10;
- Ред ОС 7.3;
- Astra Linux CommonEdition 2.12;
- Astra Linux Special Edition 1.7;
- CentOS 7;
- CentOS 8;
- Debian 11;
- Oracle Linux 8;
- Red Hat Enterprise Linux 7;
- Red Hat Enterprise Linux 8;
- SUSE Linux Enterprise Server 12 SP5;
- SUSE Linux Enterprise Server 15 SP3;
- Ubuntu 18.04;
- Ubuntu 20.04;
- Ubuntu 22.04.

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, сетевым интерфейсам 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;
- создание замкнутой программной среды для пользователей;
- межсетевое экранирование сетевого трафика;
- 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.

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;
- формировать для пользователей замкнутую программную среду;
- контролировать вывод информации на печать;
- надежно скрывать информацию, содержащуюся в удаленных файлах, предотвращая ее восстановление;
- управлять доступом пользователей к устройствам;
- осуществлять контроль действий пользователей в системе.

В процессе эксплуатации 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 и восстановление СЗИ в аварийных ситуациях.

Требования к аппаратным и программным средствам

Secret Net LSP устанавливается на компьютеры, удовлетворяющие следующим системным требованиям.

Операционная система	• Альт 8 СП; • Альт Рабочая станция/Сервер 9; • Альт Рабочая станция/Сервер 10; • Альт Рабочая станция К 10; • Ред ОС 7.3; • Astra Linux Common Edition 2.12; • Astra Linux Special Edition 1.7; • CentOS 7; • CentOS 8; • Debian 11; • Oracle Linux 8; • Red Hat Enterprise Linux 7; • Red Hat Enterprise Linux 8; • SUSE Linux Enterprise Server 12 SP5; • SUSE Linux Enterprise Server 15 SP3; • Ubuntu 18.04; • Ubuntu 20.04; • Ubuntu 22.04
Процессор	В соответствии с требованиями операционной системы, установленной на компьютер
Количество ядер процессора	Минимально – 2 ядра
Оперативная память	Минимально – 2 Гбайт. Рекомендуется – 4 Гбайт (при использовании подсистемы замкнутой программной среды или межсетевого экранирования)
Жесткий диск	Минимально – 1 Гбайт

Лицензии на использование подсистем

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

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

Защитные механизмы

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

Механизм защиты входа в систему

Внимание!

Для корректного журналирования действий пользователя необходимо использовать утилиты Secret Net LSP. Они соответствуют стандартным утилитам Linux для работы с пользователями, но расположены в каталогах /opt/secretnet/bin и /opt/secretnet/sbin.

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 выполняются 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 — отдельное устройство, входящее в комплект аппаратного средства и предназначенное для хранения информации, необходимой для идентификации и аутентификации пользователя.

Secret Net LSP может функционировать совместно с программно-аппаратным комплексом (ПАК) "Соболь" версий 3.0, 3.1, 4. При этом ПАК "Соболь" обеспечивает дополнительную защиту от несанкционированного доступа к информационным ресурсам компьютера посредством доверенной загрузки.

В Secret Net LSP используются следующие персональные идентификаторы:

- идентификаторы iButton (поддерживаемые типы DS1993 — DS1996). Для работы с этими идентификаторами используется ПАК "Соболь". Считывающее устройство iButton подключается к разъему платы ПАК "Соболь";
- USB-ключи и смарт-карты (с любыми совместимыми USB-считывателями):

Продукт	USB-ключи	Смарт-карты
JaCarta ГОСТ	JaCarta ГОСТ JaCarta PKI/ГОСТ	—
JaCarta-2 ГОСТ	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ
JaCarta PKI	JaCarta PKI	
JaCarta SF/ГОСТ	JaCarta SF/ГОСТ	—
Rutoken	Rutoken ЭЦП S Rutoken S RF	—
Rutoken ЭЦП	Rutoken ЭЦП Rutoken ЭЦП 2.0 Rutoken ЭЦП PKI	Rutoken ЭЦП
Rutoken Lite	Rutoken Lite	—
ESMART Token	ESMART Token	ESMART Token
vdToken	vdToken 2.0	—
Guardant ID	Guardant ID	—

Режимы входа

Общий порядок идентификации при входе в систему зависит от способа ввода идентификационных данных пользователем. Предусмотрен ввод данных (имени пользователя и пароля) с клавиатуры или считывание из персонального идентификатора.

Параметр "Метод идентификации" устанавливает один из трех способов ввода данных для идентификации:

Имя пользователя вводится с клавиатуры
Имя пользователя определяется при предъявлении его персонального идентификатора
Имя пользователя может вводиться с клавиатуры или определяться при предъявлении персонального идентификатора. Задан по умолчанию после установки Secret Net LSP

Метод аутентификации зависит от наличия у пользователя записанного пароля и закрытого ключа в ЭИ. Режимы использования ЭИ настраиваются администратором.

Доступные режимы использования идентификаторов:

- включить режим хранения пароля;
    - записать пароль в идентификатор;
- требовать предъявление закрытого ключа пользователя при входе в систему;
- разрешить вход в ПАК "Соболь".

Для включения режима разрешения входа с помощью идентификатора в ПАК "Соболь" необходимо, чтобы ПАК "Соболь" функционировал в режиме интеграции с Secret Net LSP LSP.

Если хотя бы на одном ЭИ пользователя включен режим "Требовать предъявления закрытого ключа пользователя при входе в систему", пользователю запрещен вход в систему без предъявления идентификатора, на котором этот ключ записан. Закрытый ключ запрашивается независимо от установленного метода идентификации.

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

Для доменных пользователей при совместном функционировании Secret Net LSP с сервером безопасности Secret Net или Secret Net Studio может быть включен режим усиленной аутентификации. В этом режиме проверяется соответствие указанного пароля эталонному значению свертки пароля пользователя, хранящемуся в БД системы защиты.

Блокировка компьютера

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

К блокировке приводят следующие ситуации:

- нарушение функциональной целостности системы Secret Net LSP и модуля ПМЭ;
- нарушение целостности контролируемых объектов;
- нарушение правил подключения контроля устройств.

Проверка целостности компонентов Secret Net LSP, модуля персонального межсетевого экрана (ПМЭ) и объектов файловой системы выполняется при загрузке операционной системы (ОС). В случае нарушения целостности контролируемых объектов система блокирует компьютер. Администратор имеет возможность заблокировать или разблокировать компьютер с помощью утилит **snblock** и **snunblock**, расположенных в каталоге /opt/secretnet/sbin.

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 превышения допустимого количества неудачных попыток входа или истечения срока действия пароля, после смены которого пользователь сможет снова войти в систему.

Администратор имеет возможность заблокировать или разблокировать учетную запись пользователя с помощью утилиты **usermod**, расположенной в каталоге /opt/secretnet/sbin.

Администратор имеет возможность разблокировать учетную запись пользователя в случае превышения допустимого количества неудачных попыток входа с помощью утилиты **pam_ tally** , расположенной в каталоге /opt/secretnet/bin.

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.

Владельцем объекта может быть только один пользователь и одна группа.

При установке 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:

- владелец;
- группа владельца;

- остальные.

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, сетевым интерфейсам и подключаемым к ним устройствам в целях предотвращения несанкционированной утечки информации с защищаемого компьютера.

Внимание!
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.

В подсистеме разграничения доступа к устройствам Secret Net LSP имеется разделение на следующие шины:

Шина/группа устройств	**Класс устройств**
LOCAL/Локальные устройства	Оптические диски
	Физические диски
	Параллельные порты
	Последовательные порты

USB/Устройства USB	Устройства хранения
	Электронные идентификаторы и считыватели
	Сотовые телефоны
	Сканеры и цифровые фотоаппараты
	Сетевые платы и модемы
	Принтеры
	Bluetooth адаптеры
	Интерфейсные устройства
	Прочие
NET/Сетевые адаптеры	Соединение Ethernet
	Соединение 1394 (FireWire)
	Беспроводное соединение (WiFi)
	Соединение Bluetooth
	Инфракрасное соединение (IrDA)

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

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

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

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

Каждое контролируемое устройство однозначно идентифицируется по следующим параметрам:

- VendorID;
- DeviceID;
- ProductID;
- серийный номер.

Значения вышеперечисленных параметров считываются 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.

Режимы контроля подключения:

- устройство не контролируется;
- устройство постоянно подключено к компьютеру;
- блокировать компьютер при изменении устройства;
- подключение устройства разрешено;

- подключение устройства запрещено.

Права доступа к устройству и режимы контроля подключения могут наследоваться от шины, класса, модели устройства соответственно.

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, членом которых является пользователь. При этом запрещающие права имеют приоритет над разрещающими.

После установки Secret Net LSP для шин USB и Local по умолчанию для всех пользователей устанавливаются права, разрешающие чтение и запись. Все устройства, подключаемые к указанным шинам, по умолчанию регистрируются в системе с правами "Наследуется от шины". Разграничение доступа доступно только для шины local (оптические диски, физические диски, параллельные порты, последовательные порты), USB (только для устройств хранения). Правила наследования могут работать не только от шины, но и от модели или класса. Модель устройств — это множество устройств с одинаковыми VID и PID.

После выполнения администратором настроек в подсистеме пользователи смогут подключать только те устройства и выполнять только те операции, которые определены для всей системы в правах доступа.

Права доступа пользователей к устройству могут наследоваться от прав доступа к шине, к которой подключается данное устройство. Порядок наследования: шина, класс, модель, экземпляр.

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.

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 компьютер. Доступ возможен только администратору. Разблокирование осуществляется администратором.

Контроль проводится в автоматическом режиме при загрузке операционной системы. Также администратор может вручную запустить проверку целостности защищаемых ресурсов, используя утилиту **snaidectl**.

Объекты и параметры контроля

Объектами контроля целостности в СЗИ Secret Net LSP являются:

- компоненты установленного ПО СЗИ (файлы и каталоги). КЦ автоматически устанавливается на часть системных каталогов;
- 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;
- удаление файла;
- 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;
- удаление каталога.

Методы контроля

В качестве проверяющих методов используется метод подсчета и проверки контрольных сумм по алгоритмам MD5, SHA-512, ГОСТ Р 34.11-2012 (только на ОС, поддерживающих работу с данным алгоритмом).

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 главе "Эксплуатация Secret Net LSP".

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.

При каждом варианте происходит регистрация событий.

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.

В Secret Net LSP реализована возможность настроить расписание для контроля целостности. При настройке можно указать проверку:

- периодическую;
- ежедневную;
- по дням недели в указанное время.

Для защищаемых объектов доступна возможность включения контроля в реальном времени. Контроль в реальном времени означает, что контроль целостности объекта происходит не по расписанию, а постоянно. КЦ в реальном времени должен включаться для каждого объекта отдельно. Проверка объектов, для которых не установлен контроль в реальном времени, должна осуществляться по установленному расписанию.

Для каждого из объектов должна быть возможность указать уровень полноты контроля целостности. Настройка полноты КЦ должна включать в себя гранулярный выбор контролируемых атрибутов объектов:

- контрольной суммы объекта;
- размера объекта;
- прав объекта;
- владельца объекта;
- даты последнего изменения объекта.

Нарушение КЦ должно регистрироваться, если для контролируемого объекта меняется состояние хотя бы одного из его контролируемых атрибутов.

Механизм замкнутой программной среды

Механизм замкнутой программной среды (ЗПС) предназначен для ограничения использования ПО на компьютере.

Режимы работы механизма

Для работы ЗПС предусмотрены следующие режимы работы:

- мягкий;
- жесткий.

Мягкий режим нужен для настройки механизма на основе правил, в том числе правил, создаваемых на основе анализа событий журнала аудита. Жесткий — это основной штатный режим работы. В мягком режиме пользователю разрешается запускать любые программы. Если при этом пользователь запускает программы, не входящие в список исключений для ресурсов, в журнале событий регистрируются соответствующие события тревоги. В жестком режиме разрешается запуск только тех программ, которые разрешены правилами ЗПС или входят в список исключений для ресурсов. Запуск других программ блокируется, а в журнале событий регистрируются события тревоги. Мягкий режим нужен для того, чтобы, не влияя на работу пользователей, накопить сведения в журнале о возможных ошибках, допущенных при настройке механизма ЗПС, и в последующем их устранить.

Примечание.
После переключения ЗПС в жесткий режим у пользователя при загрузке компьютера появится уведомление о том, что необходимо обратиться к системному администратору, чтобы подтвердить жесткий режим ЗПС. Если жесткий режим не подтвердить, то при следующей загрузке компьютера останется мягкий режим.

Регистрация событий

События, связанные с работой механизма ЗПС, регистрируются в "Журнале событий".

Белый список пользователей и групп

Пользователям и группам, находящимся в белом списке, разрешен запуск всех программ, файлов, библиотек и скриптов. Для них не осуществляется контроль ЗПС.

Примечание.
Новые пользователи по умолчанию не включены в белый список. Необходимо для них создать правила вручную.

Список исключений для ресурсов

Для всех пользователей определяется список исключений для ресурсов, в который входят разрешенные для запуска программы, файлы, библиотеки и скрипты. Контроль целостности для этих объектов не выполняется. Попытки запуска других ресурсов блокируются и регистрируются в журнале событий.

Правила

Правила ЗПС обеспечивают разграничение доступа пользователей к ресурсам.

Примечание.
При запуске ресурсов из правила ЗПС осуществляется контроль целостности. В случае нарушения контроля целостности запуск ресурсов запрещен.

Механизм персонального межсетевого экранирования

Механизм персонального межсетевого экранирования предназначен для защиты серверов и рабочих станций от несанкционированного доступа и разграничения сетевого доступа в информационных системах.

ПМЭ выполняет следующие функции:

- контроль сетевого трафика;
- нейтрализация угроз, связанных с сетевым взаимодействием;
- разграничение сетевого доступа;
- контроль папок общего доступа;
- контроль именованных файлов/каналов;
- контроль использования сети приложениями;
- фильтрация входящих соединений с использованием данных отправителя пакетов;
- принудительное завершение TCP-соединений;
- оповещение пользователя при срабатывании правила.

Правила

Правила ПМЭ Secret Net LSP обеспечивают выполнение функциональности механизма фильтрации сетевого трафика.

Фильтрация сетевого трафика

Фильтрация сетевого трафика осуществляется для отправителей и получателей информации в рамках всех операций ее передачи узлам информационной системы.

Регистрация событий

События, связанные с работой механизма ПМЭ, регистрируются в "Журнале событий".

Механизм регистрации событий

В процессе работы Secret Net LSP события, происходящие на компьютере, и события, связанные с безопасностью системы, регистрируются в подсистеме журналирования, 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.

Система Secret Net LSP предусматривает создание файлов-уведомлений для администратора безопасности в каталоге **var/spool/mail** в следующих случаях:

- при регистрации событий в журнале аудита, возникающих при срабатывании правила ПМЭ;
- при истечении срока действия лицензированных возможностей модулей защиты (за 30 дней до окончания действия лицензии);
- при окончании действия лицензии;
- при возникновении ошибок в процессе осуществления контроля лицензий.

  В случае возникновения ошибок в процессе контроля лицензий компьютер пользователя блокируется, а на экране отображается соответствующее сообщение.

Примечание.
В Secret Net LSP предусмотрена возможность получения администратором безопасности уведомлений на локальный адрес электронной почты. Для отправки почты локальному администратору необходимо установить утилиты отправки почты, рекомендуемый пакет postfix. При отсутствии утилит в журнал будет писаться соответствующее сообщение об ошибке.

Механизм затирания остаточной информации

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

Действие механизма заключается в очистке 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 Мбайт, 4 Мбайт, 1 Гбайт) на более мелкие непосредственно перед очисткой. Дополнительно выполняется затирание SWAP при выключении или 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).

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

По умолчанию после установки системы механизм затирания остаточной информации выключен. При необходимости администратор может вручную включить механизм затирания.

Архитектура

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 дискреционную модель разграничения доступа субъектов (пользователей, процессов) к объектам файловой системы.
- Подсистема разграничения доступа к устройствам. Реализует дискреционную модель разграничения доступа пользователей и групп к шинам USB, SATA, сетевым интерфейсам и подключаемым к ним устройствам.
- Подсистема контроля целостности и восстановления. 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 замкнутой программной среды. Предназначена для ограничения использования ПО на компьютере.
- Подсистема межсетевого экранирования. Обеспечивает фильтрацию сетевого трафика в рамках всех операций передачи информации узлам информационной системы на сетевом, транспортном и прикладном уровнях на основании установленных администратором МЭ правил фильтрации.
- Подсистема ведения журналов. Осуществляет сбор сведений о событиях, зарегистрированных в других подсистемах, и формирование системного журнала и журнала аудита.
- Подсистема аудита. Предназначена для настройки регистрации событий при обращении к объектам, поставленным на аудит.
- Подсистема очистки памяти. Осуществляет очистку затиранием выделенных или перераспределенных участков оперативной памяти и освобождаемых участков на жестких дисках или внешних устройствах.

Подсистема 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;
- 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 CLI-клиентов управления указанным подсистемам (сервисам, утилитам).

Работа утилит загрузки и инициализации осуществляется в фоновом режиме.

Инструменты управления

CLI-утилиты — UNIX-приложения с классическим интерфейсом, предоставляющие администратору возможность выполнять все необходимые операции по управлению Secret Net LSP в режиме командной строки.

Посредством инструментов управления Secret Net LSP обеспечивает выполнение следующих функций:

- идентификация и аутентификация пользователей в системе;
- конфигурация СЗИ;
- получение информации о текущем состоянии КСЗ;
- управление политиками Secret Net LSP;
- настройка замкнутой программной среды;
- настройка аудита;
- регистрация событий, связанных с действиями администратора, и критичных событий в работе клиента (используются средства подсистемы регистрации событий);
- конфигурация межсетевого экрана;
- контроль доступа к устройствам;
- контроль целостности;
- управление журналами;
- управление пользователями и персональными идентификаторами;
- тестирование СЗИ.

В Secret Net LSP используются следующие CLI-утилиты:

Утилита	Описание
snpolctl	Используется для выполнения настройки параметров политик
sntokenctl	Используется для выполнения операций с персональными идентификаторами
snablectl	Используется для управления интеграцией с ПАК "Соболь"
sndevctl	Используется для контроля и управления доступом к устройствам
snaidectl	Используется для выполнения процедур, связанных с контролем целостности
snauditctl	Используется для просмотра и редактирования правил аудита
snlicensectl	Используется для работы с лицензиями
snaecctl	Используется для выполнения настройки замкнутой программной среды
fw-localcfg	Используется для выполнения настройки персонального межсетевого экрана
fw-net	Используется для разрыва TCP-соединений
snnetctl	Используется для настройки удаленного управления
snbckctl	Используется для выполнения операций резервного копирования и восстановления
snjrnl	Используется для работы с журналами

Плагины безопасности

В состав подсистемы 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 свойств пароля пользователя. Связывание идентификаторов с пользователями
Плагин управления политиками	Получение текущего состояния политик. Изменение конкретной политики
Плагин резервного копирования	Резервное копирование и восстановление настроек Secret Net LSP: данных о пользователях и группах, содержимого базы данных настроек, содержимого журналов
Плагин настройки удаленного управления	Настройка режима удаленного управления для подключения к серверу безопасности СЗИ Secret Net 8

Подсистема идентификации

Подсистема предназначена для управления средствами защиты входа в систему, использующими механизмы идентификации пользователей.

Подсистема имеет плагинную архитектуру, позволяющую подключать различные методы идентификации.

Подсистема обеспечивает:

- Хранение информации, необходимой для использования сервиса идентификации, информации о сроках действия учетных записей пользователей.
- Кеширование.
- Организацию сессии работы пользователя в случае успешного прохождения процедуры проверки подлинности.
- Регистрацию событий.
- Управление пользователями и группами (создание, 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;
- 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. В CLI-утилиту входят:

- DAC (**chmod**, **chown**, **chgrp** , **chfn**);
- ACL (**setfacl**, **getfacl**).

CLI-утилита управления предназначена для выполнения общих функций по управлению правами доступа:

- предоставляет информацию о правах доступа объектов файловой системы посредством чтения ACL из **xattrs** файловой системы;
- предоставляет возможность легитимного изменения правил разграничения доступа (метки в **xattrs** файловой системы);
- совместно с подсистемой аудита может 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, сетевыми интерфейсами 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;
- встраивание в подсистему **vfs** и модификация механизмов работы ядра, связанных с контролем доступа субъектов (процессов) к объектам файловой системы;
- регистрация событий.

Приложение — обработчик событий

Приложение выполняет следующие функции:

- 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;
- набор утилит, выполняющих базовые операции конфигурирования с использованием командного интерфейса.

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

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

Режимы работы подсистемы

Предусмотрены два режима работы подсистемы:

- выключено — действия пользователей с устройствами не контролируются;
- включено — 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;
- Product ID;
- серийный номер устройства (если есть);
- метка, присвоенная устройству при его регистрации;
- результат операции подключения или отключения устройства.

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

Примечание.
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 файлов и каталогов, поставленных на контроль;
- проверка целостности защищаемых ресурсов;
- проверка целостности по расписанию;
- поддержка полного контроля над объектами;
- 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:

- 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 замкнутой программной среды

Подсистема замкнутой программной среды обеспечивает ограничение для использования ПО на компьютере.

Доступ разрешается только к тем программам, которые необходимы пользователям для работы. Для каждого пользователя определяется перечень ресурсов, в который входят разрешенные для запуска программы, файлы, библиотеки и сценарии (скрипты). Попытки запуска других ресурсов блокируются, и в журнале регистрируются события тревоги.

Подсистема межсетевого экранирования

Подсистема обеспечивает работу механизма ПМЭ и предназначена для выполнения им следующих основных функций:

- фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
- фильтрация пакетов служебных протоколов (ICMP), необходимых для диагностики и управления работой сетевых устройств;
- фильтрация с учетом входного и выходного сетевого интерфейса для проверки подлинности сетевых адресов;
- фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);
- фильтрация на прикладном уровне IP-пакетов по протоколу SMB;
- фильтрация на прикладном уровне запросов к прикладным сервисам (фильтрация по символьной последовательности в пакетах);
- фильтрация с учетом полей сетевых пакетов;
- фильтрация с учетом правил доступа;
- фильтрация с учетом даты/времени суток.

Фильтрация сетевого трафика осуществляется на интерфейсах Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11b/g/n). События, связанные с работой персонального межсетевого экрана, регистрируются в журнале Secret Net LSP.

В состав подсистемы межсетевого экранирования входит модуль ПМЭ, являющийся локальным компонентом СЗИ Secret Net LSP. Процедуры, связанные с установкой или удалением модуля ПМЭ, выполняются отдельно от основного пакета ПО Secret Net LSP (подробнее см. стр.**29**, стр.**31**).

Примечание.
Модуль ПМЭ совместим с модулями и компонентами ПО СЗИ Secret Net LSP, начиная с версии 1.10. Использование модуля ПМЭ совместно с предыдущими версиями ПО СЗИ Secret Net LSP не предусмотрено.

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;
- затирание hugetlbfs и tmpfs;
- включение, выключение механизма синхронного затирания на жестких дисках и внешних носителях.

Внимание!
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;
- сервис синхронного 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 или перезагрузке операционной системы.

Для безопасного удаления информации на жестких дисках и внешних носителях независимо от установленного режима работы подсистемы применяется утилита **shred**.

В Secret Net LSP также предусмотрено автоматическое затирание остаточной информации в фоновом режиме, реализованное на уровне ядра. По умолчанию после установки в Secret Net LSP автоматическое затирание выключено, так как использование этого механизма приводит к повышенной нагрузке на файловую систему и физические накопители. Если необходимо, чтобы на компьютере было включено автоматическое затирание, после перезагрузки выполните включение механизма.

Подсистема ведения журналов

Подсистема предназначена для формирования журнала аудита и системного журнала.

Подсистемой выполняются следующие функции:

- сбор сведений от других подсистем о зарегистрированных в них событиях;
- первичная обработка событий и хранение их в базе данных.

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;

- сортировка отображаемой в журналах информации;
- сохранение отчетов в файл.

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;
- 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 и 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:

- 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.

Глава 2
Установка, удаление и обновление

ПО Secret Net LSP поставляется на установочном носителе в виде RPM- и DEB-пакетов. Также на этом носителе располагаются архивы с зависимостями для данных пакетов.

Процедуры установки, обновления и удаления Secret Net LSP выполняются администратором, обладающим правами суперпользователя компьютера.

Перед установкой Secret Net LSP необходимо убедиться в выполнении следующих требований:

- на компьютере установлена поддерживаемая операционная система;
- ядро операционной системы должно входить в список ядер, заявленных как поддерживаемые компанией — разработчиком СЗИ, и соответствовать устанавливаемому дистрибутиву Secret Net LSP.

Установка

Установка ПО Secret Net LSP

Процедура установки ПО СЗИ Secret Net LSP включает автоматическую регистрацию лицензии модуля базовой защиты, который включает:

- подсистему локального управления;
- подсистему идентификации и аутентификации;
- подсистему журналирования;
- подсистему аудита;
- подсистему контроля целостности;
- сервис печати;
- системный сервис печати;
- сервис безопасного удаления.

Перед установкой ПО проверьте выполнение требований к аппаратному и программному обеспечению компьютера (см. стр.**8**).

Внимание!

Отдельно необходимо проверить, входит ли версия ядра установленной на компьютере ОС в список поддерживаемых Secret Net LSP. В некоторых случаях при установке ОС на компьютер ядро из дистрибутива может быть заменено во время установки пакетов обновлений из сетевого репозитория. Поэтому при установке ОС рекомендуется включать режим "Не устанавливать обновления в процессе установки". Также следует учитывать, что в некоторых ОС и в таком случае могут загружаться критические обновления.

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

Операционная система	Установочные пакеты
RPM-пакеты	
Альт 8 СП	sn-lsp_1.12-334.alt0.c9f2.x86_64.rpm
Альт Рабочая Станция/Сервер 9	sn-lsp_1.12-334.alt0.p9.x86_64.rpm
Альт Рабочая Станция/Сервер 10; Альт Рабочая Станция К 10	sn-lsp_1.12-334.alt0.p10.x86_64.rpm
РЕД ОС 7.3	sn-lsp_1.12-334.redos7.3.x86_64.rpm

Операционная система	Установочные пакеты
CentOS 7; Red Hat Enterprise Linux 7	sn-lsp_1.12-334. el7.x86_64.rpm
CentOS 8; Oracle Linux 8; Red Hat Enterprise Linux 8	sn-lsp_1.12-334. el8.x86_64.rpm
SUSE Linux Enterprise Server 12 SP5	sn-lsp_1.12-334. sle12sp5.x86_64.rpm
SUSE Linux Enterprise Server 15 SP3	sn-lsp_1.12-334. sle15sp3.x86_64.rpm
DEB-пакеты	
Astra Linux Common Edition 2.12	sn-lsp_1.12-334. astra2.12_amd64.deb
Astra Linux Special Edition 1.7	sn-lsp_1.12-334. astra1.7_amd64.deb
Debian 11	sn-lsp_1.12-334. debian11_amd64.deb
Ubuntu 18.04	sn-lsp_1.12-334. ubuntu18.04_amd64.deb
Ubuntu 20.04	sn-lsp_1.12-334. ubuntu20.04_amd64.deb
Ubuntu 22.04	sn-lsp_1.12-334. ubuntu22.04_amd64.deb

Внимание!

- Рекомендуется перед началом установки отключить хранитель экрана и выполнить процедуру установки от начала до конца без перерыва.
- Перед выполнением установки Secret Net LSP и модуля ПМЭ необходимо подключить стандартные репозитории ОС для установки зависимостей.
- Для Secret Net LSP реализована инициализация настроек из резервной копии при установке через переменное окружение. Переменным окружением является путь к резервной копии: SNTEMPLATE_TARBALL=/tmp/backup. При установке программа проверяет наличие резервной копии и получает необходимые настройки СЗИ.

Для установки Secret Net LSP:

1. Вставьте установочный носитель Secret Net LSP в устройство чтения или загрузите на компьютер дистрибутив Secret Net LSP. Запустите программу эмулятора терминала.
2. Перейдите в каталог, соответствующий установленной ОС. В зависимости от используемой ОС выполните команды:
   - Для РЕД ОС 7.3 (далее — РЕД ОС), CentOS 7, 8 (далее — CentOS), Red Hat Enterprise Linux 7, 8 (далее — RHEL), Oracle Linux 8 (далее — Oracle Linux):

     ```
     #yum install ./<пакет sn-lsp>
     ```

   - Для Astra Linux Common Edition 2.12, Special Edition 1.7 (далее — Astra Linux), Debian 11 (далее — Debian), Ubuntu 18.04, 20.04, 22.04 (далее — Ubuntu):

     ```
     #apt install ./<пакет sn-lsp>
     ```

   - Для Альт 8 СП, Альт Рабочая Станция К 10, Альт Рабочая Станция/Сервер 9, 10:

     ```
     #apt-get install ./<пакет sn-lsp>
     ```

   - Для SUSE Linux Enterprise Server 12 SP5, 15 SP3 (далее — SLES):

     ```
     #zypper install ./<пакет sn-lsp>
     ```

Результатом выполненных действий является установка Secret Net LSP на защищаемом компьютере.

3. Перезагрузите компьютер.

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

Установка персонального межсетевого экрана

Перед установкой убедитесь в наличии достаточного объема оперативной памяти для функционирования модуля ПМЭ. Выбор необходимого объема оперативной памяти следует осуществлять с учетом системных требований ОС, на которой планируется использование ПО СЗИ Secret Net LSP.

Установка модуля персонального межсетевого экрана в зависимости от используемой операционной системы осуществляется с помощью установочных RPM- и DEB-пакетов:

Операционная система	Установочные пакеты
RPM-пакеты	
Альт 8 СП	sn-firewall_1.2-144.alt0.c9f2.x86_64.rpm
Альт Рабочая Станция/Сервер 9	sn-firewall_1.2-144.alt0.p9.x86_64.rpm
Альт Рабочая Станция/Сервер 10; Альт Рабочая Станция К 10	sn-firewall_1.2-144.alt0.p10.x86_64.rpm
РЕД ОС 7.3	sn-firewall_1.2-144.redos7.3.x86_64.rpm
CentOS 7; Red Hat Enterprise Linux 7	sn-firewall_1.2-144.el7.x86_64.rpm
CentOS 8; Oracle Linux 8; Red Hat Enterprise Linux 8	sn-firewall_1.2-144.el8.x86_64.rpm
SUSE Linux Enterprise Server 12 SP5	sn-firewall_1.2-144.sle12sp5.x86_64.rpm
SUSE Linux Enterprise Server 15 SP3	sn-firewall_1.2-144.sle15sp3.x86_64.rpm
DEB-пакеты	
Astra Linux Common Edition 2.12	sn-firewall_1.2-144.astra2.12_amd64.deb
Astra Linux Special Edition 1.7	sn-firewall_1.2-144.astra1.7_amd64.deb
Debian 11	sn-firewall_1.2-144.debian11_amd64.deb
Ubuntu 18.04	sn-firewall_1.2-144.ubuntu18.04_amd64.deb
Ubuntu 20.04	sn-firewall_1.2-144.ubuntu20.04_amd64.deb
Ubuntu 22.04	sn-firewall_1.2-144.ubuntu22.04_amd64.deb

Внимание!
Установку модуля персонального межсетевого экрана необходимо производить после того, как на защищаемый компьютер будет установлен основной пакет ПО СЗИ Secret Net LSP.

Для установки модуля ПМЭ Secret Net LSP:

1. Вставьте установочный носитель Secret Net LSP в устройство чтения. Запустите программу эмулятора терминала.
2. Перейдите в каталог, соответствующий установленной ОС. В зависимости от используемой ОС выполните команды:
   - Для РЕД ОС, CentOS, RHEL, Oracle Linux:
     ```
     #yum install ./<пакет sn-firewall>
     ```
   - Для Astra Linux, Debian, Ubuntu:
     ```
     #apt install ./<пакет sn-firewall>
     ```
   - Для Альт 8 СП, Альт Рабочая Станция К 10, Альт Рабочая Станция/Сервер 9, 10:
     ```
     #apt-get install ./<пакет sn-firewall>
     ```
   - Для SLES:
     ```
     #zypper install ./<пакет sn-firewall>
     ```

Результатом выполненных действий является установка модуля персонального межсетевого экрана Secret Net LSP на защищаемом компьютере. При наличии лицензии необходимо запустить политику. Для этого выполните команду:

```
snpolctl -p firewall -c firewall,state,1
```

Примечание.
Персональный межсетевой экран является отдельным компонентом ПО СЗИ Secret Net LSP и не входит в состав основной лицензии защитных подсистем. Для корректного функционирования модуля защиты ПМЭ предусмотрена регистрация соответствующей дополнительной лицензии (подробнее см. стр.75). Для Secret Net LSP 1.12 идет свой пакет межсетевого экрана версии 1.2. На данный момент обновление межсетевого экрана возможно через удаление старого пакета и установку нового. Перенос правил осуществляется через import/export. Установка возможна только совместно с Secret Net LSP 1.12 и совместимой ОС.

Удаление

Удаление ПО Secret Net LSP

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

Внимание!
Процедуру удаления ПО СЗИ Secret Net LSP необходимо производить после того, как на компьютере будет удален модуль персонального межсетевого экрана.

Примечание.
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.

Для удаления программного обеспечения:

1. Запустите программу эмулятора терминала.
2. В зависимости от типа использованного при установке дистрибутива выполните команду:
   - для RPM-пакетов:
     ```
     #rpm –e secretnet
     ```
   - для DEB-пакетов:

```
#dpkg –r secretnet
```

3. Перезагрузите компьютер.

Результатом выполнения процедуры является удаление Secret Net LSP, а также всех лицензий защитных подсистем.

Удаление персонального межсетевого экрана

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

Внимание!
Процедуру удаления ПО СЗИ Secret Net LSP необходимо производить после того, как на компьютере будет отключена политика ПМЭ. Для этого выполните команду:

```
snpolctl -p firewall -c firewall,state,0
```

Для удаления модуля персонального межсетевого экрана:

1. Запустите программу эмулятора терминала.
2. В зависимости от типа использованного при установке дистрибутива выполните команду:
   - для RPM-пакетов:

     ```
     #rpm –e snlsp-firewall
     ```

     или

     ```
     #yum remove snlsp-firewall
     ```

     При выполнении приведенных выше команд система управления пакетами предложит удалить указанный RPM-пакет модуля ПМЭ.

     В результате подтверждения действия выполняется удаление файлов конфигурации и правил. Файлы журналов остаются в каталоге **/opt/snlsp-firewall/var/log/suricata**.

   - для DEB-пакетов:

     ```
     #dpkg –P snlsp-firewall
     ```

     или

     ```
     #apt purge snlsp-firewall
     ```

     При выполнении команды система управления пакетами предложит удалить указанный DEB-пакет модуля ПМЭ.

     В результате подтверждения действия выполняется удаление файлов конфигурации, журналов и правил.

     ```
     #apt remove snlsp-firewall
     ```

     При выполнении команды система управления пакетами предложит удалить указанный DEB-пакет модуля ПМЭ.

     В результате подтверждения действия производится удаление пакета из системы. При этом в каталоге **/opt/snlsp-firewall** остаются файлы журналов и файлы конфигурации.

После удаления модуля ПМЭ рекомендуется перезагрузить компьютер. Результатом выполнения процедуры является удаление модуля ПМЭ.

Обновление

Обновление ПО Secret Net LSP

В Secret Net LSP реализована возможность обновления программного обеспечения с версии 1.11 на текущую 1.12 только для следующих ОС:

- Альт Рабочая Станция/Сервер 9;
- РЕД ОС 7.3;
- Astra Linux Common Edition 2.12;
- CentOS 7;
- Red Hat Enterprise Linux 7;
- Ubuntu 18.04, 20.04.

Для остальных случаев процедуру обновления ПО необходимо выполнять путем резервного копирования настроек Secret Net LSP (см. стр. **56**) с последующим удалением текущей версии ПО (см. стр.**30**, стр.**33**).

Перед установкой и обновлением продукта необходимо выполнить подключение системных репозиториев.

Для обновления ПО:

1. Вставьте установочный носитель Secret Net LSP в устройство чтения или загрузите на компьютер дистрибутив Secret Net LSP. Запустите программу эмулятора терминала.
2. Перейдите в каталог, соответствующий установленной ОС. В зависимости от используемой ОС выполните команды:

   При обновлении с версии 1.11:

   - Для РЕД ОС 7.3, CentOS 7, Red Hat Enterprise Linux 7:

     ```
     #yum install ./<пакет sn-lsp>
     ```

   - Для Astra Linux Common Edition 2.12, Ubuntu 18.04, 20.04:

     ```
     #apt install ./<пакет sn-lsp>
     ```

   - Для Альт Рабочая Станция/Сервер 9:

     ```
     #apt-get install ./<пакет sn-lsp>
     ```

3. Перезагрузите компьютер.

При добавлении файла ранее зарегистрированной лицензии данными из лицензии автоматически заполняются следующие модули защиты:

- базовая защита;
- контроль устройств;
- дискреционное управление доступом;
- замкнутая программная среда.

Персональный межсетевой экран является отдельным компонентом ПО СЗИ Secret Net LSP и не входит в состав основной лицензии защитных подсистем. При обновлении продукта Secret Net LSP происходит удаление пакета персонального межсетевого экрана, так как он является одной из его зависимостей. После обновления ПО СЗИ Secret Net LSP до версии 1.12 необходима установка пакета персонального межсетевого экрана обновленной версии (1.2).

Активация модуля защиты персонального межсетевого экрана осуществляется отдельно посредством регистрации дополнительной лицензии на соответствующий механизм. Если существует необходимость переноса политик персонального межсетевого экрана необходимо заранее, перед установкой обновления ПО СЗИ Secret Net LSP, выполнить экспорт правил персонального межсетевого экрана. После установки пакета персонального межсетевого экрана новой версии необходимо выполнить импорт правил ПМЭ.

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 поддерживаемая операционная система.

В случае обновления операционной системы, под управлением которой находится защищаемый компьютер, в Secret Net LSP реализована возможность сохранения ранее произведенных настроек ПО.

При обновлении операционной системы:

1. Создайте резервную копию настроек ПО СЗИ Secret Net LSP с помощью утилиты **snbckctl** (см. стр.**56**).
2. Выполните удаление ПО СЗИ Secret Net LSP (см. стр.**30**).
3. Выполните обновление операционной системы компьютера.
4. Выполните установку зависимостей и актуальной версии ПО СЗИ Secret Net LSP (см. стр.**27**).
5. Восстановите произведенные ранее настройки ПО СЗИ Secret Net LSP с помощью утилиты **snbckctl** (см. стр.**56**).

Глава 3
Эксплуатация Secret Net LSP

Утилиты Secret Net LSP

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

Приведенные ниже утилиты используются в следующих задачах:

- настройка параметров политик;
- управление персональными идентификаторами;
- управление взаимодействием с ПАК "Соболь";
- безопасное удаление;
- разграничение доступа к устройствам;
- контроль целостности объектов файловой системы;
- настройка правил аудита;
- работа с лицензиями;
- настройка замкнутой программной среды;
- управление режимом аутентификации;
- настройка удаленного управления;
- резервное копирование;
- работа с журналами.

Утилиты расположены в каталогах /opt/secretnet/bin и /opt/secretnet/sbin.

Внимание!

Для корректного журналирования действий с пользователями необходимо использовать утилиты Secret Net LSP. Они соответствуют стандартным утилитам Linux для работы с пользователями, но расположены в каталогах /opt/secretnet/bin и /opt/secretnet/sbin.

Настройка параметров политик

Для выполнения настройки параметров политик используется утилита **snpolctl**, расположенная в каталоге /opt/secretnet/bin. Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
snpolctl <ключ> [<параметр>] ... [<ключ>] [<параметр>]
```

Описание ключей представлено в следующей таблице:

Ключ		Описание
–h	––help	Выводит справочную информацию о применении команды
–l	––list	Выводит список плагинов с указанием политик и состоянием их параметров
–p <плагин>	––plugin <плагин>	Настройка параметра <плагин> – выбор и установка плагина управления из доступного перечня: • aec – замкнутая программная среда; • aide – контроль целостности; • control – модули ядра; • cups – контроль печати; • devices – устройства; • firewall – межсетевой экран; • service_mgr – системные сервисы; • system – системные настройки; • token_mgr – аутентификация; • users – пользователи и группы
–c <политика>, <параметр>, <значение>	––change <политика>, <параметр>, <значение>	Настройка параметра <политика> – выбор и установка политики из доступного перечня: • aec – замкнутая программная среда; • aide – контроль целостности; • access_control – дискреционное управление доступом; • cups – контроль печати; • memory – очистка оперативной памяти; • devices_control – управление устройствами; • firewall – межсетевой экран; • services – установка сервисов; • system – системные настройки; • authentication – параметры аутентификации; • users – управление настройками паролей пользователей

Ключ		Описание
–c <политика>, <параметр>, <значение>	––change <политика>, <параметр>, <значение>	Настройка параметра <параметр> – выбор и установка параметра из доступного перечня: • state – состояние; • mode – режим работы; • log_perm_exec – регистрация исполнения файлов; • log_deny_exec – регистрация запрета исполнения файлов; • log_perm_openlib – регистрация загрузки библиотек; • log_deny_openlib – регистрация запрета загрузки библиотек; • log_perm_openfile – регистрация открытия файлов; • log_deny_openfile – регистрация запрета открытия файлов; • alg – алгоритм расчета контрольных сумм • verbose – детализация сообщений; • snauditd – сервис аудита; • sntrashd – сервис безопасного удаления; • snjournald – сервис журналирования; • snnetwork – сервис удаленного управления; • clear_log – перезапись журнала при переполнении; • system_lock – сервис блокировки системы при нарушении КЦ; • ident – метод идентификации; • strength – усиленная аутентификация; • lock – реакция на изъятие идентификатора; • cache – кешировать данные идентификатора для доменных пользователей; • deny – кол-во неудачных попыток входа; • unlock_time – время блокировки при достижении количества неудачных попыток аутентификации (мин.); • lock_delay – максимальный период неактивности до блокировки экрана (мин.); • last_log – оповещение пользователя о последнем успешном входе; • min_passwd_size – минимально допустимая длина для нового пароля; • passwd_strength – пароль должен соответствовать требованиям сложности; • max_days – число дней, после которых срок действия пароля истекает; • min_days – минимальное количество дней между сменами пароля; • warn_days – дни до истечения срока действия пароля, когда пользователь будет предупрежден; • inactive_days – число дней после устаревания пароля до его блокировки

Плагин	Политика	Параметр	Значение
aec	aec	state	0 – выключено; 1 – включено
		mode	0 – мягкий режим; 1 – жесткий режим
		log_perm_exec	0 – выключено; 1 – включено
		log_deny_exec	0 – выключено; 1 – включено
		log_perm_ openlib	0 – выключено; 1 – включено
		log_deny_openlib	0 – выключено; 1 – включено
		log_perm_ openfile	0 – выключено; 1 – включено
		log_deny_ openfile	0 – выключено; 1 – включено
aide	aide	state	0 – выключено; 1 – включено
		alg	0 – алгоритм MD5; 1 – алгоритм GOST R 34.11-2012; 2 – алгоритм SHA-512. Значение по умолчанию
control	access_control	mode	0 – выключено; 1 – включено
	memory	mode	0 – выключено; 1 – включено
cups	cups	state	0 – выключено; 1 – включено
devices	devices_control	state	0 – выключено; 1 – включено
		verbose	0 – выключена регистрация; 1 – включена регистрация неуспешных попыток доступа; 2 – включена регистрация всех попыток доступа
firewall	firewall	state	0 – выключено; 1 – включено
service_ mgr	services	snauditd	0 – выключено; 1 – включено
		sntrashd	0 – выключено; 1 – включено
		snjournald	0 – выключено; 1 – включено
		snnetwork	0 – выключено; 1 – включено
system	system	clear_log	0 – выключено; 1 – включено
		system_lock	0 – выключено; 1 – включено

Плагин	Политика	Параметр	Значение
token_mgr	authentication	ident	0 – логин введен с клавиатуры; 1 – логин определен персональным идентификатором; 2 – смешанный (используется клавиатура или персональный идентификатор)
		strength	0 – выключено; 1 – включено
		state	0 – выключено; 1 – включено
		lock	0 – не блокировать; 1 – блокировать станцию при изъятии любого идентификатора; 2 – блокировать станцию при изъятии USB-идентификатора
		cache	0 – выключено; 1 – включено
		deny	<число> – количество неудачных попыток входа в диапазоне от 0 до 999999
		unlock_time	<число> – время блокировки учетной записи при достижении количества неудачных попыток аутентификации в диапазоне от 0 до 90 минут
		lock_delay	<число> – максимальный период неактивности до блокировки экрана. Возможный диапазон зависит от ОС
		last_log	0 – выключено; 1 – включено
users	users	min_passwd_size	<число> – длина для нового пароля в диапазоне от 6 до 16
		passwd_strength	0 – выключено; 1 – включено
		max_days	<число> – количество дней в диапазоне от -1 до 9999
		min_days	<число> – количество дней в диапазоне от 0 до 999999
		warn_days	<число> – количество дней в диапазоне от 0 до 999999
		inactive_days	<число> – количество дней в диапазоне от -1 до 999999

Примеры команд:

snpolctl -p token_mgr -c authentication,strength,1	Установить значение параметра "Усиленная аутентификация" — "Включено"
snpolctl -p token_mgr -c authentication,lock,0	Установить значение параметра "Реакция на изъятие электронного идентификатора" — "Не блокировать"
snpolctl -p control -c access_control,mode,1	Установить значение параметра "Режим работы" подсистемы разграничения доступа к объектам файловой системы на основе дискреционного управления доступом — "Включено"

snpolctl -p aec -c aec,mode,1	Установить значение параметра "Режим работы" подсистемы разграничения доступа к объектам файловой системы на основе ЗПС — "Жесткий режим"
snpolctl -p users -c users,min_passwd_size,10	Установить значение параметра "Минимально допустимая длина для нового пароля" — "10" символов

Управление персональными идентификаторами

Для выполнения операций с персональными идентификаторами используется утилита **sntokenctl**, расположенная в каталоге /opt/secretnet/bin. Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
sntokenctl <ключ> [<параметр>] ... [<ключ>] [<параметр>]
```

Описание ключей представлено в следующей таблице:

Ключ		Описание
–h	––help	Выводит справочную информацию о применении утилиты
–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", "–L", "–U" и "–u"
–c <ПОЛЬЗОВАТЕЛЬ>	––change <ПОЛЬЗОВАТЕЛЬ>	Меняет ключи пользователя. Не используется с ключами "–P", "–K", "–b", "–L", "–U"и "–u"
–p	––write–password	Записывает пароль пользователя в идентификатор. Используется с ключом "–b"
–k	––write–key	Записывает закрытый ключ в идентификатор. Используется с ключом "–b". Если у пользователя еще нет пары ключей, она генерируется. Если у пользователя уже есть пара ключей, необходимо предъявить идентификатор, в котором хранится закрытый ключ
–E	––enable–sable	Разрешает работу персональных идентификаторов с ПАК "Соболь". Используется с ключами "–b" и "–p"
–A	––bind–sable–admin	Привязывает персональный идентификатор администратора ПАК "Соболь". Используется с ключами "–b" и "–p"
–s <НОМЕР>	––serial <НОМЕР>	Выполняет операцию с идентификатором с указанным серийным номером. Используется с ключами "–u", "–P", "–K", "–r", "–L", "–U" и "–R"
–P	––add–password	Дозаписывает пароль на уже привязанный идентификатор. Не используется с ключами "–b", "–R", "–L", "–U" и "–u"

Ключ		Описание
–K	––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 "–b", "–r", "–L", "–U" и "–u"
-t	--store-password	Включает режим хранения пароля. Используется вместе с опциями '-b' или '-s'
–r	––remove–password	Удаляет пароль пользователя из привязанного идентификатора
–R	––remove–key	Удаляет закрытый ключ из ранее привязанного идентификатора
–D	––disable–sable	Запрещает вход в ПАК "Соболь" по персональному идентификатору. Используется с ключом "–s"
–u	––unbind	Отвязывает идентификатор. Не используется с ключами "–P", "–K", "–L", "–U" и "–b"
–d	––delete	Удаляет данные Secret Net LSP из идентификатора. Используется с ключом "–u"
–e	––erase	Удаляет данные из идентификатора. Идентификатор не должен быть присвоен пользователю
–L	––lock	Блокирует идентификатор
–U	––unlock	Разблокирует идентификатор
–S	––change–password	Меняет пароль пользователя на пароль, хранящийся в идентификаторе. Используется совместно с ключом "–B"

Примеры команд:

sntokenctl –b test_user –p –E	Привязать новый идентификатор к пользователю test_user и записать в идентификатор пароль для разрешения входа в ПАК "Соболь"
sntokenctl –b test_user –p –A	Привязать персональный идентификатор администратора ПАК "Соболь" для пользователя test_user и записать в идентификатор пароль
sntokenctl –s 12345678 –D	Запретить вход в ПАК "Соболь" по персональному идентификатору с серийным номером 12345678
sntokenctl –u –s 12345678	Отвязать идентификатор с серийным номером 12345678
sntokenctl –L –s 12345678	Заблокировать идентификатор с серийным номером 12345678

Управление ПАК "Соболь" в режиме интеграции с Secret Net LSP

Для управления взаимодействием с ПАК "Соболь" используется утилита **snsablectl**, расположенная в каталоге /opt/secretnet/bin. Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
snsablectl <ключ> [-l <пользователь>] [-p <пароль>]
```

Описание ключей представлено в следующей таблице:

Ключ		Описание
-h	--help	Вывести справочную информацию о применении утилиты
-c	--connect	Подключить ПАК "Соболь" к Secret Net LSP
-d	--disconnect	Отключить ПАК "Соболь" от Secret Net LSP
-s	--status	Отобразить текущее состояние взаимодействия ПАК "Соболь" и Secret Net LSP
-n	--network	Включить режим удаленного управления ПАК "Соболь". Используется с опцией -c
-l <пользователь>	--login <пользователь>	Задать логин администратора домена. Используется с опцией -n
-p <пароль>	--password <пароль>	Задать пароль администратора домена. Используется с опцией -n
-r	--remove-users	Запретить доступ к ПАК "Соболь" для всех локальных пользователей
-a	--copy-admin-token	Копировать идентификатор администратора ПАК "Соболь". До окончания копирования идентификатора необходимо наличие подключенного идентификатора администратора ПАК "Соболь"
-g	--get-icheck	Получить конфигурации контроля целостности
-t	--set-icheck <объект>	Поставить на контроль целостности объект: files, sectors, smbios, pci-lite, pci-norm, pci-exit
-u	--unset-icheck <объект>	Снять с контроля целостности объект: files, sectors, smbios, pci
-k	--recalc-checksum	Пересчитать контрольные суммы шаблонов
-f	--force	Не запрашивать подтверждение

Примеры команд:

snsablectl –s	Выполняется отображение текущего состояния взаимодействия ПАК "Соболь" и Secret Net LSP
snsablectl –c –n –l DOMAIN\\Petrov	Выполняется включение удаленного режима управления для администратора домена. После выполнения команды необходимо ввести пароль

Разграничение доступа к устройствам

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

Ключ		Описание
-l	--list	Отображает список шин и устройств. Для отображения подробной информации используется ключ verbose. Список контролируемых устройств формируется автоматически при подключении устройств к шинам. Устройства регистрируются, только если для модели/класса/шины задан параметр подключения dc=enabled. При режиме not-control устройство не регистрируется. Некоторые устройства в контроле устройств могут определяться по-иному. Например, современные телефоны/смартфоны, как правило, являются составными устройствами, в связи с чем они будут разнесены по нескольким классам, например: ethernet, bluetooth, digital-camera
-r	--rules	Отображает правила для шин и устройств. Используется с параметрами --dev-id, --bus-id для отображения детальной информации
-a	--add	Добавляет устройство. Необходимо указать параметры '--idVendor', '--idProduct', '--vendor', '--product' и '--serial' . Добавление устройств, в том числе через csv-шаблон, доступно только для устройств из шины USB
-m	--model	Добавляет модель. Необходимо указать параметры '--idVendor', '--idProduct', '--product', '--bus-id' и '--class-id' . Невозможно добавить модель устройства в класс электронных идентификаторов и считывателей --class-id=usb_uid. Несколько USB-флеш-накопителей одной модели или электронные идентификаторы определяются как одно устройство (с одним id, правила для них общие)
-d	--delete	Удаляет устройство или модель
-s	--set	Устанавливает параметры для шины или устройства. При работе с PCI-слотами назначенные права сохраняются для слота. Один и тот же адаптер при подключении к разным слотам определяется как разные адаптеры. Для одного адаптера в разных слотах можно задать разные права. Невозможно назначить правила в случае действующего наследования
-c	--config	Проверяет и утверждает аппаратную конфигурацию
-i	--import	Импортирует устройства и модели из csv-файла. Добавление устройств через csv-шаблон доступно только для устройств из шины USB

Параметры для команд:

Параметр	Описание
--bus-id	Идентификатор для шины
--class-id	Идентификатор для класса
--dev-id	Идентификатор для устройства
--object-id	Идентификатор для объекта
--idVendor	Идентификатор производителя
--idProduct	Идентификатор продукта
--vendor	Производитель

Параметр	Описание
--product	Продукт
--serial	Серийный номер
--desc	Описание объекта
--user=[<пользователь>]:[RULE]	Данные пользователя. Описание параметра RULE: • none – нет доступа; • read – только чтение; • write – чтение и запись; • delete – удаление всех установленных прав на устройства
--group=[<группа>]:[RULE]	Данные группы
--default=[RULE]	Правило разграничения доступа для группы BCE
--dc=[RULE_DC]	Правило контроля подключения. Описание параметра RULE_DC: • not-control – подключение не контролируется; • enabled – подключение разрешено; • disabled – подключение запрещено; • fixed – устройство подключено постоянно; • lock – блокировать станцию при изменении состояния устройства. Подробное описание правил указано в таблице ниже. Для шины "Локальные устройства", классов устройств "Последовательные порты", "Параллельные порты" должны быть доступны режимы доступа: **not-control**, **fixed**, **lock**. Для всех остальных объектов должны быть доступны все режимы, перечисленные выше
--inh-acl=[INH]	Наследование правил разграничения доступа. Описание параметра INH: • enabled – наследовать правила от родительского объекта; • disabled – наследование отключено; • enable-child – включить наследование для всех дочерних объектов и устройств
--inh-dc=[INH]	Наследование правил контроля подключения

Правило	Описание
Устройство не контролируется (**not-control**)	Для объекта отключен режим контроля. Изменение состояния устройства не отражается в журнале
Устройство постоянно подключено к компьютеру (**fixed**)	Для объекта включен режим контроля, при котором устройство должно быть постоянно подключено к компьютеру. При включении компьютера и в процессе его работы осуществляется контроль аппаратной конфигурации. В случае изменения состояния (отключения, подключения, модификации) устройства с режимом "Постоянно подключено к компьютеру": • в журнале должен регистрироваться Alert ("Hardware configuration control error."); • в сеансе пользователя должно всплывать окно с тревогой; • система должна ожидать утверждение изменений аппаратной конфигурации администратором; • на СБ SNS должно отправляться событие несанкционированного доступа (если осуществляется централизованное управление)

Блокировать компьютер при изменении устройства (**lock**)	Режим автоматического блокирования компьютера при изменении состояния устройств. Возможность разблокировки компьютера должен иметь только администратор
Подключение устройства разрешено (**enabled**)	Включен режим контроля, при котором устройство разрешается подключать к компьютеру и отключать. В случае изменения состояния устройства в журнале регистрируются соответствующие события. Утверждение изменений аппаратной конфигурации при этом не требуется
Подключение устройства запрещено (**disabled**)	Для объекта включен режим контроля, при котором устройство запрещается подключать к компьютеру. При попытке подключения устройства: • доступ к устройству должен быть запрещен; • в журнале должен регистрироваться Alert (Device connection denial. Reason: specified connection control parameters. Device: <Параметры устройства>); • в сеансе пользователя должно всплывать окно с тревогой; • на СБ SNS должно отправляться событие несанкционированного доступа (если осуществляется централизованное управление)

Примечание.
- При утверждении аппаратной конфигурации в шине local будет показано уведомление (система запрашивает, не повлияет ли изменение на возможность загрузки системы).
- Если правила конфигурации компьютера будут нарушены, появится уведомление, и в некоторых случаях компьютер будет заблокирован.

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 --set --dev-id=1 --user=test:write --group=test:read --default=none	Установить права доступа к устройству 1. Права доступа: для пользователя test — запись; для группы test — чтение; для остальных — нет доступа
sndevctl --set --bus-id=usb --user=test:write --group=test:read --default=none	Установить права доступа к USB-шине: для пользователя test — запись; для группы test — чтение; для остальных — нет доступа

Работа с CSV-файлами

При добавлении устройства через csv-шаблон необходимо создать .csv-файл. Для этого необходимо ввести в командную строку следующее:

```
touch ИМЯ_ФАЙЛА.csv
```

Csv-файл должен заполняться по шаблону:

```
Serial Number;Manufacturer;Description;PID;VID;
Device Class;Comment - заголовок
```

Внимание!
При заполнении csv-файла заголовок является обязательным.

Примечание.
Шаблон для заполнения csv-файла поставляется с пакетом Secret Net LSP и располагается в /opt/secretnet/share/device_templates/new_devices.csv.

В файле для параметра Device Class класс указывается в виде идентификатора:

Идентификатор	Описание
1002	Сетевые платы и модемы
1003	Интерфейсные устройства (мышь, клавиатура, ИБП и др.)
1006	Сканеры и цифровые фотоаппараты
1007	Принтеры
1008	Устройства хранения
1256	Bluetooth-адаптеры
1257	Сотовые телефоны (смартфоны, КПК)
1258	Электронные считыватели
1299	Прочие

Пример заполнения csv-файла:

```
0001;vend storage;storage;1001;2001;
1008; - параметры устройств
```

Независимо от уровня объекта, из которого вызвано добавление, при добавлении экземпляров и моделей устройств путем импорта .csv-файла требуются следующие параметры:

	Обязательные	Необязательные
Экземпляр устройства	Класс, VID, PID, Описание, Производитель, Серийный номер	Комментарий
Модель устройства	Класс, VID, PID, Описание	Производитель, Комментарий

Для добавление устройства через csv-шаблон:

1. Введите в командную строку следующее:

   ```
   sndevctl -i ИМЯ_ФАЙЛА.csv
   ```

Появится строка "Введите действие".

2. В строке "Введите действие" введите **a** и нажмите клавишу "Enter".

   Примечание.
   Для вывода справки введите **h**.

Контроль целостности

Для выполнения процедур, связанных с контролем целостности объектов файловой системы, 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
-i	--init	Проводит инициализацию базу данных контроля целостности. Если указан данный ключ, остальные ключи не учитываются
-l	--list=[ФАЙЛ,…]	Показывает файлы, для которых включен контроль целостности. Может принимать аргумент — разделенный запятыми список файлов. Формат вывода: csopm bl [R] <object> Опции полноты КЦ: • c – контрольная сумма; • s – размер; • o – владелец (user и group); • p – права доступа; • m – время изменения. Опции действий: • b – восстановить объект; • l – заблокировать станцию; • [R] – признак КЦ в реальном времени. 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: • 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
-v	--view-schedule	Выводит текущие настройки расписания КЦ

Ключ		Описание
-a	--add-schedule-entry '<мм чч дд мес дн>'	Добавляет новую запись в расписание КЦ, где: • мм – минуты; • чч – часы; • дд – день; • мес – месяц; • дн – день недели (допустимые значения 0-6. 0 – воскресенье). Вместо неиспользуемых параметров используйте символ *
-d	--delete-schedule-entry <НОМЕР>	Удаляет запись под определенным номером из расписания КЦ
-r	--real-time	Устанавливает контроль целостности в реальном времени для всех объектов в данном запросе. Используется с действием --set

Внимание!
В некоторых случаях, в зависимости от структуры каталогов и наличия символических 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
snaidectl --add-schedule '* * -'	Всегда выключено
snaidectl --add-schedule '12-14 1-5 +'	Добавляет расписание КЦ: с 12.00 по 14.59.59 Понедельник-Пятница Включено
snaidectl --add-schedule '10-12,14,16 6,7 + '	Добавляет расписание КЦ:с 10.00 по 12.59.59 и с 14.00 по 14.59.59, и с 16.00 по 16.59.59 Суббота,Воскресенье Включено
snaidectl --add-schedule '* * -# 12-14 1-5 + # 10-12,14,16 6,7 + '	Три примера выше в одной команде
snaidectl --add-schedule '30 12 * * *'	Добавляет расписание КЦ на каждый день в 12:30
snaidectl --add-schedule '* * 17 * *'	Добавляет расписание КЦ на 17 день каждого месяца. Можно указать время
snaidectl --add-schedule '* * * 6 *'	Добавляет расписание КЦ на июнь
snaidectl --add-schedule '* * * * 3'	Добавляет расписание КЦ на каждую среду

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 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
-r	--result=РЕЗУЛЬТАТ	Результат выполнения действия: 0 – любой; 1– успех; 2 – неудача. Если аргумент не указан или имеет неверное значение, используется значение 0
-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: • 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

Работа с лицензиями

Для работы с лицензиями используется утилита **snlicensectl**, расположенная в каталоге /opt/secretnet/bin.

Ключ		Описание
-s	--status	Отображает текущий статус лицензии
-c	--change <путь к файлу лицензии>	Изменяет текущую лицензию
-d	--delete <имя компонента>	Удаляет текущую лицензию для компонента
-n	--name <имя компонента>	Выводит имя компонента для замены лицензии
-h	--help	Отображает доступные команды для утилиты

Примечание.
Невозможно удалить лицензию для модуля CORE.

В Secret Net LSP предусмотрено централизованное управление лицензиями через сервер безопасности SNS.

В случае истечения срока лицензии, Secret Net LSP перейдет в "ограниченный режим". Изменение политик при работе в "ограниченном режиме" будет недоступно. Для выхода из "ограниченного режима" необходимо заменить просроченную лицензию или отключить подсистему с истекшей лицензией.

Примеры команд:

snlicensectl -n FW -c license.lic	Выполнить замену лицензии для компонента FW
snlicensectl -d FW	Удалить лицензию у компонента FW

Замкнутая программная среда

Для выполнения настройки замкнутой программной среды используется утилита **snaecctl** , расположенная в каталоге /opt/secretnet/bin. Утилита выполняет действия в режиме командной строки от имени текущего пользователя. Строка команды имеет следующий формат:

```
snaecctl [<аргумент>] [<команда>] [<ключ> [<параметр>]] ...
[<ключ> [<параметр>]]
```

Описание аргументов представлено в следующей таблице:

Аргумент		Описание
-h	--help	Выводит справочную информацию о применении утилиты

Описание команд и ключей представлено в таблицах ниже.

Команда view

Команда view выводит список правил, пользователей или групп.

Ключ		Описание
-h	--help	Выводит справочную информацию о применении команды
-n<имя правила>	--name<имя правила>	Выводит пользовательское правило с указанием имени, режима, статуса, списка пользователей, групп и ресурсов
-u<имя пользователя>	--user<имя пользователя>	Выводит правила, действующие для конкретного пользователя
-g<имя группы>	--group<имя группы>	Выводит правила, действующие для конкретной группы

Ключ		Описание
-U	--view-users	Выводит белый список пользователей
-G	--view-groups	Выводит белый список групп
-R	--view-white-resources	Выводит список исключений для ресурсов
-r	--view-resources	Выводит список правил и ресурсов
-s	--system	Выводит перечень всех системных правил

Примеры команд:

snaecctl view	Выводит перечень всех правил без списков ресурсов
snaecctl view -u Petrov -r	Выполняется отображение правил и ресурсов, действующих для пользователя Petrov, а также правил, действующих для всех пользователей
snaecctl view -U -G	Выполняется отображение белого списка пользователей и групп

Команда add

Команда add добавляет ресурсы в правила, не перезаписывая их.

Ключ		Описание
-h	--help	Выводит справочную информацию о применении команды
-n<имя правила>	--name <имя правила>	Добавление нового правила. По умолчанию правило создается со статусом "True", с режимом "Standard", с пустым списком ресурсов и разрешенным для всех пользователей системы
-u <имя пользователя>	--user <имя пользователя>	Добавление нового пользователя в белый список
–g <имя группы>	--group <имя группы>	Добавление новой группы в белый список
-r <путь к ресурсу>	--resource <путь к ресурсу>	Добавление ресурса в список исключений. Допускается использовать относительный путь к ресурсу, при добавлении в правило он преобразуется в абсолютный путь
-d	--no-depend	Отключение поиска зависимостей от динамических библиотек при добавлении бинарных исполняемых файлов
–R	––recursive	Добавление ресурсов в правило рекурсивно
-f <имя ресурсного файла>	--resource-file <имя ресурсного файла>	Добавление ресурсного файла json-формата в правило
-D	--disable	Добавление нового правила в выключенном режиме. Ключ можно использовать только для создаваемого правила
-X	--extended	Добавление нового правила в усиленном режиме. Ключ можно использовать только для создаваемого правила. Для подтверждения жесткого режима на компьютере пользователя, выполните команду с правами учетной записи суперпользователя: **snaecctl confirm**
-C	--force	Не спрашивать подтверждение

Примеры команд:

snaecctl add –n newrule –D	Выполняется добавление нового правила newrule в выключенном режиме
snaecctl add –u Ivanov -g Test	Выполняется добавление пользователя Ivanov и группы Test в белый список
snaecctl add –n newrule1 -r /usr/sbin/ -R	Выполняется добавление ресурсов в правило newrule1 рекурсивно

Команда rm

Команда rm удаляет правила, пользователей или группы.

Ключ		Описание
-h	--help	Выводит справочную информацию о применении команды
-n <имя правила>	--name <имя правила>	Удаление правила с указанием его имени
-r <путь к ресурсу>	--resource <путь к ресурсу>	Удаление из правила ресурсов. Правило может остаться с пустым списком ресурсов
-u<имя пользователя>	--user<имя пользователя>	Удаление пользователя из правила
-g<имя группы>	--group<имя группы>	Удаление группы из правила
-A	--all-rules	Удаление всех правил
-C	--force	Не спрашивать подтверждение

Примеры команд:

snaecctl rm –n newrule	Выполняется удаление правила newrule. При выполнении операции запрашивается подтверждение
snaecctl rm –n newrule –u Petrov -g Test	Выполняется удаление пользователя Petrov и группы Test из правила newrule. Если при этом в правиле не останется пользователей и групп, для которых действует правило, будет предложено удалить правило. В случае отказа вся операция удаления отменяется, так как правило не может быть не разрешенным ни для кого

Команда update

Команда update перезаписывает правила. При этом ресурсы, добавленные ранее в правило, удаляются.

Ключ		Описание
-h	--help	Выводит справочную информацию о применении команды
-n<имя правила>	--name<имя правила>	Обновление правила
-u<имя пользователя>	--user<имя пользователя>	Обновление списка пользователей, для которых действует правило
-g<имя группы>	--group<имя группы>	Обновление списка групп, для которых действует правило
-r<путь к ресурсу>	--resource<путь к ресурсу>	Обновление списка ресурсов в правиле
-d	--no-depend	Отключение поиска зависимостей бинарных исполняемых файлов от динамических библиотек при обновлении списка ресурсов

Ключ		Описание
-R	--recursive	Обновление ресурсов в правиле рекурсивно
-f <имя ресурсного файла>	--resource-file <имя ресурсного файла>	Обновление ресурсного файла json-формата в правиле
-a	--all-users	Разрешение действия правила для всех пользователей системы
-C	--force	Не спрашивать подтверждение

Примеры команд:

snaecctl update –n newrule -r /usr/bin/fly-wm /usr/sbin/cupsd -f resource_file.json -d -R	Выполняется обновление списка ресурсов /usr/bin/fly-wm и /usr/sbin/cupsd, ресурсного файла json-формата, отключение поиска зависимостей. Обновление ресурсов в правиле newrule рекурсивно
snaecctl update –n newrule –a	Выполняется разрешение действия правила для всех пользователей системы

Команда reload

Команда reload выполняет перерасчет контрольных сумм для ресурсов.

Ключ		Описание
–h	––help	Выводит справочную информацию о применении команды
–n<имя правила>	––name<имя правила>	Перерасчет контрольных сумм для ресурсов, указанных в правиле
–w	––whitelist	Перерасчет контрольных сумм для белого списка пользователей и групп

Пример команды:

snaecctl reload	Обновление контрольных сумм для всех ресурсов и загрузка правил в ядро
snaecctl reload–n newrule	Выполняется перерасчет контрольных сумм для ресурсов, указанных в правиле newrule

Команда enable

Команда enable включает правило.

Ключ		Описание
–h	––help	Выводит справочную информацию о применении команды
–n<имя правила>	––name<имя правила>	Включает правило

Пример команды:

snaecctl enable –n newrule newrule1	Выполняется включение правил newrule и newrule1

Команда disable

Команда disable выключает правило.

Ключ		Описание
–h	––help	Выводит справочную информацию о применении команды
–n<имя правила>	––name<имя правила>	Выключает правило

Пример команды:

snaecctl disable –n newrule newrule1	Выполняется выключение правил newrule и newrule1

Команда rename

Команда rename переименовывает правила.

Ключ		Описание
–h	––help	Выводит справочную информацию о применении команды
–n<имя правила> –N<новое имя правила>	––name<имя правила> ––new–name<новое имя правила>	Переименование текущего имени правила на новое имя

Пример команды:

snaecctl rename –n newrule -N newrule1	Выполняется переименование текущего имени правила newrule на новое имя newrule1

Команда export

Команда export экспортирует ресурсы правила в файл.

Ключ		Описание
–h	––help	Выводит справочную информацию о применении команды
–n<имя правила> –f<имя ресурсного файла>	––name<имя правила> ––resource–file<имя ресурсного файла>	Экспортирование ресурсов правила в json-файл

Пример команды:

snaecctl export –n newrule -f data	Выполняется экспортирование ресурсов правила newrule в json-файл data

Команда log

Команда log осуществляет анализ журнала аудита для построения правил ЗПС.

Ключ		Описание
–l	––list	Выводит список всех пользователей и групп, для которых в журнале аудита зарегистрированы события ЗПС
–n<имя правила>	––name<имя правила>	Задает правило ЗПС с указанием его имени и сохраняет в правиле ресурсы, для которых в журнале аудита зарегистрированы события ЗПС
–u<имя пользователя>	––user<имя пользователя>	Задает правило ЗПС с указанием имени конкретного пользователя, для которого действует правило и по имени которого будет фильтроваться журнал аудита
–g<имя группы>	––group<имя группы>	Задает правило ЗПС с указанием имени группы пользователей, для которой действует правило и по имени которой будет фильтроваться журнал аудита
–f<имя файла>	––resource-file<имя файла>	Сохраняет ресурсы, запущенные пользователем, в файл с указанием его имени
–e	––exec-file<путь к исполняемому файлу>	Задает правило ЗПС с указанием исполняемого файла, для которого действует правило и по которому будет фильтроваться журнал аудита
–I	––initial–time<время начала анализа ресурсов	Задает правило ЗПС с указанием времени начала анализа ресурсов по журналу аудита. Значения ключа –I/––initial–time должны иметь формат: "день-месяц-годТчасы:минуты:секунды". • Параметр "год" указывается в диапазоне от 1900 до 9999; • Параметр "месяц" указывается в диапазоне от 1 до 12; • Параметр "день" указывается в диапазоне от 1 до 31; • Параметр "часы" указывается в диапазоне от 0 до 23; • Параметр "минуты" указывается в диапазоне от 0 до 59; • Параметр "секунды" указывается в диапазоне от 0 до 59. При вводе параметров даты начала анализа ресурсов разделяйте их символом "-" (дефис). При вводе параметров времени начала анализа ресурсов разделяйте их символом ":" (двоеточие). Для разделения параметров даты и параметров времени используйте прописную букву "T"

Ключ		Описание
–F	––final–time<время окончания анализа ресурсов>	Задает правило ЗПС с указанием времени окончания анализа ресурсов по журналу аудита, не включая время, указанное в значении аргумента. Значения ключа –F/––final–time должны иметь формат: "день-месяц-годТчасы:минуты:секунды". • Параметр "год" указывается в диапазоне от 1900 до 9999; • Параметр "месяц" указывается в диапазоне от 1 до 12; • Параметр "день" указывается в диапазоне от 1 до 31; • Параметр "часы" указывается в диапазоне от 0 до 23; • Параметр "минуты" указывается в диапазоне от 0 до 59; • Параметр "секунды" указывается в диапазоне от 0 до 59. При вводе параметров даты окончания анализа ресурсов разделяйте их символом "-" (дефис). При вводе параметров времени окончания анализа ресурсов разделяйте их символом ":" (двоеточие). Для разделения параметров даты и параметров времени используйте прописную букву "T"
-C	--force	Не спрашивать подтверждение

Примеры команд:

snaecctl log -u user -n RULE_1	Выполняется сохранение всех ресурсов, запущенных пользователем "user", в правило "RULE_1" с разрешением этого правила для данного пользователя
snaecctl log -n RULE_1 -u user -I 28-2-2020T17:00–a	Выполняется сохранение в правило "RULE_1" всех ресурсов, запущенных пользователем "user", начиная с 17:00 28 февраля 2020 года до текущего момента

Настройка удаленного управления

Для настройки удаленного управления используется утилита **snnetctl**, расположенная в каталоге /opt/secretnet/bin. Компьютер должен быть включен в домен и подчинен серверу безопасности в структуре управления.

Ключ		Описание
-e	--enable	Включает режим удаленного управления. В обязательном порядке также необходимо указать параметр -u
-d	--disable	Выключает режим удаленного управления
-s	--status	Показывает текущее состояние соединения с сервером безопасности
-u	--login <login>	Определяет доменное имя пользователя данного компьютера, под которым он будет входить в систему
-t	--timeout <value>	Определяет периодичность, с которой клиент обновляет свои настройки при включенном удаленном управлении. Возможные значения: 0, 10, 30, 60
-v	--servers	Показывает lds сервера
-c	--lds-server <server>	Определяет приоритетный сервер lds для подключения
-h	--help	Выводит справочную информацию о применении утилиты

Примеры команд:

snnetctl -e -u user1	Подключиться к серверу безопасности под именем пользователя user1
snnetctl --disable	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.

Примечание.
Утилита **snbckctl** предназначена для переноса и восстановления настроек Secret Net LSP между ОС одного типа.

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: • snsettings – база данных настроек Secret Net LSP; • logs – журналы; • policies – политики; • auth – параметры аутентификации; • access – управление доступом; • aec – правила ЗПС; • firewall – параметры межсетевого экрана. Не может использоваться с опциями "-r" или "-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. Допустимые объекты: • snsettings – база данных настроек Secret Net LSP; • logs – журналы; • policies – политики; • auth – параметры аутентификации; • access – управление доступом; • aec – правила ЗПС; • firewall – параметры межсетевого экрана. Не может использоваться с опциями "-b" и "-d"
-e	--export	Экспортирует резервные копии. Требуется указание опции "-i"
-m	--import	Импортирует резервные копии. Требуется указание опции "-i"

Ключ		Описание
-f	--force	Игнорирует различие схем баз данных
-i	--id <ID>	Указывает ID резервной копии. Используется совместно с опциями "-r" и "-d"
-c	--comment	Комментарий для новой резервной копии. Используется совместно с опцией "-b"
-L	--license	Восстанавливает лицензию. Используется совместно с опцией '-r' Действует только при восстановлении настроек Secret Net LSP

Примеры команд:

snbckctl -b	Выполняет полное резервное копирование
snbckctl -r -i 10	Выполняет полное восстановление из резервной копии с ID 10
snbckctl --backup=snsettings	Выполняет резервное копирование базы данных настроек Secret Net LSP
snbckctl -i 11 --restore=aec	Восстанавливает правила ЗПС из резервной копии с ID 11

Экспорт и импорт настроек Secret Net LSP

Для экспорта настроек:

1. Выполните резервное копирование настроек Secret Net LSP:

   ```
   #snbckctl –b
   ```

   или

   ```
   #snbckctl ––backup
   ```

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

2. Проверьте, что резервная копия была создана:

   ```
   #snbckctl –l
   ```

   или

   ```
   #snbckctl ––list
   ```

3. Выполните экспорт необходимой резервной копии:

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

   или

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

   При экспорте будет создан файл архива резервной копии настроек с расширением .tar.gz.

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>
```

Перенос конфигурации Secret Net LSP предыдущих версий на текущую версию Secret Net LSP

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 при обновлении версии СЗИ. Также доступна возможность применить сохраненную конфигурацию при установке.

Для переноса конфигурации:

1. Выполните вход в систему под учетной записью суперпользователя.
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 (см. стр.30).
5. Обновите ОС до необходимой версии ядра.
6. Установите текущую версию Secret Net LSP (см. стр.27).
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.

Для применения конфигурации при установке:

1. Создайте временную переменную. Для этого в командной оболочке выполните команду:

   ```
   export SNTEMPLATE_TARBALL=
   /home/tester/backup/1645535542.tar.gz
   ```
2. Выполните установку с указанием этой переменной. Для этого в командной оболочке выполните команду:

   ```
   SNTEMPLATE_TARBALL=
   /home/tester/backup/1645535542.tar.gz rpm –ivh <имя пакета
   secretnet>
   ```

   ```
   SNTEMPLATE_TARBALL=
   /home/tester/backup/1645535542.tar.gz dpkg -i <имя пакета
   Firewall>
   ```

Работа с журналами

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

- просматривать записи системного журнала и журнала аудита;
- удалять записи из базы данных журналов;
- экспортировать записи журналов в файл;
- импортировать записи журналов из файла;
- сортировать события.

Утилита вызывается из каталога /opt/secretnet/bin.

Ключ		Описание
-h	--help	Вывести справочную информацию о применении утилиты
-S	--syslog	Использовать базу данных системных журналов
-A	--audit	Использовать базу данных событий аудита
-w	--view	Просмотр только выбранных записей. Если временной период не указан, по умолчанию берется текущий день
-e	--export=ФАЙЛ	Экспорт журналов из базы в ФАЙЛ
-d	--delete	Удалить экспортированные записи из базы
-i	--import=ФАЙЛ	Импорт журналов из ФАЙЛа в базу данных
-D	--delete-only	Удаление записи только 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)
-p	--priority= ПРИОРИТЕТ	Просмотр/экспорт записей с заданным приоритетом. Принимает числовой уровень журнала: "emerg" (0), "alert" (1), "crit" (2), "err" (3), "warning" (4), "notice" (5), "info" (6), "debug" (7)
-m	--min=ПРИОРИТЕТ	Просмотр/экспорт записи, начиная с заданного приоритета. Работает только с базой данных системных журналов
-M	--message=ТЕКСТ	Просмотр/экспорт записи, содержащей ТЕКСТ
-u	--user= ПОЛЬЗОВАТЕЛЬ	Просмотр/экспорт записи для определенного пользователя. Работает только с базой данных событий аудита
-g	--group=ГРУППА	Просмотр/экспорт записи для определенной группы. Работает только с базой данных событий аудита
-a	--app= ПРИЛОЖЕНИЕ	Просмотр/экспорт записи для определенного приложения
-o	--object=ОБЪЕКТ	Просмотр/экспорт записи для определенного объекта. Работает только с базой данных событий аудита

Ключ		Описание
-r	--result=РЕЗУЛЬТАТ	Просмотр/экспорт записи с определенным результатом. Принимает числовой результат: "Ошибка" (0), "Успешно" (1)
-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 SecretNet events/Общие события Secret Net LSP
System services events/События системных сервисов
Audit events/События подсистемы аудита
Authentication/Аутентификация и идентификация
Integrity/Контроль целостности
Printing/Система печати
Testing/Тестирование
Selftest/Самодиагностика
Trash daemon/Сервис очистки файловой системы
Journal subsystem/Сервис журналирования
Backup/Резервное копирование
Hardware Trusted Boot/ПАК "Соболь"
AEC management/Управление ЗПС
Firewall management/Управление межсетевым экраном
Common control/Общие настройки
Audit control/Управление аудитом

Service control/Управление сервисами
User control/Управление пользователями
Integrity control/Управление контролем целостности
Access control/Управление контролем доступа
Strengthen authentication control/Управление усиленной аутентификацией
Backup control/Управление резервным копированием
Management and monitoring/Централизованное управление и мониторинг
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
Error/Ошибка
Warning/Предупреждение
Debug/Отладочное сообщение
License policy error/Нарушение лицензионной политики
Computer blocked/Компьютер заблокирован
Computer unblocked/Компьютер разблокирован

Группа событий "Системные сервисы"

System services group msg/Группа событий системных сервисов
Event log service is started/Старт службы регистрации
Event log service is stopped/Остановка службы регистрации
Event writing error/Ошибка записи в журнал
Event log cleared/Очистка (ротация) журнала аудита

Группа событий "Подсистема аудита"

Audit group msg/Группа событий подсистемы аудита

Группа событий "Аутентификация и идентификация"

Authentication group msg/Группа событий аутентификации
Authentication error/Ошибка аутентификации
User blocked/Запрет входа пользователя
Sudo/Выполнение задания от имени другого пользователя
User login/Вход пользователя
User logout/Завершение работы 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
Resource integrity checked/Завершение проверки целостности объекта
Error in Integrity database/Ошибка открытия БД КЦ
Create integrity database/Создание БД КЦ
Refresh integrity database/Обновление 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 "Тестирование"

Testing group msg/Группа сообщений тестирования

Группа событий "Самодиагностика"

Self-testing group msg/Группа сообщений самодиагностики

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 "Резервное копирование"

Backup group msg/Группа сообщений резервного копирования
The data is recovered/Данные восстановлены
Error recovering data/Ошибка восстановления данных
The data is recovered/Данные сохранены
Error saving data/Ошибка сохранения данных

Группа событий "ПАК Соболь"

Hardware Trusted Boot: User logon/Соболь: Вход пользователя

Hardware Trusted Boot: Operating mode changed/Соболь: Изменение режима работы
Hardware Trusted Boot: Log has been cleared/Соболь: Очистка журнала
Hardware Trusted Boot: Parameter synchronization error/Соболь: Ошибка синхронизации параметров
Hardware Trusted Boot:Checksum recalculation/Соболь: Перерасчет контрольных сумм
Hardware Trusted Boot: Authenticator has been changed/Соболь:Смена аутентификатора
Hardware Trusted Boot:User logon prohibited/Соболь: Запрет входа пользователя
Hardware Trusted Boot:Resource integrity violation/Соболь: Нарушена целостность ресурса
Hardware Trusted Boot:Synchronization of parameters/Соболь: Синхронизация параметров
Hardware Trusted Boot:Password changed/Соболь: Смена пароля
Hardware Trusted Boot:Electronic lock enabled/Соболь: Включен режим совместной работы
Hardware Trusted Boot:Error enabling electronic lock/Соболь: Ошибка при включении режима совместной работы
Hardware Trusted Boot:Electronic lock disabled/Соболь: Выключен режим совместной работы
Hardware Trusted Boot: Error disabling electronic lock/Соболь: Ошибка при выключении режима совместной работы
Hardware Trusted Boot: CRC error in identifier memory/Соболь: Ошибка КС в памяти идентификатора
Hardware Trusted Boot: Boot disk settings have been changed/Соболь: Изменены параметры загрузочного диска
Hardware Trusted Boot: checksums not calculated/Соболь: Не рассчитаны контрольные суммы
Hardware Trusted Boot: automatic checksum re-calculation/Соболь: Автоматический перерасчет контрольных сумм
Hardware Trusted Boot: manual checksum re-calculation/Соболь: Ручной перерасчет контрольных сумм
Hardware Trusted Boot: error deleting all users/Соболь: Ошибка при удалении всех пользователей
Hardware Trusted Boot: Log export completed/Соболь: Экспорт журнала завершен
Hardware Trusted Boot: Password setting time is in the future/Соболь: Время установки пароля опережает системное
Hardware Trusted Boot: System clock changed/Соболь: Изменено системное время и дата
Hardware Trusted Boot: System clock setting back detected/Соболь: Обнаружен перевод системных часов назад
Hardware Trusted Boot: Last logon time adjusted/Соболь: Скорректировано время последнего входа
Hardware Trusted Boot: Log export failed/Соболь: Ошибка при экспорте журнала
Hardware Trusted Boot: Delete all users/Соболь: Удаление всех пользователей

Группа событий "КЦ ПАК Соболь"

sable: Sobol integrity check group msg/Группа сообщений управления контролем целостности ПАК "Соболь"
sable: Add a object to integrity check/Установка объекта на контроль целостности в ПАК "Соболь"
sable: Error on object integrity check addition/Ошибка добавления/обновления ресурса к контролю в ПАК "Соболь"

sable: Remove object from integrity check/Снятие объекта с контроля целостности в ПАК "Соболь"
sable: Error while disabling integrity check for object/Ошибка снятия объекта с контроля целостности в ПАК "Соболь"
sable: Sobol integrity check templates were changed/Изменение шаблонов контроля целостности ПАК "Соболь"
sable: Integrity check was enabled for object list from file <Название файла>. Successfully processed objects: <Число успехов>. Processing errors: <Число ошибок>/Список объектов из файла <Название файла> поставлен на контроль. Успешно обработано <Число успехов> объектов. Ошибок при постановке объектов: <Число ошибок>
sable: Error while enabling integrity check for object list from file <Название файла>/Ошибка при постановке списка объектов из файла <Название файла>
sable: Integrity check was disabled for object list from file <Название файла>. Successfully processed objects: <Число успехов>. Processing errors: <Число ошибок>/Снят с контроля список объектов из файла <Название файла>. Успешно обработано <Число успехов> объектов. Ошибок при снятии объектов: <Число ошибок>
sable: Error while disabling integrity check for object list from file <Название файла>/Ошибка при снятии с контроля списка объектов из файла <Название файла>
sable: Integrity check was enabled for object list. Successfully processed objects: <Число успехов>. Processing errors: <Число ошибок>/Список объектов поставлен на контроль. Успешно обработано <Число успехов> объектов. Ошибок при постановке объектов: <Число ошибок>
sable: Error while enabling integrity check for object list/Ошибка при постановке списка объектов

Группа событий "Управление ЗПС"

Enabling a AEC rule/Включение правила ЗПС
Disabling a AEC rule/Выключение правила ЗПС
Adding an account to a AEC rule/Добавление учетной записи к правилу ЗПС
Deleting an account from a AEC rule/Удаление учетной записи из правила ЗПС
Creating a AEC rule/Создание правила ЗПС
Deleting a AEC rule/Удаление правила ЗПС
Changing a AEC rule/Изменение правила ЗПС
Changing resources of a AEC rule/Изменение ресурсов правила ЗПС
An error occures during calculation of the resource reference values/Ошибка при расчете эталона ресурсов
Recalculation of the resource reference values completed/Выполнен перерасчет эталона ресурсов

Группа событий "Управление межсетевым экраном"

Firewall management group msg/Группа сообщений управления межсетевым экраном

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 blocked/Пользователь заблокирован
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 управления резервным копированием

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 событий "Централизованное управление и мониторинг"

Management and monitoring group msg/Группа сообщений централизованного управления и мониторинга

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

Неизвестно
Чтение файла/каталога
Получение информации
Запись файла
Изменение атрибутов
Переименование
Удаление
Создание
Открытие сетевого соединения
Запуск приложения
Открытие файла на чтение
Открытие файла/каталога на запись
Запуск программы
Запрет запуска программы
Загрузка библиотеки
Запрет загрузки библиотеки
Открытие файла
Запрет открытия файла
Прием/передача датаграмм
Установление соединения
Добавление устройства
Удаление устройства
Монтирование устройства
Чтение с устройства
Запись на устройство
Срабатывание правила межсетевого экрана

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.

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 возникает ошибка при запуске, функциональный контроль регистрирует ошибку с описанием проблемы. 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 выключить блокировку системы при нарушении КЦ и оставить только регистрацию события в системном журнале. Для этого администратор должен ввести в командную строку:

```
snpolctl -p system -c system,system_lock,0
```

Для включения блокировки необходимо заменить 0 на 1.

Администратор может вручную запустить процедуру функционального контроля, используя утилиту **snfc**.

Запуск утилиты осуществляется в режиме командной строки командой #/opt/secretnet/sbin/snfc. В таблице ниже 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
-t	--test	Полная проверка целостности компонентов Secret Net LSP и сервисов

Замена файла лицензии демонстрационной версии

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

Для замены файла лицензии из консоли:

1. Запустите программу эмулятора терминала и проверьте вид используемой лицензии командой:

   ```
   #/opt/secretnet/bin/snlicensectl -s [--status]
   ```

   Если используется демонстрационная версия, то для каждого компонента в списке будет указано значение "Демонстрационный режим".

2. Замените файл лицензии командой:

   ```
   #/opt/secretnet/bin/snlicensectl -c [--change] <путь и имя файла лицензии>
   ```

   Если был задан неверный файл лицензии, на экране появится сообщение "Ошибка при установке новой лицензии".

3. Выполните проверку установленной лицензии командой:

```
#/opt/secretnet/bin/snlicensectl -s [--status]
```

При правильной установке и успешной активации лицензии на экране будет отображен список компонентов защиты без значения "Демонстрационный режим".

Удаленное управление

Secret Net LSP может функционировать совместно с СЗИ Secret Net Studio (версии 8.6, 8.8). Эти СЗИ в режиме совместного функционирования позволяют 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.

Внимание!

- Для совместного функционирования Secret Net LSP с СЗИ Secret Net Studio (версии 8.6, 8.8) необходимо включить данный компьютер в домен, связанный с нужным сервером безопасности.
- Компьютер должен быть включен в домен и подчинен серверу безопасности в структуре управления.

Включение и выключение режима удаленного управления

Пояснение.

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

Для включения/выключения режима удаленного управления введите в командную строку:

```
snpolctl -c snnetwork 1
snpolctl -c snnetwork 0
```

Включение компьютера в домен Windows

Включение в домен Windows выполняется средствами ОС администратором системы, обладающим правами суперпользователя компьютера. Пакеты, необходимые для ввода компьютера в домен, исключены из зависимостей пакета Secret Net LSP и не устанавливаются при его установке.

Внимание!

Включение компьютера в домен рекомендуется выполнять после установки ПО СЗИ Secret Net LSP. В случае если компьютер был включен в домен Windows до установки ПО СЗИ Secret Net LSP, необходимо выполнить проверку конфигурационных файлов на соответствие приведенной ниже инструкции.

Процедура включения компьютера в домен осуществляется штатными средствами операционных систем. Так, для ОС семейства ALT Linux включение в домен осуществляется с помощью сервиса **The System Security Services Daemon (SSSD)** (см. стр. **72**) а для всех остальных ОС обеспечение корректной работы сетевого взаимодействия достигается с помощью пакета программ **Samba** (см. стр.**69**) или **SSSD**.

Примечание.

Управление службами, отвечающими за сетевое взаимодействие с доменом, осуществляется средствами ОС. За корректное функционирование сервиса **SSSD** и пакета программ **Samba** отвечает администратор системы.

Для включения компьютера в домен Windows:

Процедура включения в домен компьютера под управлением операционной системы, отличной от ОС семейства ALT Linux, осуществляется штатными средствами ОС с помощью пакета программ **Samba** или **SSSD**.

Примечание.
Процедура, описанная ниже, представлена на примере включения компьютера в домен **SECRET.LOC**.

1. Укажите IP-адрес DNS-сервера домена в параметрах сетевого подключения или в файле конфигурации (первая запись nameserver в **/etc/resolv.conf**) в качестве первичного DNS (например, nameserver 192.168.10.10).
2. Измените имя компьютера. Для этого отредактируйте файлы конфигурации **/etc/hosts** и **/etc/hostname** следующим образом:
   - в файле конфигурации **/etc/hosts** необходимо добавить строку следующего формата:

     ```
     127.0.0.1 ИМЯ_КОМПЬЮТЕРА.ДОМЕН ИМЯ_КОМПЬЮТЕРА
     ```

   - в файле конфигурации **/etc/hostname** необходимо указать имя компьютера, включаемого в домен.
3. Выполните настройку синхронизации времени, указав сервер точного времени. Для этого в зависимости от используемой ОС добавьте в файлы конфигурации **chrony.conf** или **ntp.conf** строку с указанием сервера синхронизации времени (например, server dc1.secret.loc).
4. Выполните настройку авторизации через сетевой протокол аутентификации **Kerberos**. Для этого отредактируйте файл конфигурации **/etc/krb5.conf** следующим образом:

   ```
   [libdefaults]
   default_realm = SECRET.LOC

   [realms]
   SECRET.LOC = {
   kdc = dc1.secret.loc
   admin_server = dc1.secret.loc
   }

   [domain_realm]
   secret.loc = SECRET.LOC
   .secret.loc = SECRET.LOC
   ```

   Внимание!
   Для ОС ubuntu при настройке параметров пакета программ **samba** не нужно устанавливать пакет **libpam-krb5** и настройка **krb5.conf** не нужна.
5. Выполните настройку пакета программ **Samba** для включения компьютера в домен. Для этого укажите необходимые настройки в файле конфигурации **/etc/samba/smb.conf**. Ниже представлен пример настроек в файле конфигурации:

```
[global]
    workgroup = SECRET
    security = ADS
    printing = cups
    printcap name = cups
    load printers = yes
    cups options = raw
    realm = SECRET.LOC
    idmap config *: backend = tdb
    idmap config *: range = 10000-50000
    idmap config SECRET: backend = rid
    idmap config SECRET: range = 50001-99999
    template shell = /bin/bash
    wins support = no
    idmap cache time = 900
    winbind offline logon = yes
    template homedir = /home/%D/%U
    winbind use default domain = no
    winbind cache time = 300
    winbind enum users = yes
    winbind enum groups = yes
    winbind refresh tickets = yes
    nt pipe support = no
```

Примечание.

В зависимости от используемой ОС при настройке параметров пакета программ **Samba** для осуществления входа в домен вместо параметров **yes/no** могут использоваться параметры **true/false**. Для получения подробной информации об особенностях обеспечения корректной работы сетевого взаимодействия с помощью пакета программ **Samba** обратитесь к документации **Samba** для ОС, под управлением которой осуществляется включение компьютера в домен.

Внимание!

Для ОС Ubuntu при настройке параметров пакета программ **samba** нужно указать необходимые настройки в файле конфигурации **/etc/ssl/openssl.conf**:

```
[default_conf]
    ssl_conf = ssl_sect

    [ssl_sect]

    system_default = ssl_default_sect

    [ssl_default_sect]
    MinProtocol = TLSv1.2
    CipherString = DEFAULT:@SECLEVEL=1
```

6. Для всех DEB-систем при использовании сервиса **The System Security Services Daemon (SSSD)** необходимо указать необходимые настройки в конфигурации. Ниже представлен пример настроек в конфигурации:
   - Замените **sufficient** в секции **password** и **password-initial** файла конфигурации **/usr/share/pam- configs/sss** на [success=end default=ignore] и выполните 'pam-auth-update --package'
   - В файле конфигурации **/etc/sssd/sssd.conf** в секцию **[domain/SECRET.LOC]** добавьте следующие строки:

```
enumerate = true
cache_credentials = true
use_fully_qualified_names = true
full_name_format = %1$s@%2$s
```

Примечание.
Строку full_name_format с форматом через '@' нужно вводить для всех ОС, кроме Alt linux, либо эту строку можно не вводить. Для Alt linux нужно вводить в формате с '\', например: full_name_format = %2$s\%1$s

7. Выполните настройку диспетчера службы имен. Для этого в файле конфигурации **/etc/nsswitch.conf** отредактируйте строки **passwd** и **group** следующим образом:

```
passwd:  files winbind system
group:   files winbind system
```

При использовании сервиса **The System Security Services Daemon (SSSD)**:

```
passwd: files sss
group: files sss
```

8. С помощью стандартной утилиты **ping** выполните проверку корректной работы DNS-сервера и убедитесь в доступности контроллера домена по IP-адресу и по имени домена FQDN.
9. Выполните проверку конфигурации на отсутствие ошибок. Для этого в программе эмулятора терминала выполните команду:

```
#testparm
```

10. В случае отсутствия ошибок выполните проверку авторизации в домене:
    - очистите кеш пользовательских сессий. Для этого в программе эмулятора терминала выполните команду:

      ```
      #kdestroy
      ```

    - получите билет для доменного пользователя. Для этого в программе эмулятора терминала выполните команду:

      ```
      #kinit administrator@SECRET.LOC
      ```

    - в случае отсутствия ошибок выполните просмотр билета для доменного пользователя. Для этого в программе эмулятора терминала выполните команду:

      ```
      #klist
      ```

      Ниже представлен пример результата выполнения команды **#klist**:

      ```
      Ticket cache: FILE:/tmp/krb5cc_0
      Default principal: administrator@SECNET.LOC
      Valid starting Expires Service principal
      01/14/15 16:13:05 01/15/15 02:13:14
      krbtgt/SECRET.LOC@SECRET.LOC
      renew until 01/15/15 16:13:05
      Kerberos 4 ticket cache: /tmp/tkt0
      ```

11. Выполните включение компьютера в домен Windows. Процесс включения в домен различен в зависимости от ОС. Процессы описаны далее в документе.
12. После настройки параметров и изменения конфигурационных файлов выполните перезапуск сервисов, для которых были отредактированы конфигурационные файлы, либо выполните перезагрузку ОС.

Примечание.
Для обеспечения постоянной работы служб для них необходимо настроить автозапуск.

После завершения процедуры настройки параметров и изменения конфигурационных файлов убедитесь в том, что в системе обеспечивается корректное отображение доменных пользователей и групп. Для этого выполните команды:

```
#getent passwd
#getent group
```

или

```
#wbinfo -u
#wbinfo -g
```

Для компьютеров под управлением ОС семейства ALT Linux:

Процедура включения компьютера под управлением ОС семейства ALT Linux в домен осуществляется штатными средствами ОС с помощью сервиса **The System Security Services Daemon (SSSD)**. Для ввода компьютера в Active Directory потребуется установить пакет **task-auth-ad-sssd** и все его зависимости.

1. Вызовите меню включения компьютера в домен:
   - Перейдите в меню "Система".
   - Выберите раздел "Администрирование".
   - Выберите раздел "Центр управления системой".
   - Введите пароль администратора безопасности и нажмите кнопку "Режим эксперта".
   - В Центре управления системой в разделе "Пользователи" выберите "Аутентификация".
   - Выберите "Домен Active Directory".
   - В появившемся окне "Домен Active Directory" заполните поля "Домен" и "Имя компьютера" (например, Домен: SECRET.LOC, Имя компьютера: CLIENTVM).
   - Для сохранения настроек нажмите кнопку "Применить" и введите логин и пароль администратора домена.
2. Выполните настройку авторизации через сетевой протокол аутентификации **Kerberos**. Для этого отредактируйте файл конфигурации **/etc/krb5.conf** следующим образом:

```
[libdefaults]
default_realm = SECRET.LOC

[realms]
SECRET.LOC = {
kdc = dc1.secret.loc
admin_server = dc1.secret.loc
}

[domain_realm]
secret.loc = SECRET.LOC
.secret.loc = SECRET.LOC
```

3. Выполните настройку экранного менеджера **LightDM** для отображения пользователей при входе в систему. Для этого в файле конфигурации **/etc/lightdm/lightdm.conf** отредактируйте строку **greeter-hide-users** следующим образом:

```
greeter-hide-users = true
```

4. Выполните настройку сервиса **The System Security Services Daemon (SSSD)**. Для этого в файле конфигурации **/etc/sssd/sssd.conf** в секцию **[domain/SECRET.LOC]** добавьте следующие строки:

```
enumerate = true
cache_credentials = true
use_fully_qualified_names = true
full_name_format = %2$s\%1$s
```

5. После настройки параметров и изменения конфигурационных файлов выполните перезапуск сервиса **The System Security Services Daemon (SSSD)**. Для этого в программе эмулятора терминала выполните команду:

```
#systemctl restart sssd
```

После завершения процедуры настройки параметров и изменения конфигурационных файлов убедитесь в том, что в системе обеспечивается корректное отображение доменных пользователей и групп в формате DOMAIN\username. Для этого выполните команды:

```
#getent passwd
#getent group
```

Для компьютеров под управлением ОС семейства Astra Linux:

В Astra Linux присутствует графическая утилита для ввода компьютера в домен Active Directory.

Для ввода средствами winbind – это fly-admin-ad-client.

Для ввода средствами SSSD – это fly-admin-ad-sssd-client.

Для подключения к домену используется пакет fly-admin-ad-sssd-client или fly-admin-ad-client, который может быть установлен с помощью графического менеджера пакетов или из командной строки командой:

```
# sudo apt install astra-ad-sssd-client
```

или

```
# sudo apt install astra-ad-client
```

Для подключения к домену Windows AD выполните команду с указанием имени домена, к которому нужно подключиться, и имени администратора этого домена:

```
# sudo astra-ad-sssd-client -d <домен> -u <администратор>
```

или

```
# sudo astra-ad-client -d <домен> -u <администратор>
```

Проверить статус подключения можно командой:

```
#sudo astra-ad-sssd-client –i
```

Для удаления компьютера из домена (удаление механизма авторизации) используйте команду:

```
#sudo astra-ad-sssd-client –U
```

Для компьютеров под управлением ОС семейств Ubuntu:

В ОС Ubuntu ввод в домен происходит через стандартные средства системы.

Для **Winbind**:

Необходимо установить зависимости:

```
# sudo apt update
# sudo apt-get install krb5-user samba winbind libpam-krb5
libpam-winbind libnss-winbind
```

И ввести в домен:

```
# sudo net ads join -U username -D MYDOMAIN
```

Для **SSSD**:

Необходимо установить зависимости:

```
# sudo apt update
# sudo apt -y install realmd libnss-sss libpam-sss sssd sssd-tools adcli samba-common-bin oddjob oddjob-mkhomedir packagekit
```

И ввести в домен:

```
# sudo realm join -U Administrator example.com
```

Настройка удаленного управления

Для настройки удаленного управления используется утилита **snnetctl**. Описание утилиты и особенности ее применения приведены на стр.**55**.

Глава 4
Персональный межсетевой экран

Персональный межсетевой экран представляет собой компонент СЗИ Secret Net LSP , предназначенный для защиты серверов и рабочих станций от несанкционированного доступа и разграничения сетевого доступа в информационных системах.

Ниже представлены основные функции персонального межсетевого экрана:

- фильтрация с независимым принятием решений по каждому пакету;
- фильтрация пакетов служебных протоколов, необходимых для диагностики и управления работой сетевых устройств;
- фильтрация на транспортном уровне запросов к прикладным сервисам;
- фильтрация на уровне параметров протоколов стека TCP/IP;
- фильтрация на уровне пользователей или групп пользователей;
- фильтрация на уровне параметров прикладных протоколов;
- фильтрация на уровне исполняемого файла/процесса;
- фильтрация входящих соединений с использованием данных отправителя пакетов;
- фильтрация с учетом расписания;
- оповещение пользователя при срабатывании правила.

Процедуры, связанные с установкой или удалением модуля ПМЭ, выполняются отдельно от основного пакета ПО Secret Net LSP (подробнее см. стр. **29** , стр.**31**).

Персональный межсетевой экран является локальным компонентом СЗИ Secret Net LSP. Процедуры, связанные с управлением механизмом персонального межсетевого экранирования, описанные далее в этой главе, выполняются локально на пользовательском компьютере в режиме командной строки и не предполагают возможности удаленного управления посредством сервера безопасности СЗИ Secret Net 8 (пакет обновлений 8).

Для выполнения процедур настройки ПМЭ используется утилита **fw-localcfg**. Описание утилиты и особенности ее применения приведены на стр.**79**.

Внимание!
При нехватке объема оперативной памяти, необходимого для функционирования ПМЭ, защищаемый компьютер будет заблокирован.

Регистрация лицензии на механизм ПМЭ

Процедура регистрации лицензии ПМЭ аналогична процедурам регистрации лицензий на другие механизмы защиты Secret Net LSP.

Примечание.
Персональный межсетевой экран является отдельным компонентом ПО СЗИ Secret Net LSP и не входит в состав основной лицензии защитных подсистем. Для активации модуля защиты ПМЭ предусмотрена регистрация соответствующей дополнительной лицензии.

Контроль целостности подсистемы межсетевого экранирования

Механизм контроля целостности ПМЭ предназначен для обеспечения контроля за неизменностью содержимого ресурсов подсистемы межсетевого экранирования.

Примечание.
Механизм КЦ подсистемы межсетевого экранирования не связан с контролем целостности объектов файловой системы Secret Net LSP, поскольку механизм ПМЭ представляет собой отдельный модуль ПО СЗИ Secret Net LSP с заданными параметрами, настройка которых администратором безопасности не предусмотрена.

Контроль целостности ресурсов подсистемы межсетевого экранирования осуществляется на основании сравнения текущих значений контролируемых параметров проверяемых ресурсов с эталонными значениями контролируемых параметров, которые рассчитываются при первоначальной установке подсистемы межсетевого экранирования.
Контроль целостности ресурсов подсистемы межсетевого экранирования осуществляется в автоматическом режиме при загрузке операционной системы.

Постановка ресурсов подсистемы МЭ на контроль

Процедура постановки ресурсов подсистемы межсетевого экранирования на контроль осуществляется автоматически без участия администратора.

Настройка механизма КЦ подсистемы межсетевого экранирования

Настройка механизма КЦ подсистемы МЭ может осуществляться администратором безопасности, обладающим правами суперпользователя компьютера, в процессе установки подсистемы МЭ на защищаемый компьютер.

Настройка механизма КЦ подсистемы МЭ включает:

- добавление в базу данных информации о контролируемых объектах;
- расчет контрольных сумм для компонентов и процессов подсистемы;
- настройку реакции системы на нарушение КЦ объектов;
- определение перечня регистрируемых событий КЦ.

Список объектов КЦ подсистемы МЭ, а также реакция системы на нарушение КЦ защищаемых объектов задаются в конфигурационном файле **/opt/snlsp-firewall/etc/fwfc.conf**.

Объектами КЦ подсистемы межсетевого экранирования являются:

- компоненты подсистемы МЭ (файлы и каталоги);
- процессы подсистемы МЭ (осуществляется контроль работы процесса **fw-collector**).

Примечание.
Если при осуществлении контроля работы процесс **fw-collector** не отвечает в течение 20 секунд, осуществляется перезапуск подсистемы МЭ с последующим ожиданием ответа процесса. Если в течение последующих 20 секунд ответа процесса не последовало, процедура повторяется. В случае повторного неудачного результата осуществляется блокировка компьютера.

Контроль целостности компонентов подсистемы МЭ осуществляется на основании параметров, указанных в конфигурационном файле **/opt/snlsp-firewall/etc/fwfc.conf**.

Регистрация событий механизма КЦ подсистемы МЭ

Объект КЦ подсистемы МЭ считается целостным, если каждый из фиксируемых параметров объекта соответствует эталонным значениям базы данных механизма КЦ.

Если в процессе контроля целостности ресурсов подсистемы МЭ обнаруживается несоответствие текущих значений контролируемых параметров проверяемых ресурсов с их эталонными значениями, система осуществляет оповещение администратора безопасности о нарушении целостности ресурсов подсистемы и выполняет предписанное при настройке действие (например, осуществляется блокировка входа пользователя в систему). Факт нарушения КЦ фиксируется отдельно для каждого объекта. Возможные варианты реакции ПО СЗИ Secret Net LSP на факт нарушения КЦ объектов подсистемы МЭ представлены в конфигурационном файле **/opt/snlsp-firewall/etc/fwfc.conf**.

События, связанные с работой механизма КЦ подсистемы межсетевого экранирования (в том числе — с действиями администратора), регистрируются в "Журнале событий".

Восстановление объекта подсистемы МЭ из эталонного значения

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

- для объекта определено восстановление в настройках подсистемы КЦ;
- обнаружено нарушение целостности данного объекта;
- существует эталонная копия объекта, которая была сохранена ранее при его постановке на контроль.

Настройка КЦ объектов, поставленных на контроль

Настройка контроля целостности компонентов подсистемы МЭ, поставленных на контроль при установке подсистемы межсетевого экранирования, не требуется. Однако в Secret Net LSP предусмотрена возможность ручной настройки КЦ объектов, поставленных на контроль. Для этого необходимо в конфигурационный файл **/opt/snlsp-firewall/etc/fwfc.conf** внести следующие изменения:

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

Общий порядок настройки

Настройка персонального межсетевого экрана выполняется в следующем порядке:

1. Получение информации о работоспособности механизма (см. стр.**77**).
2. Вывод справочной информации о применении утилиты настройки ПМЭ (см. стр.**86**).
3. Настройка персонального межсетевого экрана на основе правил (см. стр.**86**).
4. Настройка регистрации событий ПМЭ (см. стр.**92**).
5. Проведение аудита событий ПМЭ (см. стр.**93**).

Примечание.
Настройка и управление персональным межсетевым экраном Secret Net LSP осуществляется администратором, обладающим правами суперпользователя компьютера.

Управление персональным межсетевым экраном

В рамках управления персональным межсетевым экраном администратор имеет возможность получения текущего статуса его работоспособности, перезагрузки, отключения и обратного включения ПМЭ.

Основные процедуры, связанные с управлением персональным межсетевым экраном и описанные далее, выполняются в режиме командной строки. Для выполнения процедур используются политики Secret Net LSP.

Получение текущего статуса работоспособности ПМЭ

Запустите программу эмулятора терминала и выполните команду:

```
systemctl status snlsp-firewall
```

Перезагрузка ПМЭ

Запустите программу эмулятора терминала и через политику Secret Net LSP выполните команду:

```
systemctl restart snlsp-firewall
```

Отключение ПМЭ при загрузке системы

Для отключения запуска ПМЭ при загрузке системы необходимо отключить политику Secret Net LSP.

Включение ПМЭ при загрузке системы

Для включения запуска ПМЭ при загрузке системы необходимо включить политику Secret Net LSP.

Совместное функционирование ПМЭ со специализированным ПО

ПО СЗИ Secret Net LSP предусматривает возможность совместного функционирования модуля ПМЭ с программным обеспечением Dr.Web Enterprise Security Suite (версия 11).

При установленных ПО СЗИ Secret Net LSP и ПМЭ:

1. Остановите работу ПМЭ Secret Net LSP с помощью команды:

```
/opt/secretnet/bin/snpolctl -p firewall -c
firewall,state,0
```

2. Выполните установку пакета ПО Dr.Web Enterprise Security Suite на защищаемый компьютер.
3. Выполните настройку совместного функционирования ПО СЗИ Secret Net LSP и модуля ПМЭ с ПО Dr.Web Enterprise Security Suite. Для этого внесите соответствующие изменения в настройки ПО Dr.Web Enterprise Security Suite с помощью команды:

```
drweb-ctl cfset LinuxFirewall.OutputDivertNfqueueNumber 1
```

Примечание.
Команду **drweb-ctl cfset LinuxFirewall.OutputDivertNfqueueNumber 1** необходимо выполнить на этапе установки на защищаемый компьютер ПО Dr.Web Enterprise Security Suite до ввода лицензии и запуска основных служб программного обеспечения.

4. Выполните запуск ПМЭ Secret Net LSP после приостановления его работы с помощью команды:

```
/opt/secretnet/bin/snpolctl -p firewall -c
firewall,state,1
```

5. Завершите установку пакета ПО Dr.Web Enterprise Security Suite.

При неустановленных ПО СЗИ Secret Net LSP и ПМЭ:

1. Выполните настройку совместного функционирования ПО СЗИ Secret Net LSP и модуля ПМЭ с ПО Dr.Web Enterprise Security Suite. Для этого внесите соответствующие изменения в настройки ПО Dr.Web Enterprise Security Suite с помощью команды:

```
drweb-ctl cfset LinuxFirewall.OutputDivertNfqueueNumber 1
```

2. Перезагрузите компьютер.
3. Выполните установку ПО СЗИ Secret Net LSP и модуля ПМЭ.

В случае если описанные выше процедуры не были в полной мере соблюдены, после перезагрузки компьютера вход в систему может быть заблокирован.

При блокировке входа в систему:

1. Разблокирование входа может выполнить только администратор. Для этого необходимо выполнить команду:

```
/opt/secretnet/sbin/snunblock
```

2. Выполните настройку совместного функционирования ПО СЗИ Secret Net LSP и модуля ПМЭ с ПО Dr.Web Enterprise Security Suite. Для этого внесите

соответствующие изменения в настройки ПО Dr.Web Enterprise Security Suite с помощью команды:

```
drweb-ctl cfset LinuxFirewall.OutputDivertNfqueueNumber 1
```

3. Выполните перезапуск ПМЭ Secret Net LSP с помощью команды:

```
systemctl restart snlsp-firewall
```

4. Перезагрузите компьютер.

Утилиты Secret Net LSP для работы с ПМЭ

Для выполнения настройки персонального межсетевого экрана (см. стр.**86**) используется утилита **fw-localcfg**. Утилита выполняет действия в режиме командной строки от имени суперпользователя компьютера. Строка команды имеет следующий формат:

```
fw-localcfg [<аргумент>] [<команда> [<параметр>]] ...
[<команда> [<параметр>]]
```

Примечание.
При работе с правилами ПМЭ в программе эмулятора терминала необходимо соблюдать следующую последовательность вводимых команд: [название утилиты] [<команда>] ... [<параметр=значение>].

Описание общего аргумента представлено в следующей таблице:

Команда	Описание
––help	Выводит справочную информацию о применении утилиты

Пример команды:

fw-localcfg --help	Выполняется вывод справочной информации о применении утилиты

Описание команд и параметров представлено в таблицах ниже.

Примечание.
При создании правил настройки ПМЭ Secret Net LSP необходимо включать в состав правил обязательный набор следующих параметров: --action, --protocol, --msg.

Команды add и modify

Команда add добавляет новые правила настройки межсетевого экрана.

Команда modify изменяет существующие правила настройки межсетевого экрана.

Для команд add и modify предусмотрены следующие параметры:

Параметр	Описание
--action=<action>	Добавление операции, выполняемой при фильтрации сетевых пакетов, для которых действует правило. Допустимые значения параметра --action: • pass — пропустить сетевой пакет; • drop — отбросить сетевой пакет

Параметр	Описание
--protocol=<protocol>	Добавление типа сетевых протоколов, на основании которых осуществляется фильтрация сетевых пакетов. Допустимые значения параметра --proto: • tcp; udp; ip; ftp; tls; dns; dcerpc; ssh; imap; modbus; dnp3; enip; nfs; ikev2; krb5; ntp; dhcp; rfb; snmp; tftp; sip; egp; hmp; xns-idp; rdp; rvd; http2; smb; http; • icmp — фильтрация сетевых пакетов осуществляется на основании любого протокола, инкапсулируемого в протокол IP с указанием его номера в качестве значения параметра. Например, протокол TCP может быть представлен как --proto=6; • any — фильтрация сетевых пакетов осуществляется на основании всех IP-протоколов
--msg=<message>	Добавление текстового сообщения. Значение параметра --msg необходимо указывать в кавычках. Например, --msg='Drop packet!'
--alarm=<boolValue>	Оповещение пользователя. Оповещение пользователя по умолчанию отключено. Оповещение срабатывает только при добавлении правила МСЭ со значением --alarm=true. При срабатывании выводится информация об id правила, дате и времени срабатывания, а также текстовое сообщение, указанное в правиле
--order=<order>	Добавление последовательности обработки правил. С помощью параметра --order осуществляется настройка управления приоритетом правила. Чем ниже значение, тем выше приоритет
--enable=<boolValue>	Включение и отключение правила. Допустимые логические значения параметра --enable: • true — правило включено (значение по умолчанию); • false — правило отключено
--audit=<boolValue>	Управление регистрацией событий в журнале, возникающих при срабатывании правила. Допустимые логические значения параметра --audit: • true — регистрация событий включена; • false — регистрация событий выключена (значение по умолчанию)
--icmp_type=<type>	Добавление фильтрации с учетом типа пакета ICMP. Допустимые значения параметра --icmp_type: 0-255, *. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех типов пакетов ICMP. Параметр --icmp_type применяется только с указанием параметра --proto=icmp
--icmp_code=<code>	Добавление фильтрации с учетом кода пакета ICMP. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех кодов пакетов ICMP. Параметр --icmp_code применяется только с указанием параметра --proto=icmp

Параметр	Описание
--local_addrs=<IP, IPsubnet/MASK, IP1-IP2, IP3,..., IPn>	Добавление IP-адресов отправителей. В качестве значения параметра --local_addrs укажите IP-адрес компьютера и маску подсети, чтобы задать допустимый набор локальных IP-адресов. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех локальных IP-адресов. При вводе нескольких номеров адресов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "–" (дефис)
--local_ports=<p1-p2, p3,..., pN>	Добавление портов отправителя сетевых пакетов. Параметр включает список локальных портов или диапазонов портов, для которых действует правило. В качестве значения параметра --local_ports укажите номера портов в диапазоне от 0 до 65535. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех локальных портов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "–" (дефис). Параметр --local_ports применяется только для формирования правил фильтрации сетевого потока
--remote_addrs=<IP, IPsubnet/MASK, IP1-IP2, IP3,..., IPn>	Добавление IP-адресов получателей. В качестве значения параметра --remote_addrs укажите IP-адрес компьютера и маску подсети, чтобы правило действовало для всех удаленных IP-адресов. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех удаленных IP-адресов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "–" (дефис)
--remote_ports=<p1-p2, p3,..., pN>	Добавление портов получателя сетевых пакетов. Параметр включает список удаленных портов или диапазонов портов, для которых действует правило. В качестве значения параметра --remote_ports укажите номера портов в диапазоне от 0 до 65535. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы правило действовало для всех удаленных портов. При вводе нескольких номеров портов разделяйте их символом "," (запятая). Для задания диапазона портов используйте символ "–" (дефис). Параметр --remote_ports применяется только для формирования правил фильтрации сетевого потока

Параметр	Описание
--schedule=<strValue>	Добавление фильтрации сетевого трафика с учетом расписания. Строковые значения параметра --schedule имеют следующий формат: <hour_range> <day_range> <action> [# ...] • <hour_range> — диапазон часов; • <day_range> — диапазон дней; • <action> — символ "+" включает правило, символ "-" отключает правило. Для задания диапазона часов или дней используйте символ "-" (дефис). Для задания всех возможных часов или дней используйте символ * (звездочка). При вводе нескольких групп значений <hour_range> <day_range> <action> разделяйте их символом "#" (решетка)
--exefile=<strValue>	Добавление исполняемого файла с указанием имени, для которого действует правило. Для параметра --exefile предусмотрены строковые значения. Символ * (звездочка) является значением по умолчанию для параметра. Оставьте символ * (звездочка), если требуется, чтобы осуществлялся контроль всех исполняемых файлов
--subjects=<strValue>	Определяет список пользователей и групп пользователей
--objects=<strValue>	Определяет папки общего доступа и именованные каналы. Используется только для протокола 'smb'
--substr=<boolValue>	Выделение подстрокового значения параметра --exefile. Допустимые логические значения параметра --substr: • true — значение параметра --exefile является подстроковым; • false — значение параметра --exefile не является подстроковым (значение по умолчанию). Параметр --substr применяется совместно с параметром --exefile
--content=<strValue>	Добавление маски фильтра сетевого трафика на основе прямого соответствия содержимому сетевого пакета. Введите строковое значение, определяющее необходимость обработки IP-пакета. Правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. По умолчанию параметр --content имеет пустое значение
--wildcard=<strValue>	Добавление маски фильтра сетевого трафика на основе специальных символов. Введите значение, определяющее необходимость обработки IP-пакета. Правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. Допустимые строковые значения параметра --wildcard: • * — любое количество символов; • ? — один символ. По умолчанию параметр --wildcard имеет пустое значение. Параметр применяется только для формирования правил фильтрации сетевого потока

Параметр	Описание
--regexp=<strValue>	Добавление маски фильтра сетевого трафика на основе регулярных выражений. Введите строковое значение, определяющее необходимость обработки IP-пакета. Правилом обрабатываются только IP-пакеты, содержимое которых соответствует маске фильтра. Например, значению *abcd* будет соответствовать любой пакет, в теле которого встречается последовательность abcd. По умолчанию параметр --regexp имеет пустое значение. Параметр применяется только для формирования правил фильтрации сетевого потока. Значение параметра --regexp необходимо указывать строго в одинарных кавычках. Например, --regexp='/<object\s+(?:[^<>]+\s)?(?:type=\"[^"]*javascript|codebase=\"[^"]*\.js\W)/is'
--nocase=<boolValue>	Добавление регистронезависимого поиска. Допустимые логические значения параметра: • true — чувствительность к регистру символов выключена; • false — чувствительность к регистру символов включена. Параметр --nocase применяется совместно с параметрами --content, --wildcard, --regexp, --exefile. По умолчанию для правил фильтрации сетевого потока предусмотрен регистрозависимый поиск
--direction=<direct>	Настройка направления сетевого трафика, для которого действует правило. Допустимые значения параметра --direction: • in — правило для входящего сетевого трафика; • out — правило для исходящего сетевого трафика; • inout — направление сетевого трафика не указано (значение по умолчанию). Параметр --direction применяется только для формирования правил фильтрации сетевого потока
--encode=<strValue>	Кодирование значения параметра --content. По умолчанию параметр --encode имеет пустое значение. Параметр --encode применяется совместно с параметром --content
--adapters=<name1, name2,...,nameN>	<nameN> — имя сетевого адаптера. Символ * (звездочка) является значением по умолчанию для параметра

Пример команды:

```
fw-localcfg --add --action=drop --protocol=udp --local_
addrs=192.168.0.1-192.168.0.10,192.168.0.200 --local_
ports=76-92,67,80 --remote_addrs=10.0.0.0/24,192.168.10.0 --
remote_ports=8234,80-234 --msg='Drop packet!' --order=123 --
exefile='test_exe' --substr=true --schedule="* 1,3 + # 12-13
2,4 -" --audit=true --enable=false --direction=out
```

Добавление правила фильтрации со следующими параметрами:

- запрет трафика по протоколу UDP;
- указание диапазона IP-адресов отправителей пакетов;
- указание диапазона портов отправителей пакетов;
- указание перечня IP-адресов получателей пакетов;
- указание порта назначения получателей пакетов;
- заданная последовательность обработки правил;
- добавление исполняемого файла "test_exe";

- фильтрация с учетом расписания;
- включение регистрации событий при срабатывании правила;
- отключение правила;
- правило для исходящего сетевого трафика.

Команда delete

Команда delete удаляет существующие правила настройки межсетевого экрана.

Для команды delete предусмотрены следующие параметры:

Параметр	Описание
--id	Удаление существующего правила с указанием его уникального идентификатора. Добавление id правил происходит в формате 4d024ebd-e5ea-47cf-8fe4-7c4dbbcff610
--all	Удаление всех правил

Примеры команд:

```
fw-localcfg --delete --id=3c5125e1-ee84-463c-a477-
b46afa954438
```

Удаление правила с указанием его уникального идентификатора.

```
fw-localcfg --delete --all
```

Удаление всех правил. При удалении всех правил будет необходимо подтвердить действие.

Команда import

Команда import осуществляет импорт существующих правил настройки персонального межсетевого экрана.

Для команды import предусмотрены следующие параметры:

Параметр	Описание
--file=<strValue>	Указание полного имени архивного файла резервной копии
--append	Добавляет импортируемые правила к существующим
--replace	Заменяет существующие правила
--list	Отображает список существующих архивов

Пример команды:

```
fw-localcfg --import --replace
--file=/tmp/test.tar.gz
```

Импорт существующих правил настройки персонального межсетевого экрана из архивного файла резервной копии.

После осуществления импорта правил персонального межсетевого экрана рекомендуется выполнить перезагрузку модуля ПМЭ. Для этого запустите программу эмулятора терминала и выполните команду:

```
systemctl restart snlsp-firewall
```

Команда export

Команда export осуществляет экспорт существующих правил настройки персонального межсетевого экрана. Архивный файл резервной копии сохраняется в каталоге /opt/snlsp- firewall/usr/backup/firewall с указанным именем <file_ name>.tar.gz.

Пример команды:

```
fw-localcfg --export
```

Экспорт существующих правил настройки персонального межсетевого экрана в архивный файл резервной копии.

Команда show

Команда show выводит справочную информацию о правилах межсетевого экрана.

Для команды show предусмотрены следующие параметры:

Параметр	Описание
--id	Удаление существующего правила с указанием его уникального идентификатора. Добавление id правил происходит в формате 4d024ebd-e5ea-47cf-8fe4-7c4dbbcff610
--all	Удаление всех правил

Примеры команд:

```
fw-localcfg --show --id=3c5125e1-ee84-463c-a477-b46afa954438
```

Вывод справочной информации об определенном правиле.

```
fw-localcfg --show --all
```

Вывод справочной информации обо всех правилах.

Утилита fw-net

Для просмотра и принудительного завершения выбранных TCP-соединений в Secret Net LSP предусмотрено использование утилиты **fw-net**.

Описание аргументов, применимых к утилите, представлено в следующей таблице:

Аргумент		Описание
-h	--help	Выводит справочную информацию о применении утилиты с отображением перечня допустимых команд
-k	--killc	Выполняет запуск утилиты

Примеры команд:

```
fw-net -h
```

Выполняется отображение справочной информации о применении утилиты **fw-net**.

```
fw-net -k
```

Выполняется запуск утилиты **fw-net**.

Описание команд для управления утилитой представлено в следующей таблице:

Команда	Описание
help	Выводит справочную информацию
<id>	Выполняет ввод идентификатора TCP-соединения для его принудительного завершения
list	Отображает список активных TCP-соединений
exit	Выполняет выход из утилиты

Примеры команд:

```
Enter command: list
```

Выполняется отображение списка всех активных TCP-соединений.

```
Enter command: 17
```

Выполняется ввод идентификатора TCP-соединения для его принудительного завершения.

Настройка персонального межсетевого экрана на основе правил

Правила персонального межсетевого экрана Secret Net LSP обеспечивают выполнение функциональности механизма.

В рамках настройки работы механизма администратор, обладающий правами суперпользователя компьютера, выполняет следующие действия:

- осуществляет вывод справочной информации о применении утилиты ПМЭ (см. стр.**86**);
- создает новые правила (см. стр.**87**);
- изменяет существующие правила (см. стр.**87**);
- удаляет существующие правила (см. стр.**87**);
- импортирует настройки ПМЭ из архивного файла резервной копии (см. стр.**87**);
- экспортирует правила в архивный файл резервной копии (см. стр.**88**);
- осуществляет вывод информации о существующих правилах (см. стр.**88**);
- проводит аудит событий ПМЭ (см. стр.**93**).

Пояснение.
Основные процедуры, связанные с настройкой работы ПМЭ, выполняются в режиме командной строки. При работе с правилами ПМЭ в программе эмулятора терминала необходимо соблюдать следующую последовательность вводимых команд: [название утилиты] [<команда>] ... [<параметр=значение>].

С помощью ПМЭ осуществляется:

- фильтрация по протоколам TCP/IPv4;
- фильтрация по командам сетевых протоколов;
- фильтрация по параметрам команд;
- фильтрация по контролю доступа к ресурсам, содержащим скрипты;
- контроль доступа к именованным файлам и общим папкам;
- контроль доступа для пользователей и групп пользователей.

Описание утилиты **fw-localcfg**, используемой для настройки ПМЭ, и особенности ее применения приведены на стр.**79**.

Вывод справочной информации о применении утилиты ПМЭ

Пояснение.
В Secret Net LSP для администратора предусмотрена возможность просмотра справочной информации об утилите **fw-localcfg**, содержащей правила ПМЭ, перечень команд, список допустимых параметров настройки, а также примеры использования команд.

Для вывода справочной информации об утилите:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Для вывода справочной информации предусмотрено использование общего аргумента **--help**.
4. Предусмотрен вывод информации по каждому действию отдельно.

Ниже представлена команда вывода справочной информации об импорте правил ПМЭ:

```
fw-localcfg --help --import
```

Добавление правил персонального межсетевого экрана

В рамках настройки персонального межсетевого экрана администратор формирует новые правила на основе требуемых параметров работы механизма.

Для формирования новых правил ПМЭ:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Введите ключ **--add**.
4. Введите в командной строке обязательные параметры **--action**, **--protocol**, **--msg**, без которых правило не будет создано, после чего включите в состав добавляемого правила необходимые параметры. Перечень допустимых параметров правил ПМЭ, их описание и примеры приведены на стр.**79**.

Изменение правил персонального межсетевого экрана

В рамках настройки персонального межсетевого экрана администратор имеет возможность изменять существующие правила, корректируя требуемые параметры работы ПМЭ.

Для изменения существующих правил ПМЭ:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Введите ключ **--modify**.
4. Введите в командной строке параметр **--id**. В значении параметра укажите уникальный идентификатор изменяемого правила.
5. Введите в командной строке изменяемый параметр с указанием его нового значения. Перечень допустимых параметров правил ПМЭ, их описание и примеры приведены на стр.**79**.

Удаление правил персонального межсетевого экрана

В рамках настройки персонального межсетевого экрана администратор имеет возможность удалять существующие правила работы механизма.

Для удаления правил ПМЭ:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Введите ключ **--delete**.
4. Введите в командной строке параметр **--id**. В значении параметра укажите уникальный идентификатор удаляемого правила. Также вы можете ввести в командной строке параметр **--all** для удаления всех правил.

Импорт правил персонального межсетевого экрана

В рамках настройки персонального межсетевого экрана администратор имеет возможность импортировать правила из архивного файла резервной копии.

Для импорта правил ПМЭ:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Для осуществления импорта введите ключ **--import**.
4. Укажите ключ для указания действия над существующими правилами. Для добавления импортируемых правил к существующим введите ключ **append**. Для замены существующих правил введите ключ **replace**.
5. Введите в командной строке параметр **--file** с указанием полного имени архивного файла резервной копии.

Ниже представлен пример импорта правил персонального межсетевого экрана:

```
fw-localcfg --import --replace --file=/tmp/test.tar.gz
```

После осуществления импорта правил персонального межсетевого экрана рекомендуется выполнить перезагрузку модуля ПМЭ. Для этого запустите программу эмулятора терминала и выполните команду:

```
systemctl restart snlsp-firewall
```

Экспорт правил персонального межсетевого экрана

В рамках настройки персонального межсетевого экрана администратор имеет возможность экспортировать правила в архивный файл резервной копии.

Для осуществления экспорта правил ПМЭ:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Для осуществления экспорта правил введите ключ **--export**.
4. Архивный файл резервной копии сохраняется в каталоге **/opt/snlsp-firewall/usr/backup/firewall** с указанием имени файла **<file_name>.tar.gz**.

Ниже представлен пример экспорта правил настройки межсетевого экрана в каталог с указанием имени архивного файла резервной копии:

```
fw-localcfg --export
```

Вывод справочной информации о правилах персонального межсетевого экрана

В рамках настройки персонального межсетевого экрана администратор имеет возможность просматривать список существующих правил ПМЭ.

Для просмотра списка существующих правил:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Введите ключ **--show**.
4. Введите в командной строке параметр **--id**. В значении параметра укажите уникальный идентификатор правила, чтобы вывести информацию о правиле на экран. Также вы можете ввести в командной строке параметр **--all** для вывода информации обо всех правилах.

Перечень допустимых параметров правил ПМЭ, их описание и примеры приведены на стр.**79**.

Включение и отключение правил ПМЭ

В процессе работы ПМЭ администратор может включать или отключать правила.

Для настройки включения и отключения правила:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Введите ключ **--modify**.
4. Введите в командной строке параметр **--id**. В значении параметра укажите уникальный идентификатор изменяемого правила.
5. Введите в командной строке параметр **--enable** и укажите необходимые значения параметра.

Ниже представлены примеры включения и отключения правил ПМЭ:

```
fw-localcfg --modify --id=3c5125e1-ee84-463c-a477-
b46afa954438 --enable=false
```

Выполняется отключение правила фильтрации. Соответствующее событие зарегистрировано в системном журнале Secret Net LSP.

```
fw-localcfg --modify --id=3c5125e1-ee84-463c-a477-
b46afa954438 --enable=true
```

Выполняется включение правила фильтрации. Соответствующее событие зарегистрировано в системном журнале Secret Net LSP.

Фильтрация сетевого трафика

Персональный межсетевой экран осуществляет фильтрацию сетевого трафика для отправителей и получателей контролируемой информации в рамках всех операций ее передачи узлам информационной системы на сетевом, транспортном и прикладном уровнях, а также предоставляет возможность явно разрешать или запрещать информационный поток на основании правил, устанавливаемых администратором. Функциональность ПМЭ обеспечивается за счет работы модуля межсетевого экранирования.

Основные возможности, реализуемые модулем в рамках фильтрации сетевого трафика, представлены ниже:

- фильтрация на сетевом уровне с независимым принятием решений по каждому пакету;
- фильтрация на транспортном уровне запросов на установление виртуальных соединений (TCP-сессий);
- фильтрация на прикладном уровне запросов к прикладным сервисам;
- фильтрация пакетов протокола (ICMP, SMB);
- фильтрация с учетом полей сетевых пакетов;
- фильтрация с учетом направления трафика и сетевого интерфейса;
- фильтрация с учетом прав доступа;
- фильтрация с учетом расписания.

Внимание!
Средства Secret Net LSP позволяют настроить доступ к защищаемым компьютерам по протоколам сетевого уровня IPv4. По умолчанию доступ к защищаемым компьютерам разрешен только по протоколу IPv4. Рекомендуется отключить доступ по протоколу IPv6 для сетевых адаптеров с целью обеспечения стабильной работы персонального межсетевого экрана Secret Net LSP.

Настройка фильтрации трафика на основе протокола сетевого уровня

Правила персонального межсетевого экрана, задаваемые администратором, позволяют настроить контроль соединения с данным компьютером по протоколам сетевого уровня семейства TCP/IPv4.

Для настройки фильтрации на основе протокола сетевого уровня:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. При добавлении новых правил ПМЭ (подробнее см. стр.**87**) или изменении существующих (подробнее см. стр.**87**) включите в состав правила параметр **--proto**. В качестве значения параметра укажите название протокола, на основании которого осуществляется настройка фильтрации (подробнее см. стр.**79**).

   Ниже представлен пример настройки фильтрации на основе протокола ICMP:

   ```
   fw-localcfg --add --action=drop --proto=icmp
   --order=1 --msg="BLOCK" --audit=true
   ```

   Выполняется добавление правила, блокирующего пакеты протокола ICMP.

Настройка фильтрации трафика на основе протокола транспортного уровня

Правила персонального межсетевого экрана, задаваемые администратором, позволяют настроить контроль соединения с данным компьютером по протоколам транспортного уровня семейства TCP/IPv4.

Для настройки фильтрации на основе протокола транспортного уровня:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. При добавлении новых правил ПМЭ (подробнее см. стр.**87**) или изменении существующих (подробнее см. стр.**87**) включите в состав правила параметр **--proto**. В качестве значения параметра укажите название протокола, на основании которого осуществляется настройка фильтрации (подробнее см. стр.**79**).

   Ниже представлен пример настройки фильтрации на основе протокола TCP:

   ```
   fw-localcfg --add --action=drop --proto=tcp
   --msg="Drop" --remote_addrs=10.1.1.4/24 --audit=true
   ```

   Выполняется добавление правила, запрещающего трафик по протоколу TCP. В системном журнале Secret Net LSP регистрируется соответствующее событие. В случае попытки обмена данными по протоколу TCP, в журнале аудита Secret Net LSP регистрируется соответствующее сообщение. Соединение с компьютером, от которого поступил запрос, разрывается.

Примечание.
Администратор безопасности может просматривать текущие соединения по протоколу TCP, а также завершать выбранные TCP-соединения посредством тех же механизмов, что и ПМЭ. Для завершения выбранных соединений по протоколу TCP в Secret Net LSP предусмотрено использование утилиты **fw-net**.

Просмотр и принудительное завершение TCP-соединений

Для просмотра и принудительного разрыва выбранных TCP- соединений в Secret Net LSP используется утилита **fw-net**. Описание утилиты и особенности ее применения приведены на стр.**85**.

Примеры:

Пример 1. Настройка блокировки передачи файлов по протоколу File Transfer Protocol (FTP)

Создание правил, блокирующих отправку файлов по протоколу FTP (File Transfer Protocol).

```
fw-localcfg --add --action=drop --proto=tcp --msg="Drop stor"
--audit=true --content="stor" --nocase=true
```

или

```
fw-localcfg --add --action=drop --proto=tcp --msg="Drop put"
--audit=true --content="put" --nocase=true
```

Пример 2. Настройка блокировки JavaScript

Создание правила, блокирующего загрузку файлов с расширением JS (JavaScript File).

```
fw-localcfg --add --action=drop --proto=tcp --msg="Block js"
--audit=true --content=".js"
```

Создание правила, блокирующего использование JavaScript content.

```
fw-localcfg --add --proto=http --action=drop --msg='HTTP
JavaScript script content detected!' --audit=true --
regexp='/<script\s+(?:[^<>]+\s)?(?:type=\"
[^"]*javascript\W|language=\"JavaScript\"|src=\"
[^"]+\.js\W)/is'
```

Пример 3. Настройка блокировки сетевого трафика по протоколу HTTP

Создание правил, блокирующих сетевой трафик по протоколу HTTP. Блокировка осуществляется с помощью двух приведенных ниже правил, в случае если обмен сетевыми пакетами происходит не через 80 порт.

```
fw-localcfg --add --action=pass --proto=tcp --msg="Pass port
80" --audit=true --content="http" --nocase=true --remote_
ports=80 --order=1
```

```
fw-localcfg --add --action=drop --proto=tcp --msg="Drop port"
--audit=true --content="http" --nocase=true
```

Пример 4. Настройка блокировки обмена сообщениями в Skype

Создание правила, блокирующего отправку и получение сообщений в Skype.

```
fw-localcfg --add --action=drop --proto=any
--msg="Block_skype" --audit=true
--exefile="/usr/share/skypeforlinux/skypeforlinux"
```

Настройка фильтрации трафика на основе протокола ICMP

Правила персонального межсетевого экрана, задаваемые администратором, позволяют настроить контроль соединения с данным компьютером по служебным протоколам семейства TCP/IPv4.

Для настройки фильтрации на основе протокола ICMP:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. При добавлении новых правил ПМЭ (подробнее см. стр.**87**) или изменении существующих (подробнее см. стр.**87**) включите в состав системного правила параметр **--proto** и укажите значение **icmp** (подробнее см. стр.**79**).

   Ниже представлен пример настройки фильтрации на основе протокола ICMP:

   ```
   fw-localcfg --add --action=drop --proto=icmp
   --msg='Drop_icmp'
   ```

   Выполняется добавление правила фильтрации, запрещающего трафик по протоколу ICMP. Соединение с компьютером, от которого поступил запрос, разрывается.

Для настройки фильтрации с учетом типа пакета ICMP:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Для настройки фильтрации с учетом типа пакета ICMP включите в состав системного правила параметр **--icmp_type**. В качестве значения параметра укажите тип пакета ICMP (подробнее см. стр.**79**).

   Ниже представлен пример настройки фильтрации с учетом типа пакета ICMP:

   ```
   fw-localcfg --add --action=drop --proto=icmp
   --msg="Drop_icmp_type_8" --icmp_type=8
   ```

   Выполняется добавление правила фильтрации, блокирующего эхо-запросы по протоколу ICMP.

Примечание.
Параметр --icmp_type применяется только для протокола ICMP. По умолчанию правило фильтрации действует для всех типов пакетов ICMP.

Для настройки фильтрации с учетом кода пакета ICMP:

1. Запустите программу эмулятора терминала.
2. Введите в командной строке название утилиты ПМЭ **fw-localcfg**.
3. Для настройки фильтрации с учетом кода пакета ICMP включите в состав системного правила параметр **--icmp_code**. В качестве значения параметра укажите код пакета ICMP (подробнее см. стр.**79**).

   Ниже представлен пример настройки фильтрации с учетом кода пакета ICMP:

   ```
   fw-localcfg --add --action=drop --proto=icmp --msg="Drop_
   icmp_code_0" --icmp_code=0
   ```

   Выполняется добавление правила фильтрации, блокирующего эхо-запросы и ответы по протоколу ICMP.

Примечание.
Параметр --icmp_code применяется только для протокола ICMP. По умолчанию правило фильтрации действует для всех кодов пакетов ICMP.

Регистрация событий персонального межсетевого экрана

Предусмотрены два типа событий, которые регистрирует ПМЭ:

- управление персональным межсетевым экраном;
- срабатывание правила межсетевого экрана.

По умолчанию регистрация событий, связанных с управлением механизмом, включена, события регистрируются в системном журнале Secret Net LSP. Регистрация событий, связанных со срабатыванием правила ПМЭ, по умолчанию отключена и может быть настроена администратором. События срабатывания правила межсетевого экрана регистрируются в журнале аудита Secret Net LSP.

Для уведомления пользователя предусмотрен ключ alarm, который показывает сообщение о срабатывании правила в графике.

Для отслеживания событий срабатывания правила межсетевого экрана в журнале аудита предусмотрена служба **fw-audit**, которая отслеживает события срабатывания правил с настройкой **--audit=true** и отправляет оповещение администратору безопасности, обладающему правами суперпользователя компьютера, или пользователю, которому перенаправлены сообщения на локальный адрес электронной почты.

Все процедуры по настройке регистрации событий ПМЭ выполняются только администратором, обладающим правами суперпользователя, с использованием командной строки эмулятора терминала. Описание утилиты и особенности ее применения приведены на стр.**79**.

Для включения регистрации событий срабатывания правила ПМЭ:

1. Запустите программу эмулятора терминала.
2. При добавлении новых правил ПМЭ (подробнее см. стр.**87**) или изменении существующих (подробнее см. стр.**87**) включите в состав правила параметр **--audit** и установите логическое значение **<true>** для параметра.

   Ниже представлен пример включения регистрации событий при срабатывании правила фильтрации:

   ```
   fw-localcfg --add --ac=drop --proto=tcp --msg="Drop" --
   remote_addrs=10.1.1.4 --audit=true
   ```

Примечание.
Включение регистрации событий срабатывания правила персонального межсетевого экрана осуществляется отдельно для каждого правила.

Для отключения регистрации событий срабатывания правила ПМЭ:

1. Запустите программу эмулятора терминала.
2. При изменении существующих правил ПМЭ (подробнее см. стр.**87**) включите в состав правила параметр **--audit** и установите логическое значение **<false>** для параметра.

   Ниже представлен пример отключения регистрации событий при срабатывании правила фильтрации:

   ```
   fw-localcfg --modify --id=4d024ebd-e5ea-47cf-8fe4-
   7c4dbbcff610 --audit=false
   ```

Примечание.
Отключение регистрации событий срабатывания правила персонального межсетевого экрана осуществляется отдельно для каждого правила.

Аудит ПМЭ

По умолчанию механизм ПМЭ не предусматривает отслеживание состояния сетевых соединений при осуществлении фильтрации сетевого трафика путем регистрации сообщений в журнале аудита Secret Net LSP при срабатывании соответствующего правила с атрибутом **ruleid="0:0"**.

Для включения срабатывания правила:

1. Отредактируйте файл **/opt/snlsp-firewall/etc/suricata/suricata.yaml**, установив для параметра "enabled" значение "yes" в секциях "- anomaly:".

   Внимание!
   В файле **suricata.yaml** для параметра "enabled" необходимо установить значение "yes" в двух секциях "- anomaly:" для журналов eve.json и alert.json.

2. В файле **/opt/snlsp-firewall/etc/suricata/suricata.yaml** установите для параметра "drop-invalid" значение "yes" в секции "stream".
3. Сохраните внесенные изменения в файл и закройте его.
4. Выполните команду:

   ```
   /opt/snlsp-firewall/bin/fwfc -i
   ```

5. Выполните перезапуск механизма ПМЭ. Для этого выполните команду:

   ```
   systemctl restart snlsp-firewall
   ```

Аудит событий, связанных с работой механизма персонального межсетевого экранирования, проводится в соответствии с общим порядком аудита.

Примечание.
События срабатывания правила межсетевого экрана фиксируются в журнале аудита. Регистрация событий, связанных с управлением механизмом ПМЭ, осуществляется в системном журнале.

Приложение

Правила приемки и методы контроля

Приемка Secret Net LSP проводится в следующем объеме и последовательности:

1. Проверка комплектности и маркировки изделия.
2. Проверка контрольных сумм дистрибутивного комплекта ПО изделия.

Проверка комплектности и маркировки

Комплектность изделия проверяется внешним осмотром путем сравнения с данными, приведенными в формуляре изделия.

Проверка считается успешной, если комплектность изделия соответствует требованиям, приведенным в формуляре изделия.

Сертифицированные образцы изделия должны маркироваться идентификатором РОСС RU.01.XXXXX.XXXXXX, где первая группа знаков РОСС RU.01 указывает на систему сертификации ФСТЭК России, вторая группа знаков (числа 00001–99999) – номер сертификата, третья группа (числа 000001–999999) – серийный номер сертифицированного образца. Идентификатор сертифицированного СЗИ указывается в формуляре изделия в разделе "Свидетельство об изготовлении, упаковке, маркировке и приемке", на коробке для компакт-диска и формуляра и упаковочной коробке комплекта СЗИ. Идентификатор также заносится в базу данных фирмы-изготовителя.

Требования к маркировке:

1. При маркировке лицевой стороны установочного компакт-диска указываются:
- наименование изделия;
- наименование фирмы-изготовителя;
- номер сертификата.
2. При маркировке коробки для компакт-диска и формуляра указываются:
- наименование изделия;
- реквизиты фирмы-изготовителя;
- заводской номер;
- идентификатор сертифицированного СЗИ.
3. При маркировке упаковочной коробки комплекта СЗИ указываются:
- штрихкод;
- заводской номер;
- идентификатор сертифицированного СЗИ.

Проверка считается успешной, если маркировка соответствует требованиям, приведенным выше.

Проверка контрольных сумм дистрибутивного комплекта ПО

Проверка соответствия дистрибутивного носителя эталону проводится путем расчета контрольных сумм соответствующих файлов и их сравнения с контрольными суммами, указанными в приложении 1 к формуляру изделия.

Проверка считается успешной, если все контрольные суммы проверяемых файлов совпадают с эталонными контрольными суммами, указанными в приложении 1 к формуляру изделия.

Рекомендации по настройке для соответствия требованиям о защите информации

В разделе приведены значения параметров безопасности Secret Net LSP, которые рекомендуется установить в целях соответствия информационной системы требованиям о защите информации, предъявляемым к информационным системам различных типов и классов/уровней защищенности.

Автоматизированные системы

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие требованиям для следующих классов защищенности АС согласно классификации документа "Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации":

- АС первой группы:
  - 1Г;
  - 1Д.
- АС второй группы:
  - 2Б.
- АС третьей группы:
  - 3Б.

Использование средств защиты загрузки

В АС должны применяться средства, исключающие доступ пользователя к ресурсам компьютера в обход механизмов системы защиты. Для систем любого класса до 1Б включительно в качестве таких средств может использоваться изделие "Программно-аппаратный комплекс "Соболь".

При использовании Secret Net LSP на виртуальных машинах в виртуальной инфраструктуре на базе продуктов VMware Infrastructure или VMware vSphere в качестве средства доверенной загрузки виртуальных машин может применяться изделие "Средство защиты информации vGate R2" или "Средство защиты информации vGate- S R2", совместимое с версией используемого продукта.

Вместо вышеперечисленных средств или совместно с любым из них может быть разработан и внедрен комплекс организационно-технических мероприятий, обеспечивающих невозможность доступа пользователей к информации на дисках компьютера в обход механизмов системы Secret Net LSP.

Параметры политик Secret Net LSP

Для соответствия классам защищенности АС должны быть настроены параметры политик, перечисленные в следующей таблице.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.1 Параметры политик

Параметр	Классы защищенности АС		
	1Г, 1Д	2Б	3Б
Группа "Пользователи"			
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	все: 6 (обяз.)	6 (обяз.)	6 (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	все: Нет	Нет	Нет
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	все: 180 (реком.)	180 (реком.)	180 (реком.)
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	все: –	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	все: –	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	все: –	–	–
Группа "Аутентификация"			
Метод идентификации ID: **ident** Знач. по умолч.: **2**	все: –	–	–
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	все: Да (обяз.)	Да (обяз.)	Да (обяз.)
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	все: –	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	все: –	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	все: –	–	–
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	все: –	–	–
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	все: 10 (реком.)	10 (реком.)	10 (реком.)

Параметр	Классы защищенности АС		
	1Г, 1Д	2Б	3Б
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	все: –	–	–
Группа "Подсистема контроля устройств"			
Параметры контроля	1Г: Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.) 1Д: –	–	–
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	все: –	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	1Г: 2 (обяз.) 1Д: –	–	–
Группа "Подсистема дискреционного управления доступом"			
Режим работы ID: **mode** Знач. по умолч.: **Да**	все: –	–	–
Группа "Подсистема затирания информации"			
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	1Г: Да (обяз.) 1Д: –	–	–
Группа "Подсистема замкнутой программной среды"			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	1Г: Да (обяз.) 1Д: –	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1Г: 1 (обяз.) 1Д: –	–	–
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–

Параметр	Классы защищенности АС		
	1Г, 1Д	**2Б**	**3Б**
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Белый список пользователей и групп	1Г: root (обяз.) 1Д: –	–	–
Группа "Подсистема печати"			
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: Да (реком.)	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"			
Алгоритм ID: **hash_algorithm** **Настройка КЦ обязательна**	все: sha512 (реком.)	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"			
Режим работы ID: **mode** Знач. по умолч.: **Нет**	все: –	–	–
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	все: –	–	–
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	все: –	–	–
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	все: –	–	–
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	все: –	–	–
Группа "Журналирование и аудит"			
Настройка системного журнала ID: **system_journal**	все: –	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	все: –	–	–
Группа "Межсетевой экран"			
Вкл/выкл ID: **On** Знач. по умолч.: **true**	все: true (реком.)	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	все: true	true	true

Государственные информационные системы

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие требованиям для государственных информационных систем, изложенным в следующих нормативно-методических документах:

- "Меры защиты информации в государственных информационных системах" (документ утвержден ФСТЭК России 11 февраля 2014 г.).
- "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (утверждены приказом ФСТЭК России от 11 февраля 2013 г. №17).

Для классов защищенности ГИС К1, К2, К3 и К4 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Использование средств доверенной загрузки

В ГИС классов К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net LSP в ГИС всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net LSP

Для соответствия классам защищенности ГИС должны быть настроены параметры политик, перечисленные в следующей таблице.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.2 Параметры политик

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Группа "Пользователи"			
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	8 (обяз.)	6 (обяз.)	6 (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	60 (обяз.)	90 (обяз.)	120 (обяз.)
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Группа "Аутентификация"			
Метод идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)	2 (реком.)
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	–	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	4 (обяз.)	8 (обяз.)	10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Подсистема контроля устройств"			
Параметры контроля	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	–	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Группа "Подсистема дискреционного управления доступом"			
Режим работы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Подсистема затирания информации"			
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Подсистема замкнутой программной среды"			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	–	–
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–

Параметр	Классы защищенности ГИС		
	К1	**К2**	**К3**
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Белый список пользователей и групп	root (обяз.)	–	–
Группа "Подсистема печати"			
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"			
Алгоритм ID: **hash_alorithm** **Настройка КЦ обязательна для К1 и К2**	sha512 (реком.)	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"			
Режим работы ID: **mode** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Группа "Журналирование и аудит"			
Настройка системного журнала ID: **system_journal**	–	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Межсетевой экран"			
Вкл/выкл ID: **On** Знач. по умолч.: **true**	true (реком.)	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	true	true	true

Информационные системы персональных данных

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие требованиям для информационных систем персональных данных (ИСПДн), изложенным в документе "Состав и содержание организационных и

технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (утвержден приказом ФСТЭК России от 18 февраля 2013 г. №21).

Для уровней защищенности ИСПДн 1, 2, 3 и 4 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее — машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее — инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Использование средств доверенной загрузки

В ИСПДн уровней 1 и 2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net LSP в ИСПДн всех уровней защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net LSP

Для соответствия уровням защищенности ИСПДн должны быть настроены параметры политик, перечисленные в следующей таблице.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.3 Параметры политик

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Группа "Пользователи"				
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	8 (обяз.)	6 (обяз.)	6 (обяз.)	6 (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	60 (обяз.)	90 (обяз.)	120 (обяз.)	180 (обяз.)
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	–	–	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	–	–	–	–
Группа "Аутентификация"				
Метод идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)	2 (реком.)	2 (реком.)
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	–	–	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	4 (обяз.)	8 (обяз.)	10 (обяз.)	10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)	15 (обяз.)

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	–	–	–	–
Группа "Подсистема контроля устройств"				
Параметры контроля	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)		
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	–	–	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	–	–
Группа "Подсистема дискреционного управления доступом"				
Режим работы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Подсистема затирания информации"				
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	–	–	–	–
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)	–
Группа "Подсистема замкнутой программной среды"				
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	–	–	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	–	–	–	–
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	–	–	–	–
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	–	–	–	–

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	–	–	–	–
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	–	–	–	–
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	–	–	–	–
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	–	–	–	–
Белый список пользователей и групп	–	–	–	–
Группа "Подсистема печати"				
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"				
Алгоритм ID: **hash_algorithm** **Настройка КЦ обязательна для УЗ-1 и УЗ-2**	sha512 (реком.)	sha512 (реком.)	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"				
Режим работы ID: **mode** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–	–
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–	–
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–	–
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–	–
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–	–
Группа "Журналирование и аудит"				
Настройка системного журнала ID: **system_journal**	–	–	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–	–
Группа "Межсетевой экран"				

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Вкл/выкл ID: **On** Знач. по умолч.: **true**	true (реком.)	true (реком.)	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	true	true	true	true

Информационные системы Банка России

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие требованиям, установленным Банком России к объектам информатизации (в том числе АС) финансовых организаций, изложенным в следующем стандарте:

- ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 г. №822-ст).

Для уровней защиты информации ИС Банка России УЗ-1, УЗ-2 и УЗ-3 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований для следующих процессов (направлений) защиты информации:

- процесс 1 "Обеспечение защиты информации при управлении доступом":
  - управление учетными записями и правами субъектов логического доступа:
    - идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
    - защита информации при осуществлении физического доступа;
    - идентификация, классификация и учет ресурсов и объектов доступа;
- процесс 2 "Обеспечение защиты вычислительных сетей":
  - сегментация и межсетевое экранирование вычислительных сетей;
  - выявление сетевых вторжений и атак:
    - защита информации, передаваемой по вычислительным сетям;
    - защита беспроводных сетей;
- процесс 3 "Контроль целостности и защищенности информационной инфраструктуры";
- процесс 4 "Защита от вредоносного кода";
- процесс 5 "Предотвращение утечек информации";
- процесс 6 "Управление инцидентами защиты информации":
  - мониторинг и анализ событий защиты информации;
  - обнаружение инцидентов защиты информации и реагирование на них;
- процесс 7 "Защита среды виртуализации";
- процесс 8 "Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств".

Использование средств доверенной загрузки

В ИС Банка России уровня защиты информации УЗ-1 должны применяться средства доверенной загрузки операционной системы. В качестве средства до-

веренной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net LSP в ИС Банка России всех уровней защиты информации рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net LSP

Для соответствия уровням защиты информации ИС Банка России должны быть настроены параметры политик, перечисленные в следующей таблице.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.4 Параметры политик

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Группа "Пользователи"			
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	8 (обяз.)	8 (обяз.)	8 (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	360 90 для администратора (обяз.)	360 90 для администратора (обяз.)	360 90 для администратора (обяз.)
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Группа "Аутентификация"			
Метод идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)	2 (реком.)
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	–	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	–	–	–
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	30 (обяз.)	30 (обяз.)	30 (обяз.)
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	15 (обяз.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Группа "Подсистема контроля устройств"			
Параметры контроля	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	–	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Группа "Подсистема дискреционного управления доступом"			
Режим работы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Подсистема затирания информации"			
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	Да (реком.)	–	–
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Группа "Подсистема замкнутой программной среды"			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	1 (обяз.)	–
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Белый список пользователей и групп	root (обяз.)	root (обяз.)	–
Группа "Подсистема печати"			
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"			
Алгоритм ID: **hash_algorithm** **Настройка КЦ обязательна**	sha512 (реком.)	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"			
Режим работы ID: **mode** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	–
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	–
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	–
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	–

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	–
Группа "Журналирование и аудит"			
Настройка системного журнала ID: **system_journal**	–	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Межсетевой экран"			
Вкл/выкл ID: **On** Знач. по умолч.: **true**	true (реком.)	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	true	true	true

Автоматизированные системы управления производственными и технологическими процессами

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие требованиям для автоматизированных систем управления производственными и технологическими процессами (АСУ ТП), изложенным в следующем нормативном документе:

- Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. №31).

Для классов защищенности АСУ ТП К1, К2 и К3 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;

- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Использование средств доверенной загрузки

В АСУ ТП классов К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net LSP в АСУ ТП всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net LSP

Для соответствия классам защищенности АСУ ТП должны быть настроены параметры политик, перечисленные в таблице ниже.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.5 Параметры политик

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Группа "Пользователи"			
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	8 (обяз.)	6 (обяз.)	6 (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	60	90	120
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Группа "Аутентификация"			
Метод идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)	2 (реком.)
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	–	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	4 (обяз.)	8 (обяз.)	10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Подсистема контроля устройств"			
Параметры контроля	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	–	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Группа "Подсистема дискреционного управления доступом"			
Режим работы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Подсистема затирания информации"			
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Группа "Подсистема замкнутой программной среды"			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	–	–
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Белый список пользователей и групп	root (обяз.)	–	–
Группа "Подсистема печати"			
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"			
Алгоритм ID: **hash_algorithm** **Настройка КЦ обязательна**	sha512 (реком.)	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"			
Режим работы ID: **mode** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–

Параметр	Классы защищенности АСУ ТП		
	К1	**К2**	**К3**
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Группа "Журналирование и аудит"			
Настройка системного журнала ID: **system_journal**	–	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Межсетевой экран"			
Вкл/выкл ID: **On** Знач. по умолч.: **true**	true (реком.)	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	true	true	true

Критическая информационная инфраструктура Российской Федерации

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (КИИ), изложенным в нормативном документе "Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (утверждены приказом ФСТЭК России от 25 декабря 2017 г. №239).

Для категорий значимости КИИ ТП К1, К2 и К3 определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Использование средств доверенной загрузки

В КИИ категорий значимости К1 и К2 должны применяться средства доверенной загрузки операционной системы. В качестве средства доверенной загрузки может использоваться изделие "Программно- аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net LSP в КИИ всех категорий значимости рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net LSP

Для соответствия категориям значимости КИИ должны быть настроены параметры политик, перечисленные в таблице ниже.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;
- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.6 Параметры политик

Параметр	Категории значимости КИИ		
	К1	**К2**	**К3**
Группа "Пользователи"			
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	8 (обяз.)	6 (обяз.)	6 (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	60 (обяз.)	90 (обяз.)	120 (обяз.)
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Группа "Аутентификация"			
Метод идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)	2 (реком.)

Параметр	Категории значимости КИИ		
	К1	К2	К3
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	–	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	4 (обяз.)	8 (обяз.)	10 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Подсистема контроля устройств"			
Параметры контроля	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	–	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Группа "Подсистема дискреционного управления доступом"			
Режим работы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)

Параметр	Категории значимости КИИ		
	К1	К2	К3
Группа "Подсистема затирания информации"			
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Группа "Подсистема замкнутой программной среды"			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	–	–
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Белый список пользователей и групп	root (обяз.)	–	–
Группа "Подсистема печати"			
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"			
Алгоритм ID: **hash_algorithm** **Настройка КЦ обязательна**	sha512 (реком.)	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"			
Режим работы ID: **mode** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–

Параметр	Категории значимости КИИ		
	К1	К2	К3
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Группа "Журналирование и аудит"			
Настройка системного журнала ID: **system_journal**	–	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Группа "Межсетевой экран"			
Вкл/выкл ID: **On** Знач. по умолч.: **true**	true (реком.)	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	true	true	true

Информационные системы, предназначенные для обработки биометрических персональных данных

При определенных вариантах настройки Secret Net LSP обеспечивает соответствие рекомендациям по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина РФ.

Рекомендации изложены в следующих нормативно-методических документах:

- Указание "О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года №149-ФЗ "Об информации, информационных технологиях и о защите информации", в единой биометрической системе (утверждено Центральным Банком Российской Федерации (Банк России) 9 июля 2018 года №4859-У/01/01/782-18);
- Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (утверждены Центральным

Банком Российской Федерации (Банк России) от 14 февраля 2019 г. №4-МР);

- Порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации (утвержден приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 №321).

Для уровней защиты информации ЕБС-1 (усиленный уровень, для системно значимых кредитных организаций) и ЕБС-2 (стандартный уровень) определены базовые наборы мер защиты информации. Организационные и технические меры защиты информации должны обеспечивать реализацию следующих основных требований:

- идентификация, аутентификация, авторизация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- выявление сетевых вторжений и атак;
- сегментация и межсетевое экранирование вычислительных сетей;
- контроль целостности и защищенности;
- защита технических средств и систем;
- защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств;
- управление инцидентами защиты информации;
- защита среды виртуализации.

Использование средств доверенной загрузки

В информационной системе ЕБС всех уровней защиты информации рекомендуется применение средства доверенной загрузки операционной системы в виде аппаратно-программных модулей доверенной загрузки уровня платы расширения, сертифицированных ФСТЭК России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по 2 классу защиты.

В качестве средства доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

Для обеспечения непрерывности функционирования Secret Net LSP в ЕБС всех уровней защиты информации рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net LSP

Для соответствия уровням защиты информации ЕБС должны быть настроены параметры политик, перечисленные в таблице ниже.

Условные обозначения:

- "Да" — включить параметр;
- "Нет" — отключить параметр;
- (обяз.) — действие обязательно для выполнения;
- (реком.) — действие рекомендуется для выполнения;

- "–" — значение параметра на усмотрение администратора безопасности (значение по умолчанию).

Табл.7 Параметры политик

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	ЕБС-2
Группа "Пользователи"		
Минимальная длина пароля ID: **min_passwrd_size** Знач. по умолч.: **7**	8 16 для администратора (обяз.)	8 16 для администратора (обяз.)
Сложность пароля ID: **passwd_strength** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Срок действия пароля ID: **max_days** Знач. по умолч.: **-1**	360 90 для администратора (обяз.)	360 90 для администратора (обяз.)
Предупреждать об истечении за ID: **warn_days** Знач. по умолч.: **1**	–	–
Минимум между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–
Блокировать после устаревания ID: **inactive_days** Знач. по умолч.: **0**	–	–
Группа "Аутентификация"		
Метод идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)
Блокировать экран при изъятии токена ID: **lock** Знач. по умолч.: **0**	–	–
Кешировать данные идентификатора для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	4 (обяз.)	4 (обяз.)
Время блокировки при достижении количества неудачных попыток аутентификации ID: **unlock_time** Знач. по умолч.: **0**	30 (обяз.)	30 (обяз.)
Максимальный период неактивности до блокировки экрана ID: **lock_delay** Знач. по умолч.: **10**	15 (обяз.)	15 (реком.)

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
Оповещение пользователя о последнем успешном входе ID: **last_log** Знач. по умолч.: **Нет**	Да (обяз.)	–
Группа "Подсистема контроля устройств"		
Параметры контроля	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)	Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.)
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	–	–
Аудит (детализация сообщений) ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)
Группа "Подсистема дискреционного управления доступом"		
Режим работы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Группа "Подсистема затирания информации"		
Очистка оперативной памяти ID: **mode** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Затирание диска ID: **sntrashd** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Группа "Подсистема замкнутой программной среды"		
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	1 (обяз.)
Регистрация исполнения файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация запрета исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация загрузки библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация запрета загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация открытия файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
Регистрация запрета открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Белый список пользователей и групп	root (обяз.)	root (обяз.)
Группа "Подсистема печати"		
Сервис печати ID: **sncupsd** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Группа "Подсистема контроля целостности"		
Алгоритм ID: **hash_algorithm** **Настройка КЦ обязательна**	sha512 (реком.)	sha512 (реком.)
Группа "Подсистема управления Соболем"		
Режим работы ID: **mode** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Контроль секторов ID: **sable_control_sector** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Контроль файлов ID: **sable_control_file** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Контроль PCI-устройств ID: **sable_control_pci** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Контроль SMBIOS ID: **sable_control_smbios** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Группа "Журналирование и аудит"		
Настройка системного журнала ID: **system_journal**	–	–
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–
Группа "Межсетевой экран"		
Вкл/выкл ID: **On** Знач. по умолч.: **true**	true (реком.)	true (реком.)
Блокировка ошибочных пакетов ID: **firewall/State** Знач. по умолч.: **true**	true	true