КОД безопасности

Средство защиты информации

Secret Net Studio (исполнение 2)

Руководство администратора

Linux

RU.88338853.501400.001 01 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

Список сокращений

БД	База данных
ЗПС	Замкнутая программная среда
ИС	Информационная система
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПМЭ	Персональный межсетевой экран
ПО	Программное обеспечение
СБ SNS	Сервер безопасности Secret Net Studio (для Windows)
СЗИ	Средство защиты информации
ФК	Функциональный контроль
ЭИ	Электронный идентификатор
AD	Active Directory
CLI	Command Line Interface
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
PCI	Peripheral Component Interconnect
PID	Product Identification
SMB	Server Message Block
SMBIOS	System Management Basic Input/Output System
TCP	Transmission Control Protocol
VID	Vendor Identification

Введение

Руководство предназначено для администраторов изделия "Средство защиты информации Secret Net Studio (исполнение 2)" RU.88338853.501400.001 01 (далее — СЗИ Secret Net Studio, Secret Net Studio, СЗИ), функционирующего под управлением дистрибутивов семейства Linux. В руководстве содержатся сведения, необходимые для установки, обновления, настройки и управления Secret Net Studio.

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.

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

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

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

Глава 1
Общие сведения

Назначение

Программный продукт Secret Net Studio предназначен для защиты от НСД к информационным ресурсам компьютеров, функционирующих под управлением следующих дистрибутивов семейства Linux:

- Альт 8 СП;
- Альт Рабочая Станция 10;
- Альт Сервер 10;
- Ред ОС 7.3;
- AlterOS 7.5;
- Astra Linux Special Edition 1.7.

Основные функции

Secret Net Studio 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 Studio и объектов файловой системы;
- создание замкнутой программной среды для пользователей;
- фильтрация трафика межсетевым экраном;
- регистрация событий безопасности в журналах;
- контроль действий пользователей, связанных с доступом к файлам, устройствам и узлам вычислительной сети;
- аудит действий субъектов.

Функции администратора

Функциональные возможности системы позволяют администратору решать следующие задачи:

- управлять пользователями и группами;
- контролировать вход пользователей в систему;
- разграничивать доступ пользователей к ресурсам на основе принципа дискреционного управления доступом;
- контролировать целостность ресурсов;
- формировать для пользователей замкнутую программную среду;
- осуществлять контроль печати;
- 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 Studio 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 Studio устанавливается на компьютеры, удовлетворяющие следующим системным требованиям:

Операционная система	• Альт 8 СП; • Альт Рабочая Станция 10; • Альт Сервер 10; • Ред ОС 7.3; • AlterOS 7.5; • Astra Linux Special Edition 1.7;
Процессор	В соответствии с требованиями операционной системы, установленной на компьютер
Количество ядер процессора	Минимально — 2 ядра
Оперативная память	Минимально — 4 Гбайт
Жесткий диск	Рекомендуется — 16 Гбайт

Лицензии на использование подсистем

Механизмы защиты Secret Net Studio доступны для использования при наличии соответствующих зарегистрированных лицензий. Лицензируются следующие компоненты:

- компоненты, входящие в базовую защиту (обязательная лицензия);
  - защита входа в систему;
  - контроль целостности;
  - регистрация событий;
  - затирание остаточной информации;
  - контроль печати;
  - аудит.
- контроль устройств;
- дискреционное управление доступом;
- замкнутая программная среда;
- персональный межсетевой экран.

После установки Secret Net Studio функционирует в ограниченном режиме работы до активации продукта. Порядок эксплуатации Secret Net Studio в ограниченном режиме с помощью командной строки приведен на стр. **79**.

Защитные механизмы

Защитные механизмы — это программные средства, предназначенные для реализации защитных функций Secret Net Studio. Краткое описание основных защитных механизмов, используемых в системе защиты, приводится ниже.

Механизм защиты входа в систему

Внимание!

Для корректного журналирования действий пользователя необходимо использовать утилиты Secret Net Studio. Они соответствуют стандартным утилитам Linux для работы с пользователями и размещаются в каталогах /opt/securitycode/sns/bin и /opt/securitycode/sns/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 учетных записей пользователей.

Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователя выполняются при каждом входе в систему. При входе в систему 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 системном журнале.

Для обеспечения дополнительной защиты входа в Secret Net Studio 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 Studio может функционировать совместно с комплексом "Соболь". При этом комплекс "Соболь" обеспечивает дополнительную защиту от несанкционированного доступа к информационным ресурсам компьютера посредством доверенной загрузки.

В Secret Net Studio 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):

Производитель	USB-ключи	Смарт-карты
Аладдин	JaCarta ГОСТ JaCarta PKI/ГОСТ JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ JaCarta SF/ГОСТ	JaCarta-2 ГОСТ JaCarta-2 PKI/ГОСТ
Актив	Рутокен ЭЦП Рутокен ЭЦП 2.0 Рутокен ЭЦП 3.0 Рутокен ЭЦП PKI Рутокен Lite Рутокен S	Рутокен ЭЦП
Валидата	vdToken 2.0	—
Рубинтех	Guardant ID	—
ESMART	ESMART Token	ESMART Token

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 Studio.

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;

- требовать предъявление закрытого ключа пользователя при входе в систему;
- разрешить вход в комплекс "Соболь".

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

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.

Для доменных пользователей при совместном функционировании Secret Net Studio с СБ SNS может быть включен режим усиленной аутентификации. В этом режиме проверяется соответствие указанного пароля эталонному значению пароля пользователя, хранящемуся на СБ SNS.

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 или пользователям, входящим в группу snadmin.

К блокировке приводят следующие ситуации:

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

Проверка целостности компонентов Secret Net Studio, модуля ПМЭ и объектов файловой системы выполняется при загрузке 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/securitycode/sns/sbin.

Блокировка учетных записей

Для защиты входа в систему в Secret Net Studio 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/securitycode/sns/sbin.

Администратор имеет возможность разблокировать учетную запись пользователя в случае превышения допустимого количества неудачных попыток входа с помощью утилит **pam_tally** и **pam_tally2**, расположенной в каталоге /opt/securitycode/sns/bin.

Механизм дискреционного управления доступом

Механизм дискреционного управления доступом 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.

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 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 дискреционного управления доступом 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 контроля устройств

Механизм контроля устройств обеспечивает своевременное обнаружение изменений аппаратной конфигурации компьютера и реагирование на эти изменения.

Для защиты доступа к устройствам компьютера используются механизм контроля подключения и механизм контроля доступа к устройствам. Работа этих механизмов взаимосвязана. Механизм контроля подключения предназначен для обнаружения и реагирования на изменения аппаратной конфигурации компьютера. С помощью механизма контроля доступа выполняется разграничение доступа пользователей и групп к устройствам.

Внимание!

В текущей версии Secret Net Studio 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 механизме контроля устройств Secret Net Studio имеется разделение на следующие шины:

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

Шина/группа устройств	Класс устройств
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 контроля устройств. В рамках контроля и управления администратор выполняет следующие функции:

- устанавливает и при необходимости изменяет права доступа;
- управляет подсистемой контроля устройств;
- 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;
- SystemID;
- 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.

Механизм контроля целостности

Механизм КЦ предназначен для контроля целостности 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.

По умолчанию контроль целостности проводится в автоматическом режиме при загрузке операционной системы. Администратор может выбрать ресурсы, которые будут контролироваться в реальном времени. На выбранные ресурсы не будет действовать расписание.

Объекты и параметры контроля

Объектами контроля целостности в СЗИ Secret Net Studio 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 объектов ведется по любому сочетанию следующих параметров:

- права доступа;
- владелец (пользователь и группа);
- размер объекта;
- время и дата последней модификации;
- контрольная сумма содержимого файла по выбранному алгоритму.

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). Выбор алгоритма влияет на две подсистемы: КЦ и ЗПС.

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

Регистрация событий

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

Полный перечень регистрируемых событий приведен в приложении.

Реакция СЗИ на нарушение целостности объектов

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

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

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 Studio реализована возможность настроить расписание для контроля целостности. Настройка расписания указывается в формате cron с помощью утилиты snaidectl.

В Secret Net Studio реализована возможность настроить включение КЦ при загрузке ОС.

Для защищаемых объектов доступна возможность включения контроля в реальном времени. Контроль в реальном времени означает, что контроль целостности объекта происходит не по расписанию, а при доступе к файловому объекту. КЦ в реальном времени должен включаться для каждого объекта отдельно.

Нарушение КЦ регистрируется, если для контролируемого объекта изменяется хотя бы один из его контролируемых атрибутов.

Механизм замкнутой программной среды

Механизм ЗПС предназначен для ограничения запуска ПО.

Режимы работы механизма

Для работы ЗПС предусмотрены следующие режимы работы:

- мягкий;
- жесткий.

Мягкий режим нужен для настройки механизма, жесткий — это основной штатный режим работы.

В мягком режиме пользователю разрешается запускать любые программы. Если при этом пользователь запускает программы, не входящие в перечень разрешенных, в журнале Secret Net Studio регистрируются соответствующие события тревоги. В жестком режиме разрешается запуск только тех программ, которые входят в список разрешенных. Запуск других программ блокируется, а в журнале Secret Net Studio 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 администратора появится уведомление о необходимости подтверждения жесткого режима ЗПС. Если жесткий режим не подтвердить, то при следующей загрузке компьютера останется мягкий режим.

Регистрация событий

События, связанные с настройкой механизма ЗПС, регистрируются в системном журнале.

События, связанные с работой механизма ЗПС, регистрируются в журнале аудита.

Белый список пользователей и групп

Пользователям и группам, находящимся в белом списке, разрешен запуск всех программ, файлов, библиотек и скриптов. Для них не применяются ограничения жесткого режима.

Список исключений для ресурсов

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

Правила

Правила ЗПС обеспечивают разграничение доступа пользователей к ресурсам. Правила ЗПС могут быть созданы вручную, по событиям журнала аудита или автоматической генерацией правил. Автоматическая генерация не гарантирует, что добавленное правило будет корректно разрешать запуск приложения. Оно может иметь скрытые зависимости и их нужно будет добавлять отдельно.

Примечание.
При запуске ресурсов, на которые распространяется правило ЗПС, осуществляется проверка его целостности. В случае нарушения контроля целостности запуск ресурсов запрещен.

Механизм персонального межсетевого экранирования

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

Механизм ПМЭ выполняет следующие функции:

- контроль сетевого трафика;
- нейтрализация угроз, связанных с сетевым взаимодействием;
- разграничение сетевого доступа;
- контроль папок общего доступа;
- контроль именованных 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 Studio 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 Studio события, происходящие на компьютере, и события, связанные с безопасностью системы, регистрируются в подсистеме журналирования, входящей в состав СЗИ. События обрабатываются и сохраняются в базе данных.

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 и действий с защищаемыми объектами.

Механизм затирания данных

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

Действие механизма заключается в очистке 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 включен. При необходимости администратор может вручную выключить механизм затирания.

Архитектура

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

- Подсистема 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 дискреционного управления доступом. Реализует дискреционную модель разграничения доступа субъектов (пользователей, процессов) к объектам файловой системы.
- Подсистема контроля устройств. Реализует контроль подключения и контроль доступа пользователей и групп к шинам USB, SATA, сетевым интерфейсам и подключаемым к ним устройствам.
- Подсистема контроля целостности. Осуществляет контроль целостности программных компонентов СЗИ и объектов файловой системы.
- Подсистема замкнутой программной среды. Предназначена для ограничения прав пользователя на запуск приложений.
- 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 ПМЭ правил фильтрации.
- Подсистема журналирования. Осуществляет сбор сведений о событиях, зарегистрированных в других подсистемах.
- Подсистема аудита. Предназначена для настройки регистрации событий и правил аудита.
- Подсистема затирания данных. Осуществляет очистку затиранием выделенных или перераспределенных участков оперативной памяти и памяти на локальных дисках и сменных носителях.

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

В Secret Net Studio используются следующие CLI-утилиты:

Утилита	Описание
snpolctl	Настройка параметров политик
sntokenctl	Выполнение операций с персональными идентификаторами
snsablectl	Управление интеграцией с комплексом "Соболь"
snscheck	Управление шаблонами КЦ комплекса "Соболь"
sndevctl	Контроль и управление доступом к устройствам
snaidectl	Выполнение процедур, связанных с контролем целостности
snauditctl	Просмотр и редактирование правил аудита
snlicensectl	Работа с лицензиями
snaecctl	Настройка замкнутой программной среды
fw-localcfg	Настройка персонального межсетевого экрана
fw-net	Настройка TCP-соединений
snnetctl	Настройка удаленного управления
snconnctl	Настройка подключения к серверу Security Code Orchestrator
snbckctl	Резервное копирование и восстановление
snjrnl	Работа с журналами
snjournaldctl	Работа со сторонним syslog-сервером для передачи данных журнала
snfc	Запуск процедуры проверки функционального контроля

Плагины безопасности

В состав подсистемы управления входят следующие плагины:

Плагин	Описание
Плагин управления замкнутой программной средой	Запуск утилиты ЗПС с требуемыми параметрами и регистрация событий ЗПС
Плагин управления контролем целостности	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 модулями ядра	Настройка дискреционного управления доступом и затирания данных
Плагин контроля печати	Управление состоянием контроля печати
Плагин управления доступом к устройствам	Управление состоянием КУ. Регистрация попыток доступа к устройствам
Плагин управления персональным межсетевым экраном	Управление состоянием ПМЭ. Блокировка ошибочных пакетов
Плагин управления системными сервисами	Управление состоянием системных сервисов
Плагин управления системными настройками	Управление состоянием системных настроек. Настройка минимальной критичности сообщений в журнале тревог для отправки журнала

Плагин	Описание
Плагин аутентификации	Настройка параметров идентификации и аутентификации
Плагин управления пользователями	Управление настройками паролей пользователей

Подсистема идентификации и аутентификации

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

Подсистема обеспечивает:

- предоставление консольного интерфейса для настройки идентификации и аутентификации при входе пользователей в систему;
- управление параметрами входа пользователей в систему;
- включение или выключение режима усиленной аутентификации для доменных пользователей. Работает только при управлении под СБ SNS;
- кеширование данных идентификатора для доменных пользователей;
- настройка и контроль параметров парольной политики.

Подсистема дискреционного управления доступом

Подсистема реализует дискреционную модель управления доступом 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 дискреционного управления доступом с подсистемой аудита позволяет администратору осуществлять аудит событий, связанных с доступом к защищаемым объектам.

В работе подсистемы используется механизм дискреционного управления доступом, 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-утилиты 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- утилиты управления являются приложением с классическим интерфейсом, предоставляющим администратору возможность выполнять все необходимые операции по управлению доступом средствами командной строки. В CLI-утилиты входят:

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

CLI-утилиты управления предназначены для выполнения общих функций по управлению правами доступа:

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

Подсистема контроля устройств

Подсистема контроля устройств обеспечивает своевременное обнаружение изменений аппаратной конфигурации компьютера и реагирование на эти изменения.

В состав подсистемы входят:

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

Загружаемый модуль ядра

Предназначен для выполнения следующих функций:

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

Приложение — обработчик событий

Приложение выполняет следующие функции:

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

Конфигурационный компонент

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

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

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

Модуль подсистемы локального управления предоставляет графический интерфейс настройки параметров работы механизма контроля устройств.

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

Режимы работы подсистемы

Предусмотрены два режима работы подсистемы:

- отключено — 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".

Подсистема контроля целостности

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

- расчет контрольных сумм ресурсов, поставленных на контроль;
- проверка целостности защищаемых ресурсов;
- проверка целостности по расписанию или в реальном времени;
- проверка целостности при загрузке ОС;
- обновление контрольных сумм;
- анализ результатов проверки контролируемых ресурсов;
- восстановление ресурсов;
- создание хранилища для ресурсов, 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. Обеспечивает управление настройками подсистемы контроля целостности 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 Studio 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 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 ЗПС взаимодействует с подсистемой КЦ для отслеживания неизменности ресурсов, на которые действуют правила ЗПС. Обе подсистемы используют один и тот же алгоритм расчета КС. Включение и отключение подсистемы КЦ не влияет на работу ЗПС.

Правило ЗПС содержит следующую информацию:

- статус (включено/выключено);
- для кого действует правило (пользователи и группы);
- список ресурсов, для которых применяется правило.

В состав подсистемы входят следующие компоненты:

- механизм ЗПС;
- CLI-утилиты управления;
- плагин и политика для управления ЗПС.

С помощью политики **snpolctl** доступно следующее управление ЗПС:

- включение/отключение подсистемы;
- изменение режима работы;
- включение/отключение регистрации событий.

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 адресов отправителя и получателя пакетов;
- 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 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 Studio.

В состав подсистемы межсетевого экранирования входит модуль ПМЭ, являющийся локальным компонентом СЗИ Secret Net Studio. Процедуры, связанные с установкой или удалением модуля ПМЭ, выполняются отдельно от основного пакета ПО Secret Net Studio (подробнее см. стр. **24**, стр. **25**).

Подсистема затирания данных

Подсистема предназначена для управления затиранием данных и обеспечивает выполнение следующих функций:

- затирание освобождаемых страниц оперативной памяти;
- затирание освобождаемых блоков на файловой системе;
- безопасное удаление информации на локальных дисках и сменных носителях;
- затирание SWAP;
- затирание hugetlbfs и tmpfs;
- включение и выключение механизма затирания на локальных дисках и сменных 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.

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 локальных дисках и сменных носителях независимо от установленного режима работы подсистемы применяется утилита **shred**.

Подсистема журналирования

Подсистема регистрирует и хранит события в журнале аудита и системном журнале.

Подсистемой выполняются следующие функции:

- сбор сведений от подсистем и 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;
- постраничный вывод содержимого журналов;
- сортировка отображаемой в журналах информации;
- сохранение отчетов в файл;
- интерактивный мониторинг событий.

Доступ к журналам предоставляется только администратору.

Подсистема журналирования 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 журналирования.

Подсистема аудита

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

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 журналирования 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 и удаление

ПО Secret Net Studio поставляется на установочном носителе в виде RPM- и DEB-пакетов.

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

Перед установкой Secret Net Studio 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 Studio.

Установка

Установка ПО Secret Net Studio

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 Studio. 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 Studio в зависимости от используемой операционной системы осуществляется с помощью установочных RPM- и DEB-пакетов:

Операционная система	Установочные пакеты
RPM-пакеты	
Альт Рабочая Станция/Сервер 10	sns-8.0-185.alt0.p10.x86_64.rpm
Альт 8 СП	sns-8.0-185.alt0.c9f2.x86_64.rpm
Ред ОС 7.3	sns-8.0-185.redos7.3.x86_64.rpm
AlterOS 7.5	sns-8.0-185.el7.alteros.x86_64.rpm
DEB-пакеты	
Astra Linux Special Edition 1.7.3	sns_8.0-185.astra1.7_amd64.deb
Astra Linux Special Edition 1.7.3.UU.1	sns_8.0-185.astra1.7.ci112_amd64.deb
Astra Linux Special Edition 1.7.3.UU.2	sns_8.0-185.astra1.7.ci162_amd64.deb
Astra Linux Special Edition 1.7.4	sns_8.0-185.astra1.7_amd64.deb sns_8.0-185.astra1.7.ci112_amd64.deb sns_8.0-185.astra1.7.ci162_amd64.deb

Внимание!
- Рекомендуется перед началом установки отключить хранитель экрана и выполнить процедуру установки от начала до конца без перерыва.
- Прежде чем выполнить установку ПО СЗИ Secret Net Studio на защищаемый компьютер с использованием сетевых репозиториев, необходимо убедиться в их доступности.
- Для Secret Net Studio реализована инициализация настроек из резервной копии при установке через переменное окружение. Переменным окружением является путь к резервной копии: SNTEMPLATE_ TARBALL=/tmp/<файл_ бэкапа>.tar.gz. При установке программа проверяет наличие резервной копии и получает необходимые настройки СЗИ.

Для установки Secret Net Studio:

1. Вставьте установочный носитель Secret Net Studio в устройство чтения или загрузите на компьютер дистрибутив Secret Net Studio. 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), AlterOS 7.5 (далее — AlterOS):
     ```
     #yum install ./<пакет sns>
     ```
   - для Astra Linux Special Edition (далее — Astra Linux):
     ```
     #apt update
     #apt install ./<пакет sns>
     ```
   - для Альт Рабочая станция/Сервер 10, Альт 8 СП (в системе должен быть установлен пакет lightdm-gtk-greeter-pd):
     ```
     #apt-get update
     #apt-get install ./<пакет sns>
     ```

   Результатом выполненных действий является установка Secret Net Studio 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

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

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 Studio.

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 Рабочая Станция/Сервер 10	sns-firewall-8.0-135.alt10.x86_64.rpm
Альт 8 СП	sns-firewall-8.0-135.alt8.x86_64.rpm
Ред ОС 7.3	sns-firewall-8.0-135.redos7.3.x86_64.rpm
AlterOS 7.5	sns-firewall-8.0-135.el7.alteros.x86_64.rpm
DEB-пакеты	
Astra Linux Special Edition 1.7.3	sns-firewall_8.0-135.astra1.7_x86-64_amd64.deb
Astra Linux Special Edition 1.7.3.UU.1	sns-firewall_8.0-135.astra1.7.ci112_amd64.deb
Astra Linux Special Edition 1.7.3.UU.2	sns-firewall_8.0-135.astra1.7.ci162_amd64.deb
Astra Linux Special Edition 1.7.4	sns-firewall_8.0-135.astra1.7_x86-64_amd64.deb sns-firewall_8.0-135.astra1.7.ci112_amd64.deb sns-firewall_8.0-135.astra1.7.ci162_amd64.deb

Для установки модуля ПМЭ Secret Net Studio:

1. Вставьте установочный носитель Secret Net Studio в устройство чтения. Запустите программу эмулятора терминала.
2. Перейдите в каталог, соответствующий установленной ОС. В зависимости от используемой ОС выполните команды:
   - для Ред ОС, AlterOS:
     ```
     #yum install ./<пакет sns-firewall>
     ```
   - для Astra Linux:

```
#apt update
#apt install ./<пакет sns-firewall>
```

- для Альт Рабочая станция/Сервер 10, Альт 8 СП:

```
#apt-get update
#apt-get install ./<пакет sns-firewall>
```

3. Перезагрузите компьютер.

Результатом выполненных действий является установка модуля персонального межсетевого экрана Secret Net Studio на защищаемом компьютере.

Удаление

Удаление ПО Secret Net Studio

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

Примечание.
- При удалении ПО Secret Net Studio в операционной системе сохраняется каталог /opt/securitycode/sns/ с файлами журналов установки/удаления СЗИ. Если после удаления Secret Net Studio эта информация больше не нужна, каталог и его содержимое можно удалить вручную.
- При удалении Secret Net Studio будут удалены зависимости ПМЭ.

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 sns
```

или

```
#yum remove sns
```

- для DEB-пакетов:

```
#dpkg -P sns
```

или

```
#apt remove sns
```

3. Перезагрузите компьютер.

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

Удаление персонального межсетевого экрана

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

Внимание!
Процедуру удаления ПМЭ Secret Net Studio 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 sns-firewall
```

или

```
#yum remove sns-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/securitycode/sns-firewall/var/log/suricata.

- для DEB-пакетов:

```
#dpkg -P sns-firewall
```

или

```
#apt purge sns-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 sns-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/securitycode/sns-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 Studio

В Secret Net Studio реализована возможность обновления программного обеспечения с Secret Net LSP версий 1.11 и 1.12 на текущую версию Secret Net Studio. Обновление ПМЭ возможно только с версии 1.12.

Для обновления ПО:

1. Вставьте установочный носитель Secret Net Studio в устройство чтения или загрузите на компьютер дистрибутив Secret Net Studio. Запустите программу эмулятора терминала.
2. Перейдите в каталог, соответствующий установленной ОС:
   - для ОС Astra Linux выполните команды:

     ```
     chmod +x upgrade_to_sns.sh
     upgrade_to_sns.sh /<путь_к_пакету_sns> /<путь_к_пакету_fw>
     ```

     Не указывайте <путь_к_пакету_fw> при обновлении с Secret Net LSP версии 1.11.
   - для остальных поддерживаемых ОС обновление выполняется так же, как и установка. Выполните процедуру установки Secret Net Studio при установленном пакете Secret Net LSP.
3. Перезагрузите компьютер.

Глава 3
Эксплуатация Secret Net Studio с помощью командной строки

Утилиты Secret Net Studio

В данном разделе содержится описание специализированных утилит, используемых в защитных подсистемах Secret Net Studio, 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 пользователями и персональными идентификаторами;
- управление взаимодействием с комплексом "Соболь";
- затирание оперативной памяти и остаточных данных;
- контроль устройств;
- контроль целостности объектов файловой системы;
- контроль печати;
- настройка правил аудита;
- работа с лицензиями;
- настройка замкнутой программной среды;
- управление режимом аутентификации;
- настройка централизованного управления;
- резервное копирование;
- работа с журналами.

Утилиты расположены в каталогах /opt/securitycode/sns/bin и /opt/securitycode/sns/sbin.

Примечание.
Управление работой защитных механизмов и политик с помощью командной строки выполняется администратором, обладающим правами суперпользователя компьютера.

Настройка параметров политик

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

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

Ключ		Описание
-h	--help	Выводит справочную информацию о применении команды
-l	--list	Выводит список плагинов с указанием политик и состоянием их параметров
-e	--export <путь>	Экспортировать политики в файл с путем <путь>
-i	--import <путь>	Импортировать политики из файла с путем <путь>
-f	--filter <плагин>, <политика>, <параметр>	Установить фильтр для операции экспорта/импорта. Возможные настройки <плагин>,<политика>,<параметр> указаны ниже
-p	--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
-c	--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; • data_wipe — затирание данных; • devices_control — контроль устройств; • firewall — межсетевой экран; • services — установка сервисов; • system — системные настройки; • authentication — параметры идентификации и аутентификации; • users — управление настройками паролей пользователей

Ключ		Описание
-c	--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; • ram — очистка оперативной памяти; • local_drives — затирание диска; • verbose — детализация сообщений; • block_inv_packets — блокировка ошибочных пакетов; • snauditd — сервис аудита; • snjournald — сервис журналирования; • snnetwork — сервис удаленного управления; • snconnectd — сервис подключения к серверу Security Code Orchestrator; • clear_log — перезапись журнала при переполнении; • system_lock — сервис блокировки системы при нарушении ФК; • max_log_severity — минимальная критичность сообщений в журнале тревог для отправки журнала; • ident — метод идентификации; • strength — усиленная аутентификация; • lock — реакция на изъятие идентификатора; • cache — кешировать данные идентификатора для доменных пользователей; • deny — блокировать после указанного количества 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 в систему; • 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. Доступные значения для перечисленных параметров указаны ниже

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 ГОСТ R 34.11-2012; 2 — алгоритм SHA-512. Значение по умолчанию
control	access_control	mode	0 — выключено; 1 — включено
	data_wipe	state	0 — выключено; 1 — включено
		ram	0 — выключено; 1 — включено
		local_drives	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
		block_inv_packets	0 — выключено; 1 — включено
service_mgr	services	snauditd	0 — выключено; 1 — включено
		snjournald	0 — выключено; 1 — включено
		snnetwork	0 — выключено; 1 — включено
		snconnectd	0 — выключено; 1 — включено

Плагин	Политика	Параметр	Значение
system	system	clear_log	0 — выключено; 1 — включено
		system_lock	0 — выключено; 1 — включено
		max_log_severity	<число> — числовой уровень критичности сообщения в журнале, где: 0 — очень важное ("emerg"); 1 — тревога ("alert"); 2 — критическое ("crit"); 3 — ошибка ("err"); 4 — предупреждение ("warning"); 5 — замечание ("notice"); 6 — информация ("info"); 7 — отладка ("debug")
token_mgr	authentication	state	0 — выключено; 1 — включено
		ident	0 — логин введен с клавиатуры; 1 — логин определен персональным идентификатором; 2 — смешанный (используется клавиатура или персональный идентификатор). Значения "1" и "2" недоступны для ОС Astra Linux
		strength	0 — выключено; 1 — включено
		lock	0 — не блокировать; 1 — блокировать станцию при изъятии любого идентификатора; 2 — блокировать станцию при изъятии USB-идентификатора. Значения "1" и "2" недоступны для ОС Astra Linux
		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 users -c users,min_passwd_size,10	Установить значение параметра "Минимально допустимая длина для нового пароля" — "10" символов
snpolctl -l	Показать все политики
snpolctl -i /home/user/policy.tmpl	Импортировать все политики из файла '/home/user/policy.tmpl'
snpolctl -e policy.tmpl -f token_mgr	Экспортировать политики из плагина 'token_mgr'
snpolctl -e policy.tmpl -f control -f users,users,min_passwd_size	Экспортировать все политики из плагина 'token_mgr' и политику 'min_passwd_size' из плагина 'users'

Управление персональными идентификаторами

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

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

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	--bind <имя_ пользователя>	Привязывает новый идентификатор к пользователю. Не используется с ключами "-P", "-K", "-c", "-L", "-U" и "-u"
-c	--change <имя_ пользователя>	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" и "-t"
-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, потребуется предъявить идентификатор, в котором хранится закрытый ключ . Вход с закрытым ключом на идентификаторе станет возможным только по идентификатору
-E	--enable-sable	Разрешает работу персональных идентификаторов с комплексом "Соболь". Используется с ключами "-b" и "-p"
-A	--bind-sable-admin	Привязывает персональный идентификатор администратора комплекса "Соболь". Используется с ключами "-b" и "-p"
-s	--serial <номер>	Выполняет операцию с идентификатором с указанным серийным номером. Используется с ключами "-u", "-P", "-K", "-r", "-L", "-U" и "-R"
-P	--add-password	Добавляет пароль на уже привязанный идентификатор. Не используется с ключами "-b", "-R", "-L", "-U" и "-u"
-K	--add-key	Добавляет 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"

Ключ		Описание
-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 комплекс "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 Studio 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 комплекс "Соболь"
sntokenctl -b test_user -p -A	Привязать персональный идентификатор администратора комплекса "Соболь" для пользователя test_user и записать в идентификатор пароль
sntokenctl -s 12345678 -D	Запретить вход в комплекс "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 комплексом "Соболь" в режиме интеграции с Secret Net Studio

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

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

Ключ		Описание
-h	--help	Вывести справочную информацию о применении утилиты
-c	--connect	Подключить комплекс "Соболь" к Secret Net Studio
-d	--disconnect	Отключить комплекс "Соболь" от Secret Net Studio
-s	--status	Отобразить текущее состояние взаимодействия комплексом "Соболь" и Secret Net Studio
-n	--network	Включить режим удаленного управления комплекса "Соболь". Используется с опцией -c
-l	--login <имя_пользователя>	Задать логин администратора домена. Используется с опцией -n
-p	--password <пароль>	Задать пароль администратора домена. Используется с опцией -n
-r	--remove-users	Запретить доступ к комплексу "Соболь" для всех локальных пользователей

Ключ		Описание
-a	--copy-admin-token	Копировать идентификатор администратора комплекса "Соболь". До окончания копирования идентификатора необходимо наличие подключенного идентификатора администратора комплекса "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 комплекса "Соболь" и Secret Net Studio
snsablectl -c -n -l DOMAIN\\Petrov	Выполняется включение удаленного режима управления для администратора домена. После выполнения команды необходимо ввести пароль

Управление шаблонами контроля целостности комплекса "Соболь"

Для управления шаблонами контроля целостности комплекса "Соболь" используется утилита **snscheck**, расположенная в каталоге /opt/securitycode/sns/bin. Утилита выполняет действия в режиме командной строки от имени текущего пользователя.

Ключ		Описание
-h	--help	Вывести справочную информацию о применении утилиты
--generate-report <файл>		Сгенерировать отчет об объектах на контроле целостности в формате rtf <файл> — имя файла для сохранения отчета
Информация:		
--ls-drives		Вывести список доступных дисков
--ls-path		Вывести путь к папке с шаблонами
--ls-system-smbios		Вывести список таблиц SMBIOS в системе
--ls-system-pci		Вывести список PCI-устройств в системе
Настройки контроля целостности файлов:		
--ls-files		Вывести список файлов на контроле целостности
--add-file <файл>		Поставить файл на контроль целостности
--add-ls-files <список>		Поставить список файлов на контроль целостности
--rm-file <файл>		Снять файл с контроля целостности
--rm-ls-files <список>		Снять список файлов с контроля целостности
--clear-files		Снять все файлы с контроля целостности
Настройки контроля целостности секторов:		
--ls-sectors		Вывести список секторов на контроле целостности
--add-sector <файл>		Поставить сектор на контроль целостности
--add-ls-sectors <список>		Поставить список секторов на контроль целостности
--rm-sector <файл>		Снять сектор с контроля целостности
--rm-ls-sectors <список>		Снять список секторов с контроля целостности
--clear-sectors		Снять все секторы с контроля целостности

Ключ	Описание
Настройки контроля целостности SMBIOS:	
--ls-smbios	Вывести список таблиц и полей SMBIOS на контроле целостности
--add-smbios <значение>	Возможные значения: • "SMBIOS" — поставить все таблицы SMBIOS на контроль целостности; • <название_таблицы> — поставить таблицу SMBIOS на контроль целостности; • <название_поля_таблицы> — поставить поле таблицы SMBIOS на контроль целостности
--add-ls-smbios <список>	Поставить список объектов SMBIOS на контроль целостности
--rm-smbios <значение>	Возможные значения: • "SMBIOS" — снять все таблицы SMBIOS с контроля целостности; • <название_таблицы> — снять таблицу SMBIOS с контроля целостности; • <название_поля_таблицы> — снять поле таблицы SMBIOS с контроля целостности
--rm-ls-smbios <список>	Снять список объектов SMBIOS с контроля целостности
--clear-smbios	Снять все объекты SMBIOS с контроля целостности
Настройки контроля целостности PCI-устройств:	
--ls-pci	Вывести список PCI-устройств на контроле целостности
--add-pci <значение>	Возможные значения: • "PCI" — поставить все PCI-устройства на контроль целостности; • <название_устройства> — поставить PCI-устройство на контроль целостности
--add-ls-pci <список>	Поставить список PCI-устройств на контроль целостности
--rm-pci <значение>	Возможные значения: • "PCI" — снять все PCI-устройства с контроля целостности; • <название_устройства> — снять PCI-устройство с контроля целостности
--rm-ls-pci <список>	Снять список PCI-устройств с контроля целостности
--clear-pci	Снять все PCI-устройства с контроля целостности

Контроль устройств

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

Ключ		Описание
-h	--help	Показывает доступные команды
-A	--all-bus-class	Показывает список доступных шин/классов
-U	--usb-uid-models	Показывает список поддерживаемых электронных идентификаторов и считывателей смарт-карт
-r	--rules	Отображает правила
-a	--add	Добавляет устройство. Необходимо указать параметр '--bus-class' и другие параметры в зависимости от типа устройства
-m	--model	Добавляет модель. Необходимо указать параметры '--vid', '--pid', и '--bus-class'
-s	--set	Устанавливает параметры для шины/класса/модели/устройства
-c	--config	Проверяет и утверждает аппаратную конфигурацию
-i	--import	Импортирует устройства и модели из csv-файла

Параметры для команд:

Параметр		Описание
-b	--bus-class	Идентификатор шины/класса (для команд --rules, --set, --add, --model)
--comment		Комментарий (для команд --set, --add, --model)

Параметры для команды --rules:

Параметр	Описание
--show-acl	Показать все ACL-таблицы
--show-dc	Показать все DC-таблицы
--show-acl-bus-class	Показать ACL-таблицу для шин/классов
--show-acl-mod-dev	Показать ACL-таблицу для моделей/устройств
--show-dc-bus-class	Показать DC-таблицу для шин/классов
--show-dc-mod-dev	Показать DC-таблицу для моделей/устройств
--show-dc-net	Показать DC-таблицу для сетевых адаптеров

Параметры для команд --rules, --set:

Параметр	Описание
--dev-id	Идентификатор устройства
--model-id	Идентификатор модели

Параметры для команды --set:

Ключ		Описание
-u	--user=<пользователь>:<правило>	Данные пользователя
-g	--group=<группа>:<правило>	Данные группы
--default=<правило>		Правило разграничения доступа для группы BCE Описание параметра RULE: • none — нет доступа; • read — только чтение; • write — чтение и запись; • delete — удалить ACL-правила у устройства; • delete-child — удалить ACL-правила для всех дочерних классов, моделей и устройств
--dc=<DC_правило>		DC-правило Описание параметра <DC_правило>: • delete — удалить DC-правило; • delete-child — удалить DC-правила для всех дочерних классов, моделей и устройств; • not-control — подключение не контролируется; • enabled — подключение разрешено; • fixed — устройство подключено постоянно; • lock — блокировать станцию при изменении состояния устройства; • disabled — подключение запрещено. Подробное описание правил приведено в таблице ниже

Параметр	Описание
Устройство не контролируется (**not-control**)	Для объекта отключен режим контроля. Изменение состояния устройства не отражается в журнале
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

Параметр	Описание
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)
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

Параметры для команд --add, --model:

Параметр	Описание
--to-acl	Добавить в ACL-таблицу
--to-dc	Добавить в DC-таблицу

Параметры для команды --add:

Параметр	Описание
--system-id	Идентификатор устройства в системе
--vid	Идентификатор производителя
--pid	Идентификатор продукта
--vendor	Производитель
--product	Описание устройства
--serial	Серийный номер

Параметры для добавления только сетевых адаптеров:

Параметр	Описание
--net-type	Тип сетевого адаптера (pci, usb, virtual, other)
--subsys-vid	Идентификатор производителя PCI-подсистемы
--subsys-pid	Идентификатор продукта PCI-подсистемы
--pci-class	PCI-класс
--pci-revision	PCI-ревизия
--pci-slot	PCI-слот
--virtual-type	Тип виртуального сетевого адаптера (пустой, bridge, tun, tap)
--mac	MAC-адрес (только для виртуальных и других сетевых адаптеров)

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 --rules	Показать все таблицы правил
sndevctl --rules --show-acl	Показать таблицы ACL-правил
sndevctl --rules --show-acl-mod-dev --show-dc-mod-dev	Показать все таблицы моделей/устройств
sndevctl --rules --bus-class=usb_storage	Показать правила для шины/класса
sndevctl --rules --dev-id=100	Показать правила устройства по идентификатору
sndevctl --add --to-acl --bus-class=usb_storage --vid="8564" --pid="1000" --vendor="JetFlash" --product="Transcend_8Gb" --serial="3537946797"	Добавить USB-устройство в ACL-таблицу
sndevctl --add --to-dc --bus-class=net_ethernet --net-type=pci --vid="1234" --pid="45ab" --vendor="D-Link" --product="Gigabit Ethernet Controller" --comment="ethernet adapter" --pci-class=020000 --subsys-vid=acdf --subsys-pid=09e3 --pci-revision=04 --pci-slot=0000:00:03.0	Добавить сетевой PCI-адаптер
sndevctl --add --to-dc --bus-class=net_wifi --net-type=usb --vid="9876" --pid="ab34" --vendor="TP-LINK" --product="Wi-Fi Controller" --serial="qdV-67" --comment="Archer Wi-Fi"	Добавить сетевой USB-адаптер
sndevctl --add --to-dc --bus-class=net_ethernet --net-type=virtual --virtual-type="" --mac=dc:35:71:a2:f3:b5 --comment="VPN Continent Connection" --vendor="Security Code" --product="Continent"	Добавить сетевой виртуальный адаптер
sndevctl --add --to-dc --bus-class=net_bluetooth --net-type=other --mac=01:23:45:67:89:ab --comment="Unknown Phy" --vendor="Unknown Vendor" --product="Unknown Product"	Добавить другой сетевой адаптер
sndevctl --model --to-acl --to-dc --bus-class=usb_storage --vid="8564" --pid="1000" --product="Transcend_8Gb" --comment="Transcend Flash Drive"	Добавить модель в ACL- и DC-таблицы
sndevctl --model --to-dc --dev-id=1 --comment=NAME	Создать модель по устройству и добавить в DC-таблицу
sndevctl --set --dev-id=1 --comment="Kingston" --user=test:write --group=test:read --default=none	Добавить ACL-правила для устройства и изменить комментарий
sndevctl --set --bus-class=usb_hid --dc=fixed	Установить DC-правило для шины или класса
sndevctl --set --model-id=201 --dc=delete --user=test:delete --group=test:delete	Удалить DC-правило и некоторые ACL-права для модели
sndevctl -i Devices.csv	Импортировать устройства и модели из CSV-файла

Работа с CSV-файлами

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

```
touch ИМЯ_ФАЙЛА.csv
```

Csv-файл должен заполняться по шаблонам:

- шаблон для устройств — SnDeviceAd.csv;

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

- шаблон для сетевых устройств — SnNetDeviceAd.csv.

```
Serial Number;Manufacturer;Description;PID;VID;Device Class;Comment;Net Type;
PCI-class;Subsys VID;Subsys PID;PCI-revision;PCI-slot;Interface Type;MAC
```

Примечание.
Шаблоны для заполнения csv-файла поставляются с пакетом Secret Net Studio и располагаются в каталогах:
- шаблон для устройств — /opt/securitycode/sns/share/device_templates/SnDeviceAd.csv;
- шаблон для сетевых устройств — /opt/securitycode/sns/share/device_templates/SnNetDeviceAd.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 идентификаторы и считыватели
1299	Прочие
1500	Карточки памяти
1306	Физические диски
1304	Оптические диски
1301	Последовательные порты
1302	Параллельные порты
1600	Соединение Ethernet
1601	Беспроводное соединение (WiFi)
1602	Соединение Bluetooth
1603	Соединение 1394 (Fireware)
1604	Инфракрасное соединение (IrDA)

Пример заполнения csv-файла:

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

Для добавления 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/securitycode/sns/bin.

Ключ		Описание
-c	--check	Выполняет контроль целостности. Если указана данная опция, остальные опции учитываться не будут
-i	--init	Проводит инициализацию базы 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: csopmi bl [R] <объект> 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
-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 записывать любые изменения файла; • NORMALBACK — обнаруживать, записывать и отменять любые изменения файла (восстановить файл из резервной копии); • NORMALLOCK — если файл изменен, записывать событие и заблокировать систему; • NORMALBACKLOCK — восстановить измененный файл и заблокировать систему; • [csopmibl] — установить опции полноты КЦ и действий (как в ключе --list)
-r	--real-time	Устанавливает контроль целостности в реальном времени для всех объектов в данном запросе. Используется с действием --set
-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
-a	--add-schedule-entry '<мм чч дд мес дн>'	Добавляет новую запись в расписание КЦ в формате cron, где: • мм — минуты (диапазон: 0–59); • чч — часы (диапазон: 0–23); • дд — день (диапазон: 1–31); • мес — месяц (диапазон: 1–12); • дн — день недели (диапазон: 0–6. 0 — воскресенье). Вместо неиспользуемых параметров используйте символ *
-d	--delete-schedule-entry <номер>	Удаляет запись под определенным номером из расписания КЦ

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=[csl]	Включить контроль для файлов 'file1' и 'file2' с флагами 'NORMAL' и [checksum + size + lock] соответственно
snaidectl -s file1=NORMALBACK -r	Включить контроль в реальном времени для файла 'file1' с флагом NORMALBACK
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 '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

Функциональный контроль

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

Проверка целостности компонентов СЗИ выполняется автоматически при загрузке ОС до старта Secret Net Studio. 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 с помощью утилиты **snunblock**.

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

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

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/securitycode/sns/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 установить значение 1.

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

Запуск утилиты осуществляется в режиме командной строки командой #/opt/securitycode/sns/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 Studio
-t	--test	Полная проверка целостности компонентов Secret Net Studio и сервисов

Правила аудита

Для просмотра и редактирования правил аудита используется утилита **snauditctl**, расположенная в каталоге /opt/securitycode/sns/bin.

Ключ		Описание
-l	--list	Показывает текущие правила аудита
-A	--add	Создает правила аудита, а также позволяет добавить субъектов в существующие правила
-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
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/securitycode/sns/bin.

Ключ		Описание
-s	--status	Отображает текущий статус лицензии
-c	--change <путь_к_файлу_лицензии>	Изменяет текущую лицензию

Ключ		Описание
-d	--delete <название_компонента>	Удаляет текущую лицензию для компонента
-n	--name <название_компонента>	Используется для замены лицензии компонента
-h	--help	Отображает доступные команды для утилиты

Примечание.
Невозможно удалить лицензию для модуля CORE.

В Secret Net Studio предусмотрено централизованное управление лицензиями через СБ SNS.

В случае истечения срока лицензии Secret Net Studio перейдет в "Ограниченный режим". Большая часть функционала будет недоступна. Для продолжения эксплуатации Secret Net Studio необходимо удалить или заменить лицензию с истекшим сроком либо отключить компонент.

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/securitycode/sns/bin. Строка команды имеет следующий формат:

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

Описание аргументов представлено в таблице ниже:

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	--name <название_правила>	Выводит пользовательское правило с указанием имени, режима, статуса, списка пользователей, групп и ресурсов
-u	--user <имя_пользователя>	Выводит правила, действующие для конкретного пользователя
-g	--group <название_группы>	Выводит правила, действующие для конкретной группы
-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	--name <название_правила>	Добавление нового правила. По умолчанию правило создается со статусом "True", с режимом "Standart", с пустым списком ресурсов и разрешенным для всех пользователей системы
-u	--user <имя_пользователя>	Добавление нового пользователя в белый список. Если использовать с ключом '-n', пользователь будет добавлен в правило, а не в белый список
-g	--group <название_группы>	Добавление новой группы в белый список. Если использовать с ключом '-n', группа будет добавлена в правило, а не в белый список
-r	--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. Используется с ключами '-n', 'r', 'f'
-R	--recursive	Добавление ресурсов в правило рекурсивно. Используется с ключами '-n', 'r'
-f	--resource-file <имя_ресурсного_файла>	Добавление экспортированного ресурсного файла с правилами. Используется с ключом '-n'
-C	--force	Не спрашивать подтверждение
-D	--disable	Добавление нового правила в выключенном режиме. Ключ можно использовать только для создаваемого правила
-X	--extended	Добавление нового правила расширенного типа. Ключ можно использовать только для создаваемого правила

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	--name <название_правила>	Удаление правила с указанием его имени
-r	--resource <путь_к_ресурсу>	Удаление из правила ресурсов. Правило может остаться с пустым списком ресурсов
-u	--user <имя_пользователя>	Удаление пользователя из правила. Если использовать без ключа '-n', пользователь будет удален из белого списка
-g	--group <название_группы>	Удаление группы из правила. Если использовать без ключа '-n', группа будет удалена из белого списка
-C	--force	Не спрашивать подтверждение
-A	--all-rules	Удаление всех правил

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	--name <название_правила>	Обновление правила
-u	--user <имя_пользователя>	Обновление списка пользователей, для которых действует правило
-g	--group <название_группы>	Обновление списка групп, для которых действует правило
-r	--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. Используется с ключами '-n', 'r', 'f'
-R	--recursive	Обновление ресурсов в правиле рекурсивно. Используется с ключами '-n', 'r'
-f	--resource-file <имя_ресурсного_файла>	Обновление ресурсного файла json-формата в правиле. Используется с ключом '-n'
-C	--force	Не спрашивать подтверждение
-a	--all-users	Разрешение действия правила для всех пользователей системы. Используется с ключом '-n'. Не может использоваться с ключами '-u', '-g'

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	--name <название_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

Ключ		Описание
-n	--name <название_ 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	--name <назание_ 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 -N	--name <название_правила> --new-name <новое_ название_ 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 -f	--name <название_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
-C	--force	Не спрашивать подтверждение

Ключ		Описание
-l	--list	Выводит список всех пользователей и групп, для которых в журнале аудита зарегистрированы события ЗПС
-n	--name <название_правила>	Задает правило ЗПС с указанием его имени и сохраняет в правиле ресурсы, для которых в журнале аудита зарегистрированы события ЗПС
-f	--resource-file <имя_файла>	Сохраняет ресурсы, запущенные пользователем, в файл с указанием его имени
-G	--auto-generation	Автоматически генерирует правила для каждого пользователя или группы в журнале. Для того чтобы автоматически генерировать правила только для каждой группы в журнале, используйте ключ --by-group
-u	--user <имя пользователя>	Задает правило ЗПС с указанием имени конкретного пользователя, для которого действует правило и по имени которого будет фильтроваться журнал аудита
-g	--group <название_группы>	Задает правило ЗПС с указанием имени группы пользователей, для которой действует правило и по имени которой будет фильтроваться журнал аудита
-e	--exec-file <путь_к_исполняемому_файлу>	Задает правило ЗПС с указанием исполнямого 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"
-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"
-A	--add-non-exec	Добавляет неисполняемые файлы. По умолчанию добавляются только исполняемые файлы и разделяемые библиотеки

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 подключения к серверу безопасности SNS

Для настройки подключения к СБ SNS используется утилита **snnetctl**, расположенная в каталоге /opt/securitycode/sns/bin. Компьютер должен быть включен в домен и подчинен СБ SNS в структуре управления.

Примечание.
Для подключения к СБ SNS рекомендуется использовать сервисную доменную учетную запись с неограниченным сроком пароля и с минимальными правами в домене.

Ключ		Описание
-e	--enable	Включает режим удаленного управления. В обязательном порядке также необходимо указать параметры -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. Используется к ключом '-e'
-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 Используется к ключом '-u'
-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

Настройка подключения к серверу Security Code Orchestrator

Для настройки подключения к серверу Security Code Orchestrator используется утилита **snconnctl**, расположенная в каталоге /opt/securitycode/sns/bin.

Ключ		Описание
-r	--registration	Регистрирует продукт на сервере. Используется с параметрами, указанными в таблице ниже
-D	--delete	Удаляет продукт с сервера
-R	--renewal	Перевыпускает сертификат агента
-k	-keys_gen	Создает закрытый и открытый ключи
-s	--show	Отображает текущие настройки подключения к серверу
-h	--help	Отображает справку. Используется с параметрами -r, -D, -R, -k, -s

Параметры для команды --registration:

Параметр		Описание
-n	--name <имя>	Название агента. Значение по умолчанию — имя хоста
-d	--description <описание>	Описание объекта
-t	--token <токен>	Токен делегирования
-f	--token_file <путь>	Путь к файлу, содержащему токен делегирования
-i	--ip <IP-адрес>	IP-адрес
-O	--port <порт>	Порт. Значение по умолчанию — "443"

-C	--certificate <путь>	Путь к сертификату сервера

Примеры команд:

snconnctl --registration --ip=<ip-адрес>	Регистрация продукта на сервере
snconnctl -h -r	Показать справку для регистрации продукта на сервере
snconnctl -s	Отобразить текущие настройки подключения к серверу

Резервное копирование настроек Secret Net Studio

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

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 Studio; • 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 Studio; • 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" 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"
-i	--id <ID>	Указывает ID резервной копии. Используется совместно с опциями "-r", "-d" , "-e" и "-m"
-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 Studio

Примеры команд:

snbckctl -b	Выполняет полное резервное копирование

snbckctl -r -i 10 -L	Выполняет полное восстановление, включая лицензию, из резервной копии с ID 10
snbckctl --backup=snsettings	Выполняет резервное копирование настроек Secret Net Studio
snbckctl -i 11 --restore=policies	Восстанавливает политики из резервной копии с ID 11

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/securitycode/sns/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
-r	--result=<результат>	Просмотр/экспорт записи с определенным результатом. Принимает числовой результат: "Ошибка" (0), "Успешно" (1). Работает только с базой данных событий аудита
-v	--verbose	Вывод отладочных сообщений

Работа со сторонним syslog-сервером

Для работы со сторонним syslog- сервером для передачи данных журнала используется утилита **snjournaldctl**, расположенная в каталоге /opt/securitycode/sns/bin. Утилита настраивает отправку журналов на сторонний syslog-сервер и на сервер Security Code Orchestrator.

Ключ		Описание
-h	--help	Отображает доступные команды
-l	--list	Отображает список удаленных серверов журналов
-d	--del <номер>	Удаляет сервер журнала с переданным порядковым номером
-D	--delall	Удаляет все серверы журналов
--shedule		Изменяет расписание в формате cron
--add		Добавляет новый сервер журналов

Параметры для команды --add:

Параметр		Описание
--host <IP-адрес>		IP или hostname сервера журналов
-p	--port <порт>	Порт сервера

Параметры для команды --shedule:

Параметр		Описание
-s	--set <cron>	Установить расписание отправки логов в cron формате
-c	--clear	Очистить расписание и установить отправку журналов по изменению

Примечание.
Минимальная критичность сообщений в журнале для отправки на syslog-сервер настраивается с помощью политики **system**, параметр **max_log_severity** (см. стр. 28).

Примеры команд:

snjournaldctl --add --host 193.212.222.35 -p 333	Добавить сервер журнала
snjournaldctl -d 2	Удалить сервер журнала
snjournaldctl --shedule -s "*/2 * * * * *"	Изменить расписание отправки журналов

Экспорт и импорт настроек Secret Net Studio

Для экспорта настроек:

1. Выполните резервное копирование настроек Secret Net Studio:

   ```
   #snbckctl -b
   ```

   или

   ```
   #snbckctl --backup
   ```

   Конфигурация сохраняется в каталоге /opt/securitycode/sns/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/securitycode/sns/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 Studio предыдущих версий в текущую версию Secret Net Studio

С помощью утилиты **snbckctl**, расположенной в каталоге /opt/securitycode/sns/bin, можно выполнить сохранение конфигурации Secret Net Studio предыдущих версий и ее перенос в Secret Net Studio 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 Studio. Для этого в командной оболочке выполните команду:

   ```
   #snbckctl -b
   ```

   Конфигурация сохраняется в каталоге /opt/securitycode/sns/usr/backup/<ID>, где <ID> — это сгенерированный системой номер резервной копии.
3. Экспортируйте резервную копию для создания архива. Для этого в командной оболочке выполните команду:

   ```
   #snbckctl -e
   ```
4. Скопируйте экспортированный архив резервной копии в папку пользователя.
5. Удалите Secret Net Studio предыдущей версии (см. стр. **25**).
6. Обновите ОС до необходимой версии ядра.
7. Установите текущую версию Secret Net Studio (см. стр. **23**).
8. Импортируйте архив резервную копии в каталог /opt/securitycode/sns/usr/backup. Для этого в командной оболочке выполните команду:

   ```
   #snbckctl -m
   ```
9. 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 SNS>
   ```

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

Персональный межсетевой экран

Персональный межсетевой экран представляет собой компонент СЗИ Secret Net Studio, предназначенный для защиты серверов и рабочих станций от несанкционированного доступа и разграничения сетевого трафика 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;
- 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 Studio (подробнее см. стр. **24**, стр. **25**).

Персональный межсетевой экран является локальным компонентом СЗИ Secret Net Studio. 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 правилами фильтрации посредством СБ SNS.

Для выполнения процедур настройки ПМЭ используется утилита **fw-localcfg**. Описание утилиты и особенности ее применения приведены на стр. **54**.

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 Studio.

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

Общий порядок настройки

Настройка персонального межсетевого экрана выполняется в следующем порядке:

1. Получение информации о работоспособности механизма (см. стр. **53**).
2. Вывод справочной информации о применении утилиты настройки ПМЭ (см. стр. **60**).
3. Настройка персонального межсетевого экрана на основе правил (см. стр. **59**).
4. Настройка регистрации событий ПМЭ (см. стр. **64**).
5. Настройка блокировки ошибочных пакетов (см. стр. **65**).

Примечание.
Настройка и управление персональным межсетевым экраном Secret Net Studio 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 включения и отключения используются политики Secret Net Studio.

Получение текущего статуса работоспособности ПМЭ

Запустите программу эмулятора терминала и выполните команду:

```
systemctl status sns-firewall
```

Перезагрузка ПМЭ

Запустите программу эмулятора терминала и выполните команду:

```
systemctl restart sns-firewall
```

Отключение ПМЭ

Для отключения ПМЭ необходимо отключить политику Secret Net Studio.

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

Включение ПМЭ

Для включения ПМЭ необходимо включить политику Secret Net Studio.

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

Утилиты ПМЭ Secret Net Studio

Для выполнения настройки персонального межсетевого экрана (см. стр. **59**) 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 таблице ниже.

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 Studio необходимо включать в состав правил обязательный набор следующих параметров: --action, --protocol, --msg.

Команда add и modify

Команда add добавляет новые правила настройки межсетевого экрана.

Команда modify изменяет существующее правило настройки межсетевого экрана с обязательным указанием параметра id правила.

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; • allow — пропустить сетевой пакет на следующий уровень

Параметр	Описание
--protocol=<protocol>	Добавление протоколов, на основании которых осуществляется фильтрация сетевых пакетов. Допустимые значения параметра --proto: • tcp; udp; ip; icmp; ftp; tls; dns; dcerpc; ssh; imap; modbus; dnp3; enip; nfs; ikev2; krb5; ntp; dhcp; rfb; snmp; smtp, tftp; sip; egp; hmp; xns-idp; rdp; rvd; http2; smb; http; • номер — 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 значениями --alarm=true и --audit=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. Допустимые значения параметра --icmp_code: 0-255, *. Символ * (звездочка) является значением по умолчанию для параметра. 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
--local_addrs=<IP, IPsubnet/MASK, IP1-IP2, IP3,..., IPn>	Добавление IP-адресов отправителей. В качестве значения параметра --local_addrs укажите IP-адрес компьютера или 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	Описание
--remote_addrs=<IP, IPsubnet/MASK, IP1-IP2, IP3,..., IPn>	Добавление IP-адресов получателей. В качестве значения параметра --remote_addrs укажите IP-адрес компьютера или маску подсети, чтобы задать допустимый набор 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)
--schedule=<strValue>	Добавление фильтрации сетевого трафика с учетом расписания. Строковые значения параметра --schedule имеют следующий формат: <hour_range> <day_range> [# ...] • <hour_range> — диапазон часов; • <day_range> — диапазон дней. 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> 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 или групп пользователей
--objects=<strValue>	Определяет папки общего доступа или 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	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>	Кодировка символов, используемая при фильтрации 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 --remote_
addrs=10.0.0.0/24,192.168.10.0/8 --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
--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 предусмотрен следующий параметр:

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 выполните команду:

```
systemctl restart sns-firewall
```

Команда export

Команда export осуществляет экспорт существующих правил настройки персонального межсетевого экрана. Архивный файл резервной копии сохраняется в каталоге /opt/securitycode/sns-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	Вывод правила с заданным id
--all	Вывод 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 ПМЭ предусмотрено использование утилиты **fw-net**.

Описание аргументов, применимых к утилите, представлено в таблице ниже.

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 таблице ниже.

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 Studio 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. **60**);
- создает новые правила (см. стр. **60**);
- изменяет существующие правила (см. стр. **60**);
- удаляет существующие правила (см. стр. **60**);
- импортирует настройки ПМЭ из архивного файла резервной копии (см. стр. **61**);
- экспортирует правила в архивный файл резервной копии (см. стр. **61**);
- осуществляет вывод информации о существующих правилах (см. стр. **61**);
- осуществляет блокировку ошибочных пакетов (см. стр. **65**).

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 параметрам правил;
- фильтрация по контролю доступа к ресурсам, содержащим скрипты;
- контроль доступа к именованным каналам 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. **54**.

Вывод справочной информации о применении утилиты ПМЭ

Пояснение.
В Secret Net Studio 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. **54**.

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. **54**.

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.

Экспорт правил персонального межсетевого экрана

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

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. Файл сохраняется в каталоге /opt/securitycode/sns-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 файла:

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

Импорт правил персонального межсетевого экрана

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

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 файла.

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 sns-firewall
```

Вывод сводной 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. **54**.

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 Studio.

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

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

Фильтрация сетевого трафика

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 направления трафика и сетевого интерфейса;
- фильтрация с учетом прав доступа;
- фильтрация с учетом расписания.

Внимание!
Средства Secret Net Studio 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 Studio.

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. **60**) или изменении существующих (подробнее см. стр. **60**) включите в состав правила параметр **--proto**. В качестве значения параметра укажите название протокола, на основании которого осуществляется настройка фильтрации (подробнее см. стр. **54**).

   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. **60**) или изменении существующих (подробнее см. стр. **60**) включите в состав правила параметр **--proto**. В качестве значения параметра укажите название протокола, на основании которого осуществляется настройка фильтрации (подробнее см. стр. **54**).

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 Studio регистрируется соответствующее событие. В случае попытки обмена данными по протоколу TCP, в журнале аудита Secret Net Studio 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 Studio предусмотрено использование утилиты **fw-net**.

Просмотр и принудительное завершение TCP-соединений

Для просмотра и принудительного разрыва выбранных TCP-соединений в Secret Net Studio используется утилита **fw-net**. Описание утилиты и особенности ее применения приведены на стр. **59**.

Примеры:

Пример 1. Настройка блокировки передачи файлов по протоколу FTP

Создание правил, блокирующих отправку файлов по протоколу FTP.

```
fw-localcfg --add --action=drop --proto=ftp --msg='Drop_ftp' --audit=true
```

Пример 2. Настройка блокировки JavaScript

Создание правила, блокирующего загрузку файлов с расширением 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.

```
fw-localcfg --add --action=drop --proto=http --msg='Drop_http' --audit=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. **60**) или изменении существующих (подробнее см. стр. **60**) включите в состав системного правила параметр **--proto** и укажите значение **icmp** (подробнее см. стр. **54**).

   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. **54**).

   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. **54**).

   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 Studio. 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 Studio.

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

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. **54**.

Для включения регистрации событий срабатывания правила ПМЭ:

1. Запустите программу эмулятора терминала.
2. При добавлении новых правил ПМЭ (подробнее см. стр. **60**) или изменении существующих (подробнее см. стр. **60**) 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 --action=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. **60**) 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.

Блокировка ошибочных пакетов

Механизм ПМЭ предусматривает блокировку ошибочных пакетов. Для выполнения процедуры блокировки используются политики Secret Net Studio.

Для включения срабатывания блокировки ошибочных пакетов выполните команду:

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

Для отключения срабатывания блокировки ошибочных пакетов выполните команду:

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

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 Studio, поскольку механизм ПМЭ представляет собой отдельный модуль ПО СЗИ Secret Net Studio 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 ПМЭ на контроль

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

Настройка механизма КЦ подсистемы межсетевого экранирования

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

Настройка механизма КЦ подсистемы ПМЭ 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 ПМЭ, а также реакция системы на нарушение КЦ защищаемых объектов задаются в конфигурационном файле **/opt/securitycode/sns-firewall/etc/fwfc.conf**.

Объектами КЦ подсистемы межсетевого экранирования являются:

- компоненты подсистемы ПМЭ (файлы и каталоги);
- процессы подсистемы ПМЭ (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/securitycode/sns-firewall/etc/fwfc.conf**.

Регистрация событий механизма КЦ подсистемы ПМЭ

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

Если в процессе контроля целостности ресурсов подсистемы ПМЭ происходит обнаружение несоответствия 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 Studio на факт нарушения КЦ объектов подсистемы ПМЭ представлены в конфигурационном файле **/opt/securitycode/sns-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 ПМЭ 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 ПМЭ, поставленных на контроль при установке подсистемы межсетевого экранирования, не требуется. Однако в Secret Net Studio предусмотрена возможность ручной настройки КЦ объектов, поставленных на контроль. Для этого необходимо в конфигурационный файл **/opt/securitycode/sns-firewall/etc/fwfc.conf** внести следующие изменения:

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

Совместное функционирование ПМЭ со специализированным ПО

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

При установленных ПО СЗИ Secret Net Studio и ПМЭ:

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

   ```
   /opt/securitycode/sns/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 Studio 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 Studio после приостановления его работы с помощью команды:

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

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

При неустановленных ПО СЗИ Secret Net Studio и ПМЭ:

1. Выполните настройку совместного функционирования ПО СЗИ Secret Net Studio 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 Studio 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/securitycode/sns/sbin/snunblock
```

2. Выполните настройку совместного функционирования ПО СЗИ Secret Net Studio 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 Studio с помощью команды:

```
systemctl restart sns-firewall
```

4. Перезагрузите компьютер.

Редактирование прав доступа UNIX

Утилита chown

В СЗИ Secret Net Studio предусмотрена возможность изменения владельца и/или группы, владеющей каждым из указанных файлов, в режиме командной строки с помощью утилиты **chown**.

Примечание.
Изменение владельца и/или группы посредством утилиты **chown** доступно только владельцу объектов файловой системы или администратору, обладающему правами суперпользователя компьютера.

Если задано только имя пользователя (или его числовой идентификатор), то данный пользователь становится владельцем каждого из указанных файлов, а группа этих файлов не изменяется.

Если за именем пользователя через двоеточие следует имя группы (или числовой идентификатор группы) без пробелов между ними, то изменяется также и группа файлов.

Если двоеточие или точка следует за именем пользователя, но группа не задана, то данный пользователь становится владельцем указанных файлов, а группа указанных файлов изменяется на основную группу пользователя.

Если опущено имя пользователя, а двоеточие или точка вместе с группой заданы, то будет изменена только группа указанных файлов.

Строка команды имеет следующий формат:

```
chown [<аргумент>] [<ключ> [<владелец>[:[группа]] <имя объекта>]],...[<ключ>
[<владелец>[:[группа]] <имя объекта>]]
```

```
chown [<аргумент>] [<ключ> [:[группа] <имя объекта>]],...[<ключ> [:[группа] <имя объекта>]]
```

```
chown [<аргумент>] --reference=<ФАЙЛ> [<имя объекта>]
```

Примечание.

- Команда **chown** изменяет владельца и/или группу каждого <имя объекта> на <владелец> и/или <группа>.
- Разделение команд изменения прав доступа к объектам файловой системы в рамках одной командной строки осуществляется с помощью запятых.
- Владелец не изменяется, если он не существует. Группа также не изменяется, если отсутствует, но изменяется на группу по умолчанию, если не задан пользователь.

Описание общего аргумента представлено в таблице ниже.

Аргумент	Описание
--help	Выводит справочную информацию о применении утилиты
--version	Выводит информацию о версии утилиты
--	Завершает ввод аргументов командной строки

Описание ключей представлено в таблице ниже.

Ключ		Описание
-c	--changes	Включение подробного описания действия для объектов доступа, права которых действительно изменяются
-f	--silent --quiet	Отключение сообщений об ошибке для объектов доступа, права которых не могут быть изменены
-v	--verbose	Включение подробного описания действия или отсутствия действия для каждого объекта доступа
-R	--recursive	Рекурсивное изменение прав доступа для объектов файловой системы и их содержимого
--reference=<ФАЙЛ>		Изменение права доступа к файлу на те права, что имеет <ФАЙЛ>
--dereference		Изменение прав для файла, к которому ведет символическая ссылка, вместо самой ссылки
--no-dereference		Работа с самими символьными ссылками, а не с файлами, на которые они указывают. Данный параметр доступен, только если имеется системный вызов lchown
--from=<текущий_владелец>:<текущая_группа>		Изменяет владельца и/или группу каждого файла, только если текущий владелец и/или группа совпадает с <текущий_владелец>:<текущая_группа>. Как группа, так и владелец могут быть опущены, в этом случае совпадение для данного атрибута не обязательно

Примечание.

Ключи могут отличаться от версии утилит.

Утилита chmod

В СЗИ Secret Net Studio предусмотрена возможность изменения прав доступа к объектам файловой системы в режиме командной строки с помощью утилиты **chmod**.

Примечание.

Изменение прав доступа к объектам файловой системы посредством утилиты **chmod** доступно только владельцу объектов файловой системы или администратору, обладающему правами суперпользователя компьютера.

Строка команды имеет следующий формат:

```
chmod [<аргумент>] [<ключ> [<параметр — режим доступа> <имя объекта>]],...[<ключ> [<параметр — режим доступа> <имя объекта>]]
```

```
chmod [<аргумент>] --reference=<ФАЙЛ> [<имя объекта>]
```

Примечание.
Разделение команд изменения прав доступа к объектам файловой системы в рамках одной командной строки осуществляется с помощью запятых.

Описание общего аргумента представлено в таблице ниже.

Аргумент	Описание
--help	Выводит справочную информацию о применении утилиты
--version	Выводит информацию о версии утилиты
--	Завершает ввод аргументов командной строки

Описание ключей представлено в таблице ниже.

Ключ		Описание
-c	--changes	Включение подробного описания действия для объектов доступа, права которых действительно изменяются
-f	--silent --quiet	Отключение сообщений об ошибке для объектов доступа, права которых не могут быть изменены
-v	--verbose	Включение подробного описания действия или отсутствия действия для каждого объекта доступа
-R	--recursive	Рекурсивное изменение прав доступа для объектов файловой системы и их содержимого
--reference=<ФАЙЛ>		Изменить права доступа к файлу на те права, что имеет <ФАЙЛ>

Примечание.
Ключи могут отличаться от версии утилит.

Команда **chmod** может быть представлена в символьном или числовом формате.

Символьный формат команды chmod

Использование команды **chmod** в символьном формате позволяет гибко добавлять, устанавливать или удалять права доступа к объектам файловой системы для разных типов пользователей.

В символьном формате параметр **[режим доступа]** представляет собой символьную команду изменения прав доступа, состоящую из следующих элементов:

- <категория пользователей> — определяет пользователей, которым будут изменяться права;
- <оператор> — определяет операцию, которая будет выполняться с объектами файловой системы;
- <права доступа> — определяет, какие именно права доступа к объектам файловой системы будут установлены, добавлены или удалены.

Описание элемента <категория пользователей> представлено в таблице ниже.

Категория пользователей	Описание
u	Владелец объекта файловой системы
g	Пользователи, входящие в группу владельца объекта файловой системы
o	Остальные пользователи

Примечание.
В случае если в рамках параметра [режим доступа] не указана ни одна категория пользователей, изменение прав доступа к объектам файловой системы осуществляется автоматически для всех пользователей.

Описание элемента <оператор> представлено в таблице ниже.

Оператор	Описание
+	Добавляет права доступа к правам, уже имеющимся у объекта файловой системы
–	Удаляет права доступа, уже имеющиеся у объекта файловой системы
=	Устанавливает определенные права доступа конкретному объекту файловой системы

Описание элемента <права доступа> представлено в таблице ниже.

Права доступа	Описание
r	Право на открытие объекта на чтение
w	Право на открытие объекта на запись
x	Право на выполнение объекта (для каталогов — право на чтение содержимого каталога)
X	Право на выполнение объекта, если файл является каталогом или уже имеет право на исполнение для какого-либо пользователя
s	Присвоение объектам файловой системы атрибутов SUID или SGID, позволяющих запускать файлы на выполнение с правами владельца файла или группы владельца файла соответственно
t	Присвоение объекту файловой системы sticky бита, предоставляющего право на удаление файла в каталоге только владельцу файла или владельцу каталога
u	Предоставление остальным пользователям права доступа владельца объекта файловой системы
g	Предоставление остальным пользователям права доступа группы владельца объекта файловой системы
o	Предоставление остальным пользователям права доступа пользователей, не входящих в группу владельца объекта файловой системы

Примеры:

```
chmod u=rwx,g=rx,o=x filename
```

Предоставление владельцу файла права на чтение, запись и выполнение, группе владельца файла права на чтение и выполнение, остальным пользователям права на выполнение.

```
chmod u+x,g-x,o-wx filename
```

Добавление для владельца файла права на выполнение, удаление для группы владельца файла права на выполнение, удаление для остальных пользователей права на запись и выполнение.

```
chmod -R a+r directory
```

Рекурсивное добавление для всех пользователей права на чтение каталога.

```
chmod -R u-s,g-s directory
```

Рекурсивное удаление атрибутов SUID и SGID для каталога.

Числовой формат команды chmod

Использование команды **chmod** в числовом формате позволяет устанавливать абсолютные права доступа к объектам файловой системы.

При вводе команды в числовом формате параметр **[режим доступа]** записывается для прав типа "rwx" в виде трехзначного восьмеричного числа, а при установленных битах SUID, SGID и Sticky в виде четырехзначного восьмеричного числа одной строкой сразу для трех типов пользователей:

- владельца объекта файловой системы (u);
- пользователей, входящих в группу владельца объекта файловой системы (g);
- остальных пользователей (o).

Описание числового формата команды **chmod** представлено в таблице ниже.

Числовой формат	Символьный формат	Права на файл	Права на каталог
0	---	Нет прав	Нет
1	--x	Выполнение	Чтение файлов и их свойств
2	-w-	Запись	Нет
3	-wx	Запись и выполнение	Все, кроме чтения списка файлов
4	r--	Чтение	Чтение имен файлов
5	r-x	Чтение и выполнение	Доступ на чтение
6	rw-	Чтение и запись	Чтение имен файлов
7	rwx	Все права	Все права

Примечание.
Право на запись файла предоставляет пользователю возможность его записи или изменения, а право на запись каталога — возможность создания новых файлов или удаления файлов из этого каталога. В случае если для каталога установлено право записи (w), пользователь с назначенными правами может удалить файл внутри этого каталога, даже если право на запись не установлено для данного файла.

Помимо стандартных прав типа "rwx" команда **chmod** осуществляет управление битами:

- SUID — имеет вес 4000 и позволяет запускать объекты файловой системы на выполнение с правами владельца файла;
- SGID — имеет вес 2000 и позволяет запускать объекты файловой системы на выполнение с правами группы владельца файла;
- бит Sticky — имеет вес 1000, используется только с каталогами и запрещает удаление файла из каталога всем пользователям, кроме владельца данного файла.

Примечание.
Присвоение бита SGID каталогу устанавливает принадлежность каждого нового создаваемого внутри него файла к группе каталога, а не к группе владельца файла.

Примеры:

```
chmod 400 filename
```

Предоставление владельцу файла права на чтение. Никто другой не имеет права выполнять никакие действия с файлом.

```
chmod 744 filename
```

Предоставление владельцу файла всех прав доступа, группе владельца файла и остальным пользователям — права на чтение файла.

```
chmod 2555 directory
```

Предоставление каждому пользователю права на чтение файлов внутри каталога с правами группы владельца каталога.

```
chmod 4555 filename
```

Предоставление каждому пользователю права на чтение и на выполнение файла с правами владельца файла.

Редактирование списка POSIX ACL

Утилита getfacl

В СЗИ Secret Net Studio предусмотрена возможность вывода имени файла, владельца, группы-владельца и ACL в режиме командной строки с помощью утилиты **getfacl**.

Если каталог имеет ACL по умолчанию, то утилита выводит также ACL по умолчанию. Файлы не могут иметь ACL по умолчанию.

Для большого количества файлов утилита выводит ACL, разделенные пустыми строками. Результаты утилиты могут использоваться как входные данные для утилиты **setfacl**.

Строка команды имеет следующий формат:

```
getfacl [-dRLP] <ФАЙЛ> ...
```

Пример ввода команды:

```
1: # file: <ПУТЬ>
2: # owner: <владелец>
3: # group: <группа>
4: user::rwx
5: user:<пользователь>:rwx              #effective:r-x
6: group::rwx                           #effective:r-x
7: group:<группа>:r-x
8: mask:r-x
9: other:r-x
10: default:user::rwx
11: default:user:<пользователь>:rwx     #effective:r-x
12: default:group::r-x
```

```
13: default:mask:r-x
14: default:other:---
```

Строки 4, 6 и 9 относятся к традиционным битам прав доступа к файлу для владельца, группы-владельца и всех остальных соответственно. Эти три элемента являются базовыми.

Строки 5 и 7 являются элементами для отдельных пользователя и группы.

Строка 8 является маской эффективных прав. Этот элемент ограничивает эффективные права, предоставляемые всем группам и отдельным пользователям. Маска не влияет на права для владельца файла и всех других.

Строки 10–14 показывают ACL по умолчанию для данного каталога.

Описание ключей представлено в таблице ниже.

Ключ		Описание
-d	--default	Вывод только ACL – по умолчанию
-R	--recursive	Осуществить вывод для подкаталогов рекурсивно
-L	--logical	Следовать по символическим ссылкам. По умолчанию символические ссылки, не указанные в командной строке, игнорируются
-P	--physical	Не следовать по символическим ссылкам, даже если они указаны в командной строке
-a	--access	Вывести только ACL файла
-c	--omit-header	Не показывать заголовок (имя файла)
-e	--all-effective	Показывает все эффективные права
-E	--no-effective	Не показывает эффективные права
-s	--skip-base	Пропускает файлы, имеющие только основные записи
-t	--tabular	Использует табулированный формат вывода
-n	--numeric	Показывает числовые значения пользователя/группы
-p	--absolute-names	Не удалять ведущие "/" из пути файла
-h	--help	Выводит справочную информацию о применении утилиты
-v	--version	Выводит информацию о версии утилиты

Примечание.
Ключи могут отличаться от версии утилит.

Утилита setfacl

В СЗИ Secret Net Studio предусмотрена возможность редактировать ACL к файлам и каталогам в режиме командной строки с помощью утилиты **setfacl**.

Строка команды имеет следующий формат:

```
setfacl [-bkndRLP] { -m|-M|-x|-X ... } <ФАЙЛ> ...
```

Описание ключей представлено в таблице ниже.

Ключ		Описание
-m	--modify=<ACL>	Изменяет текущий ACL для файла
-M	--modify-file=<ФАЙЛ>	Прочитывает записи ACL для модификации из файла
-x	--remove=<ACL>	Удаляет записи из ACL файла
-X	--remove-file=<ФАЙЛ>	Прочитывает записи ACL для удаления из файла
-b	--remove-all	Удаляет все расширенные записи ACL
-k	--remove-default	Удаляет ACL по умолчанию

Ключ		Описание
-n	--no-mask	Не пересчитывать маску эффективных прав. Обычно утилита **setfacl** пересчитывает маску (кроме случая явного задания маски) для того, чтобы включить ее в максимальный набор прав доступа элементов, на которые воздействует маска (для всех групп и отдельных пользователей)
-d	--default	Применить ACL по умолчанию
-R	--recursive	Осуществить вывод для подкаталогов рекурсивно
-L	--logical	Следовать по символическим ссылкам. По умолчанию ссылки, не указанные в командной строке, игнорируются
-P	--physical	Не следовать по символическим ссылкам, даже если они указаны в командной строке
--set=<ACL>		Устанавливает ACL для файла, заменив текущий ACL
--set-file=<ЗАПИСИ_ACL>		Прочитывает записи ACL для установления из файла
--mask		Пересчитывает маску эффективных прав
--restore=<ФАЙЛ>		Восстанавливает резервную копию прав доступа, созданную командой **getfacl -R** или ей подобной. Все права доступа дерева каталогов восстанавливаются, используя этот механизм. Если вводимые данные содержат элементы для владельца или группы-владельца и команда **setfacl** выполняется пользователем с именем **root**, то владелец и группа-владелец всех файлов также восстанавливаются. Этот параметр не может использоваться совместно с другими параметрами, за исключением параметра **--test**
--test		Режим тестирования (ACL не изменяются)
-h	--help	Выводит справочную информацию о применении утилиты
-v	--version	Выводит информацию о версии утилиты

Примечание.
Ключи могут отличаться от версии утилит.

Удаленное управление

Secret Net Studio может функционировать совместно с СБ SNS и Security Code Orchestrator. Эти средства защиты информации в режиме совместного функционирования позволяют осуществлять:

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

Внимание!
Для подключения к СБ SNS компьютер должен быть включен в домен и подчинен серверу безопасности в структуре управления.

Включение и выключение режима удаленного управления

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

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

```
snpolctl -p service_mgr -c services,snnetwork,1
snpolctl -p service_mgr -c services,snnetwork,0
```

Для регистрации продукта на сервере Security Code Orchestrator введите в командную строку:

```
snconnctl --registration --ip=<ip-адрес>
```

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 Studio и не устанавливаются при его установке.

Внимание!
Включение компьютера в домен рекомендуется выполнять после установки ПО СЗИ Secret Net Studio. В случае если компьютер был включен в домен Windows до установки ПО СЗИ Secret Net Studio, 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)**, а для всех остальных ОС обеспечение корректной работы сетевого взаимодействия достигается с помощью пакета программ **Samba** 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
   ```
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.

6. 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 можете 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@SECRET.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 при помощи 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 Ред ОС 7.3 и AlterOS 7.5:

В Ред ОС и AlterOS 7.5 присутствует скрипт для автоматизации ввода компьютера в домен или стандартные средства ввода в домен.

Для установки скрипта введите команду:

```
# sudo dnf install join-to-domain
```

Скрипт может выполнятся в трех режимах:

- с графическим интерфейсом;
- в консоли (интерактивный режим);
- в консоли с входными параметрами.

Для запуска скрипта ввода в домен с графическим интерфейсом, перейдите в главное Меню — Системные — Ввод ПК в домен.

Для запуска скрипта в консоли в интерактивном режиме добавления к домену, выполните:

```
# join-to-domain.sh
```

Скриптом будет запрошен ввод имени домена, компьютера, а также имя администратора домена и его пароль.

Для запуска скрипта с параметрами в консоли:

```
# join-to-domain.sh -d example.com -n client1 -u admin -p password
```

Чтобы ввести стандартными средствами нужно установить зависимости.

Для **Winbind**:

```
# sudo dnf install samba samba-client samba-winbind samba-winbind-clients oddjob
oddjob-mkhomedir
```

И ввести в домен:

```
# net ads join -U Administrator
```

Для **SSSD**:

```
# sudo dnf install -y realmd sssd oddjob oddjob-mkhomedir adcli samba-common samba-
common-tools krb5-workstation
```

И ввести в домен:

```
# sudo realm join -U -v <имя_администратора_домена> <realm_name>
```

Настройка подключения к серверу безопасности SNS

Для настройки подключения к серверу безопасности SNS используется утилита **snnetctl**. Описание утилиты и особенности ее применения приведены на стр. **48**.

Настройка подключения к серверу Security Code Orchestrator

Для настройки подключения к серверу Security Code Orchestrator используется утилита **snconnctl**. Описание утилиты и особенности ее применения приведены на стр. **48**.

Сигнализация и аудит

Система Secret Net Studio 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 системе Secret Net Studio предусмотрена возможность получения администратором безопасности уведомлений на локальный адрес электронной почты.

Ограниченный режим работы Secret Net Studio

После установки Secret Net Studio функционирует в ограниченном режиме работы до активации продукта. Для выхода из ограниченного режима необходимо ввести действительную лицензию "Базовая защита". Для других компонентов необходимо либо наличие активной лицензии, либо отсутствие лицензии.

В случае истечения лицензии для работающего компонента Secret Net Studio будет функционировать в ограниченном режиме. Для возврата СЗИ в штатный режим функционирования необходимо отключить подсистемы с истекшей лицензией или заменить лицению.

Работа ограниченного режима распространяется на следующие утилиты:

- snpolctl;
- snjournaldctl;
- snaidectl;
- snsablectl;
- snscheck;
- snaecctl;
- sndevctl;
- fw-localcfg.

Примечание.
Доступно выключение защитных подсистем и отключение интеграции с комплексом "Соболь".

Работа ограниченного режима не распространяется на следующие утилиты:

- sntokenctl;
- snlicensectl;
- snnetctl;
- fw-net;
- snjrnl;
- snconnctl.

Примечание.
- Очистка журналов с использованием командной строки разрешена.
- Утилиты управления пользователями и правами доступа работают без ограничений.

Приложение

Рекомендации по настройке для соответствия требованиям о защите информации

В разделе приведены значения параметров безопасности Secret Net Studio, 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 Studio 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 Studio 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 Studio.

Параметры политик Secret Net Studio

Для соответствия классам защищенности АС 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.1 Параметры политик

Параметр	Классы защищенности АС		
	1Г, 1Д	2Б	3Б
Политика "Пользователи" (users)			
Минимальная длина пароля (символ) ID: **min_passwd_size** Знач. по умолч.: **7**	все: 6 (обяз.)	6 (обяз.)	6 (обяз.)

Параметр	Классы защищенности АС		
	1Г, 1Д	**2Б**	**3Б**
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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	все: –	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	все: –	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	все: –	–	–
Политика "Идентификация и аутентификация" (authentication)			
Режим идентификации ID: **ident** Знач. по умолч.: **2**	все: –	–	–
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	все: Да (обяз.)	Да (обяз.)	Да (обяз.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	все: –	–	–
Кэшировать данные идентификаторов 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 (мин) ID: **unlock_time** Знач. по умолч.: **0**	все: –	–	–
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	все: 10 (реком.)	10 (реком.)	10 (реком.)
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	все: –	–	–
Политика "Контроль устройств" (devices_control)			
Параметры контроля	1Г: Параметры заданы, при этом для класса "Устройства USB" включен режим "Подключение устройства запрещено" (обяз.) 1Д: –	–	–

Параметр	Классы защищенности АС		
	1Г, 1Д	2Б	3Б
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	все: –	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	1Г: 2 (обяз.) 1Д: –	–	–
Политика "Дискреционное управление доступом" (access_control)			
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	все: –	–	–
Политика "Затирание памяти и файлов" (data_wipe)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –		
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	1Г: Да (обяз.) 1Д: –	–	–
Политика "Замкнутая программная среда" (aec)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	1Г: Да (обяз.) 1Д: –	–	–
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	1Г: 2 (обяз.) 1Д: –	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1Г: 1 (обяз.) 1Д: –	–	–
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: –	–	–
Белый список пользователей и групп	1Г: root (обяз.) 1Д: –	–	–
Политика "Контроль печати" (cups)			

Параметр	Классы защищенности АС		
	1Г, 1Д	2Б	3Б
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	1Г: Да (обяз.) 1Д: Да (реком.)	Да (реком.)	Да (реком.)
Политика "Контроль целостности" (aide)			
Настройка КЦ	все: (обяз.)	(обяз.)	(обяз.)
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	все: Да (обяз.)	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	все: 2 (реком.)	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)			
Режим работы Знач. по умолч.: **Нет**	все: –	–	–
Контроль секторов Знач. по умолч.: **Нет**	все: –	–	–
Контроль файлов Знач. по умолч.: **Нет**	все: –	–	–
Контроль PCI-устройств Знач. по умолч.: **Нет**	все: –	–	–
Контроль SMBIOS Знач. по умолч.: **Нет**	все: –	–	–
Политика "Системные настройки" (system)			
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	все: Да (реком.)	Да (реком.)	Да (реком.)
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	все: –	–	–
Политика "Межсетевой экран" (firewall)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	все: Да (реком.)	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	все: –	–	–

Государственные информационные системы

При определенных вариантах настройки Secret Net Studio 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 Studio в ГИС всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия классам защищенности ГИС 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.2 Параметры политик

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Политика "Пользователи" (users)			
Минимальная длина пароля (символ) ID: **min_passwd_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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Политика "Идентификация и аутентификация" (authentication)			

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Режим 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.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	–	–	–
Кэшировать данные идентификаторов 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 (мин) ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	–	–	–
Политика "Контроль устройств" (devices_control)			
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: **state** Знач. по умолч.: **Да**	–	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Политика "Дискреционное управление доступом" (access_control)			
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Затирание памяти и файлов" (data_wipe)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	Да (обяз.)	–	–

Параметр	Классы защищенности ГИС		
	К1	**К2**	**К3**
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Замкнутая программная среда" (aec)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	2 (обяз.)	–	–
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	–	–
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Белый список пользователей и групп	root (обяз.)	–	–
Политика "Контроль печати" (cups)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Политика "Контроль целостности" (aide)			
Настройка КЦ	(обяз.)	(обяз.)	–
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	2 (реком.)	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)			
Режим работы Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль секторов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль файлов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–

Параметр	Классы защищенности ГИС		
	К1	К2	К3
Контроль PCI-устройств Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль SMBIOS Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Политика "Системные настройки" (system)			
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (реком.)
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Политика "Межсетевой экран" (firewall)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	–	–	–

Информационные системы персональных данных

При определенных вариантах настройки Secret Net Studio 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 Studio в ИСПДн всех уровней защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

Для соответствия уровням защищенности ИСПДн 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.3 Параметры политик

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Политика "Пользователи" (users)				
Минимальная длина пароля (символ) ID: **min_passwd_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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	–	–	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	–	–	–	–
Политика "Идентификация и аутентификация" (authentication)				
Режим 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.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	–	–	–	–
Кэшировать данные идентификаторов для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–	–

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
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 (мин) ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	–	–	–	–
Политика "Контроль устройств" (devices_control)				
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: **state** Знач. по умолч.: **Да**	–	–	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	–	–
Политика "Дискреционное управление доступом" (access_control)				
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Затирание памяти и файлов" (data_wipe)				
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)	–
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	–	–	–	–
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)	–
Политика "Замкнутая программная среда" (aec)				
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	–	–	–	–
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	–	–	–	–

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Режим работы ID: **mode** Знач. по умолч.: **0**	–	–	–	–
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	–	–	–	–
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	–	–	–	–
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	–	–	–	–
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	–	–	–	–
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	–	–	–	–
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	–	–	–	–
Белый список пользователей и групп	–	–	–	–
Политика "Контроль печати" (cups)				
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Политика "Контроль целостности" (aide)				
Настройка КЦ	(обяз.)	(обяз.)	–	–
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	2 (реком.)	2 (реком.)	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)				
Режим работы Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–	–
Контроль секторов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–	–
Контроль файлов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–	–
Контроль PCI-устройств Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–	–
Контроль SMBIOS Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–	–
Политика "Системные настройки" (system)				
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (реком.)	Да (реком.)

Параметр	Уровни защищенности ИСПДн			
	1	2	3	4
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–	–
Политика "Межсетевой экран" (firewall)				
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	–	–	–	–

Информационные системы Банка России

При определенных вариантах настройки Secret Net Studio 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 основных требований для 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 доверенной загрузки может использоваться изделие "Программно-аппаратный комплекс "Соболь".

Обеспечение непрерывности функционирования

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

Параметры политик Secret Net Studio

Для соответствия уровням защиты информации ИС Банка России 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.4 Параметры политик

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Политика "Пользователи" (users)			
Минимальная длина пароля (символ) ID: **min_passwd_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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Политика "Идентификация и аутентификация" (authentication)			
Режим 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.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	–	–	–
Кэшировать данные идентификаторов для доменных пользователей ID: **cache** Знач. по умолч.: **Нет**	–	–	–

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Количество неудачных попыток входа ID: **deny** Знач. по умолч.: **4**	–	–	–
Время блокировки при достижении количества неудачных попыток аутентификации (мин) ID: **unlock_time** Знач. по умолч.: **0**	30 (обяз.)	30 (обяз.)	30 (обяз.)
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	15 (обяз.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Политика "Контроль устройств" (devices_control)			
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: **state** Знач. по умолч.: **Да**	–	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Политика "Дискреционное управление доступом" (access_control)			
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Затирание памяти и файлов" (data_wipe)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	Да (реком.)	–	–
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)
Политика "Замкнутая программная среда" (aec)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	2 (обяз.)	2 (обяз.)	

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	**УЗ-2**	**УЗ-3**
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	1 (обяз.)	–
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	–
Белый список пользователей и групп	root (обяз.)	root (обяз.)	–
Политика "Контроль печати" (cups)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Политика "Контроль целостности" (aide)			
Настройка КЦ	(обяз.)	(обяз.)	(обяз.)
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	2 (реком.)	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)			
Режим работы Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	–
Контроль секторов Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	–
Контроль файлов Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	–
Контроль PCI-устройств Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	–
Контроль SMBIOS Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	–
Политика "Системные настройки" (system)			
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–

Параметр	Уровень защиты информации ИС Банка России		
	УЗ-1	УЗ-2	УЗ-3
Политика "Межсетевой экран" (firewall)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	–	–	–

Автоматизированные системы управления производственными и технологическими процессами

При определенных вариантах настройки Secret Net Studio 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 Studio в АСУ ТП всех классов защищенности рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

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**
Политика "Пользователи" (users)			
Минимальная длина пароля (символ) ID: **min_passwd_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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Политика "Идентификация и аутентификация" (authentication)			
Режим 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.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	–	–	–
Кэшировать данные идентификаторов 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 (мин) ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	–	–	–
Политика "Контроль устройств" (devices_control)			
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: **state** Знач. по умолч.: **Да**	–	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Политика "Дискреционное управление доступом" (access_control)			
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Затирание памяти и файлов" (data_wipe)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Замкнутая программная среда" (aec)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	2 (обяз.)		
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	–	–
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–

Параметр	Классы защищенности АСУ ТП		
	К1	К2	К3
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Белый список пользователей и групп	root (обяз.)	–	–
Политика "Контроль печати" (cups)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)
Политика "Контроль целостности" (aide)			
Настройка КЦ	(обяз.)	(обяз.)	(обяз.)
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	2 (реком.)	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)			
Режим работы Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль секторов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль файлов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль PCI-устройств Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль SMBIOS Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Политика "Системные настройки" (system)			
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (реком.)
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Политика "Межсетевой экран" (firewall)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	–	–	–

Критическая информационная инфраструктура Российской Федерации

При определенных вариантах настройки Secret Net Studio 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 Studio в КИИ всех категорий значимости рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

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
Политика "Пользователи" (users)			
Минимальная длина пароля (символ) ID: **min_passwd_size** Знач. по умолч.: **7**	8 (обяз.)	6 (обяз.)	6 (обяз.)

Параметр	Категории значимости КИИ		
	К1	**К2**	**К3**
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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	–	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	–	–	–
Политика "Идентификация и аутентификация" (authentication)			
Режим 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.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	–	–	–
Кэшировать данные идентификаторов 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 (мин) ID: **unlock_time** Знач. по умолч.: **0**	60 (обяз.)	30 (обяз.)	15 (обяз.)
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	5 (обяз.)	15 (реком.)	15 (реком.)
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	–	–	–
Политика "Контроль устройств" (devices_control)			
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.)

Параметр	Категории значимости КИИ		
	К1	К2	К3
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	–	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)	2 (обяз.)
Политика "Дискреционное управление доступом" (access_control)			
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Затирание памяти и файлов" (data_wipe)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Политика "Замкнутая программная среда" (aec)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	–	–
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	2 (обяз.)	–	
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	–	–
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	–	–
Белый список пользователей и групп	root (обяз.)	–	–
Политика "Контроль печати" (cups)			
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)	Да (реком.)

Параметр	Категории значимости КИИ		
	К1	К2	К3
Политика "Контроль целостности" (aide)			
Настройка КЦ	(обяз.)	(обяз.)	(обяз.)
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	2 (реком.)	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)			
Режим работы Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль секторов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль файлов Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль PCI-устройств Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Контроль SMBIOS Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	–
Политика "Системные настройки" (system)			
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)	Да (реком.)
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–	–
Политика "Межсетевой экран" (firewall)			
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	–	–	–

Информационные системы, предназначенные для обработки биометрических персональных данных

При определенных вариантах настройки Secret Net Studio 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 Studio в ЕБС всех уровней защиты информации рекомендуется в каждом домене безопасности использовать не менее двух серверов безопасности.

Параметры политик Secret Net Studio

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**
Политика "Пользователи" (users)		
Минимальная длина пароля (символ) ID: **min_passwd_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.)
Предупреждение о смене пароля (день) ID: **warn_days** Знач. по умолч.: **1**	–	–
Интервал между сменами пароля ID: **min_days** Знач. по умолч.: **0**	–	–
Блокировать пользователя после устаревания пароля ID: **inactive_days** Знач. по умолч.: **0**	–	–
Политика "Идентификация и аутентификация" (authentication)		
Режим идентификации ID: **ident** Знач. по умолч.: **2**	1 (обяз.)	1 (реком.)
Усиленная аутентификация ID: **strength** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)
Реакция на изъятие идентификатора ID: **lock** Знач. по умолч.: **0**	–	–
Кэшировать данные идентификаторов 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 (мин) ID: **unlock_time** Знач. по умолч.: **0**	30 (обяз.)	30 (обяз.)
Максимальный период неактивности до блокировки монитора (мин) ID: **lock_delay** Знач. по умолч.: **10**	15 (обяз.)	15 (обяз.)
Оповещение пользователя о последнем успешном входе в систему ID: **last_log** Знач. по умолч.: **Нет**	Да (обяз.)	–
Политика "Контроль устройств" (devices_control)		

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	**ЕБС-2**
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: **state** Знач. по умолч.: **Да**	–	–
Детализация сообщений ID: **verbose** Знач. по умолч.: **0**	2 (обяз.)	2 (обяз.)
Политика "Дискреционное управление доступом" (access_control)		
Статус подсистемы ID: **mode** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Политика "Затирание памяти и файлов" (data_wipe)		
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Очистка оперативной памяти ID: **ram** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Затирание диска ID: **local_drives** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Политика "Замкнутая программная среда" (aec)		
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)
Алгоритм хеширования ID: **alg** Знач. по умолч.: **2**	2 (обяз.)	2 (обяз.)
Режим работы ID: **mode** Знач. по умолч.: **0**	1 (обяз.)	1 (обяз.)
Регистрация событий: исполнение файлов ID: **log_perm_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация событий: запрет исполнения файлов ID: **log_deny_exec** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация событий: загрузка библиотек ID: **log_perm_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация событий: запрет загрузки библиотек ID: **log_deny_openlib** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация событий: открытие файлов ID: **log_perm_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Регистрация событий: запрет открытия файлов ID: **log_deny_openfile** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)

Параметр	Уровень защиты информации ЕБС	
	ЕБС-1	ЕБС-2
Белый список пользователей и групп	root (обяз.)	root (обяз.)
Политика "Контроль печати" (cups)		
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (реком.)	Да (реком.)
Политика "Контроль целостности" (aide)		
Настройка КЦ	(обяз.)	(обяз.)
Статус подсистемы ID: **state** Знач. по умолч.: **Да**	Да (обяз.)	Да (обяз.)
Алгоритм ID: **alg** Знач. по умолч.: **2**	2 (реком.)	2 (реком.)
Подсистема "Комплекс "Соболь" (утилита snsablectl)		
Режим работы Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Контроль секторов Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Контроль файлов Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Контроль PCI-устройств Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Контроль SMBIOS Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Политика "Системные настройки" (system)		
Блокировать компьютер при нарушении ФК ID: **system_lock** Знач. по умолч.: **Нет**	Да (обяз.)	Да (обяз.)
Перезапись журнала при переполнении ID: **clear_log** Знач. по умолч.: **Нет**	–	–
Политика "Межсетевой экран" (firewall)		
Статус подсистемы ID: **state** Знач. по умолч.: **Нет**	Да (реком.)	Да (реком.)
Блокировка ошибочных пакетов ID: **block_inv_packets** Знач. по умолч.: **0**	true	true

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 Studio 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 Studio
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
Journal subsystem/Сервис журналирования
Backup/Резервное копирование
Hardware Trusted Boot/комплекс "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 Studio"

Common Secret Net group msg/Группа событий общих сообщений Secret Net Studio
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 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
Successful connection to the Security Code Orchestrator/Успешное подключение к Security Code Orchestrator
Security Code Orchestrator connection error/Ошибка подключения к Security Code Orchestrator
Successful disconnection from the Security Code Orchestrator/Успешное отключение от Security Code Orchestrator
Security Code Orchestrator disconnection error/Ошибка отключения от Security Code Orchestrator

Группа сообщений "События модулей ядра"

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

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

Правила приемки и методы контроля

Приемка Secret Net Studio 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.